HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 104 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, May 3, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 3, 2018

● (0845)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I will call order meeting number 104 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h)(vii), we are studying the breach of personal information involving Cambridge Analytica and Facebook.

Today we welcome our friends from across the water. From the United Kingdom House of Commons Digital, Culture, Media and Sport Select Committee, we have Mr. Damian Collins.

Welcome to Canada this morning.

Mr. Damian Collins (Chair, MP, United Kingdom House of Commons Digital, Culture, Media and Sport Select Committee): Thank you. It's a pleasure to be part of your inquiry.

The Chair: We appreciate your time.

Go ahead. We'll hear your opening comments. Then we'll open it up for questions.

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

I thought I would just set out the nature of the work we're doing in the United Kingdom at the moment.

Our inquiry is slightly different in scope from yours. It's looking at the use of fake news and disinformation and the disruptive impact they have on elections and democracy. A particular focus in recent weeks has been the use of data in targeting voters with particular pieces of information, the lack of transparency of that and how it's done and, in particular, the legality of some of those practices, particularly if information about people's political views is being held by private companies and consultantcies and being used in campaigns directed toward them.

We are conducting our inquiry as a parliamentary committee, and therefore as a consequence of that work, there's been a particular interest for us in the work of Cambridge Analytica, SCL, and AggregateIQ, particularly because of AIQ's work in the European referendum, the Brexit referendum in the U.K. We have particular interests in that area.

We're also working quite closely with the U.K. Information Commissioner. She is conducting an investigation into these matters, as you know. In particular, she is looking at the use of data in elections. She'll be producing a policy report on that later this month, as well as conducting what are now criminal investigations of certain individuals involved in this work. The U.K. Electoral Commission is also conducting an inquiry into some of the questions around the way in which the leave campaigns were run and whether there was coordination between them in the U.K. during that same referendum as well.

We have three separate inquiries going on. They overlap in places but will report separately.

Certainly for my committee, our main interest at the moment, as part of our disinformation campaign, is looking at the way data is used to target the information of people on social media.

The Chair: Thank you, Mr. Collins.

We'll open it up for questions, starting with Mr. Erskine-Smith.

You have seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much, Mr. Collins. It's nice to see you.

My first question is about AIQ. We certainly had them before us, and they were less than forthcoming. Have they agreed to testify before your committee?

Mr. Damian Collins: They've agreed in principle to testify. They wanted to get back to us to confirm when they would testify, but after they've given evidence to your committee. We are currently in discussions with them about when they will give evidence, but I hope that will be in the next few weeks.

● (0850)

Mr. Nathaniel Erskine-Smith: I'm curious. We typically do not swear witnesses in, although we have the powers to do so. Have you sworn in witnesses in the course of your investigation and inquiry?

Mr. Damian Collins: No, we haven't yet. Similar you in Canadian House of Commons, there is a general presumption that people should tell the truth in front of parliamentary committees. It can be considered contempt of Parliament if you don't.

We do have a separate power to get people to swear on oath, which would carry a similar offence to perjury if someone were found to have lied under oath, but we've not yet used that. It's certainly not the custom in the British House of Commons to use that, but it's a power we can use.

Mr. Nathaniel Erskine-Smith: It's the same in our Parliament, of course. It's not our custom traditionally, but I would encourage you to consider it when you have AIQ before you.

When Chris Vickery testified before you recently, he seemed to directly contradict the testimony we heard from AIQ. Perhaps you could give a brief rundown for our committee the nature of that testimony and how directly in conflict it was.

Mr. Damian Collins: Chris Vickery identified on GitLab a set of files and data that had been placed there by AIQ. He made a copy of that dataset, and he's given us a copy, but he also discussed some elements of that data and what it contained when he gave evidence to the committee.

What it does seem to demonstrate, though, is the high level of coordination between AIQ, SCL, and Cambridge Analytica, the ability to access and share information in files between those different companies. Also, all of the data that was being managed as part of the Brexit referendum campaign was interchangeable and easily shared. Indeed, at some point, all of that information was made publicly available on the web.

Of course the question is, why was it made available in that way? Was that just a mistake that someone made? Chris Vickery seems to think it could have been a mistake. But, of course, it could have been done deliberately so that the people they wanted to find it could find it if they knew what they were looking for—and Chris Vickery managed to find it.

Mr. Nathaniel Erskine-Smith: Obviously, we are not engaged with the issue of Brexit. Our investigation was specific to the Facebook-Cambridge Analytica data scandal. However, we heard testimony that seemed to be relevant to your purposes. We heard testimony from AIQ that there wasn't coordination between the various Brexit campaigns, and yet the evidence seemed to directly contradict their testimony. Their testimony and the answers they gave us didn't seem all that solid.

What are the next steps for your committee in examining this, and can our committee be of assistance?

Mr. Damian Collins: Absolutely. One of the reasons I was particularly pleased to be speaking to you today is that I think the more closely our respective committees coordinate in examining these issues, the more effective we will be. We have different jurisdictional powers but common interests. I think the evidence that you received from AIQ is certainly significant for us. They said that the invoices that have come from different campaign groups in the referendum campaign were paid by Vote Leave, which would suggest a degree of coordination. Certainly, in the management of data, there seems to be coordination by AIQ across different campaigns. We know that the U.K. Information Commissioner is trying to get access to the data and has been frustrated in that process.

Mr. Nathaniel Erskine-Smith: On the point of co-operation, I completely agree with you. That's why we had been in touch with you one how important co-operation is even before your attendance today. What specific areas of co-operation do you see? Are there witnesses you think we should hear from that we perhaps haven't heard from? One option would of course be to have AIQ back after we've heard from Christopher Wylie and other potential witnesses. Maybe you could give us some broad strokes on how you think we could co-operate going forward.

Mr. Damian Collins: Just to give you an idea of what we're looking to do next, we want AIQ to come in front of us. We want Alexander Nix to come back in front of us as well. We also want Dominique Cummings to give evidence to the committee about the work of Vote Leave. We're also interested in hearing from Arron Banks and Andy Wigmore of Leave.EU. I think there could be other areas where we have a common interest. I think one of the key things on jurisdictional issues is where the AIQ servers are and where they service data from. Are they in Canada, or are they in the U.K.? I know that the U.K. Information Commissioner is Canadian herself. I know she's obviously seeking to pursue all of this in fine detail.

● (0855)

Mr. Nathaniel Erskine-Smith: Of course, we can continue to co-operate, and since AIQ is a Canadian player we can have them back if they refuse to co-operate with your committee going forward. Certainly, we'd be interested in doing so.

We heard a revelation yesterday that Cambridge Analytica and SCL Group are declaring bankruptcy. Perhaps it comes as no surprise that they're looking for a way out. How does this impact your inquiry, if at all? What steps are you taking in the course of your investigation to deal with that new information?

Mr. Damian Collins: As far as we're concerned, it doesn't change our inquiry at all. I discussed this just this morning with Elizabeth Denham, the Information Commissioner. As far as she's concerned, it doesn't make any difference to her inquiry, either. She's investigating whether civil criminal offences have been committed. She can pursue the directors of these companies even if the companies themselves have been declared insolvent. She can still press charges, issue fines, just as she would have done before. There is an interest in saying that if wrong-doing has occurred, people should be able to go after the wrong-doers and they should face whatever penalties they should face. There's also a public service provided in being able to say in public what happened, what these companies did. Did they breach the law? How it [*Technical Difficulty—Editor*].

Your final question talked about some of the parties we're interested in seeing again who are directly involved in this particular issue, and we are seeking to pursue Facebook as well, as I know you are doing, too. Of course, a lot of these interactions are with Facebook and Facebook data, because Facebook itself is an important repository of information that would be useful to us—if only we could get hold of it.

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

Next up is Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair, and thank you, Mr. Collins, for hooking up with us today.

Just to follow on the last question regarding Cambridge Analytica's declaration of bankruptcy and announcement that it's shutting down, what provisions or protections are in place to prevent the destruction of evidence in your inquiry and the Information Commissioner's inquiry?

Mr. Damian Collins: Well, you are right to say there is that risk, but [*Technical difficulty—Editor*] had already received a warrant and had the power to go into Cambridge Analytica's offices and take their servers and information that was relevant to her inquiry. She holds that. I know they—as we have done as a committee—have received a great deal of information and evidence directly that we can investigate.

I think we are in quite a strong position there, but of course both we and the Information Commissioner, in particular, can follow the data trail wherever it takes us. If that takes her into companies like Emerdata, which is another entity that is effectively connected to SCL and Cambridge Analytica, then she can pursue it there as well. There's no limit to where she can go while following the data and the people connected with it.

I think an interesting issue here—and this is something we discussed with Chris Vickery yesterday—is that we talk about these companies as though they are legal entities and physical companies. What if they're not really that at all? What we're dealing with is massive data and tools to process it and people who do it. They wear different hats and sit in different organizations, but effectively, it's just one thing. In that case, we can still go after the thing, even if the brass plates on the door are changed.

Hon. Peter Kent: Also, following up on your suspicion of the possibility—even probability—that AIQ's files were left open for users to come in to use as they might, but still giving AIQ plausible deniability that they were not engaged in improper or even criminal activity, AIQ's testimony to us also indicated that they had received data, but didn't particularly care where that data came from. They merely massaged it through their different programs like Saga and others.

Have you discovered this as well? Do you see this as an attempted defence of their basically trafficking in improperly acquired or stolen property?

Mr. Damian Collins: Well, I think an area of great concern is where this data is coming from, and obviously, with the Cambridge Analytica data breach and the data acquired through Aleksandr Kogan, we're looking at that directly.

Looking at the transcript of AIQ's evidence to your committee, I think they're very careful in the words they use. They talk about being a whole big dataset and that they don't hold the data. That may be technically true if exists in the cloud somewhere, but they have access to it. They may say, “We don't have big databases of data. We don't keep data”, but they may have access to it, and they can use it.

Certainly the techniques that have been used here seem to be the gathering of multiple datasets, some of it commercial data that can be acquired through companies like Experian, some of it data acquired from Facebook profiles, and some of it voter data and other data—anything you can get your hands on effectively all put into the mix. You get the very sophisticated profiling of individuals crucially linked to their Facebook profile with the ability then to target them directly through Facebook in that way. Not only that, but you can also create a custom audience of those people, and then take that up to Facebook. Facebook will then find you a look-alike audience of people like them that will make your campaign even more widespread and successful.

What's clear is that, once you've built these custom audience datasets, and you've linked them back to Facebook, you don't need the original datasets anymore. These companies can then say—and maybe honestly—that they've given back that data or have destroyed that data. That may be true, but the derivative of that data is something they own in perpetuity, and there's certainly nothing Facebook can do to get that data back.

As you rightly say, there could be all sorts of datasets acquired in there. Our concern would be if that data had been acquired illegally. That's a serious a matter, and we as a parliamentary committee would certainly come to a view on that, but it's right that the UK authorities would seek to bring criminal charges against people who have broken the law.

● (0900)

Hon. Peter Kent: Going back to the source of this evolving scandal, Mr. Kogan, he still denies.... He says he's being scapegoated, that what he did was common practice, that Facebook has endured harvesting—improper harvesting, if you will—by any number of companies. He says that what he did was perfectly legal and within the terms of Facebook service. Now, that's obviously one of many contradictions, denials, deflections, mistruths, and flat-out lies that we have seen through the testimony to our committees.

Is there an element of truth in what Professor Kogan says, that he may well be only a very small part of a much broader misuse of harvested social media data, whether from Facebook or anywhere else?

Mr. Damian Collins: I think that's right. Sandy Parakilas gave evidence to our committee a few weeks ago. He used to work at Facebook and had oversight of their relationships with developers and the way they use data. His concern was that abuse of data was widespread; large amounts of data were being taken from the platform by developers; there was no real scrutiny by Facebook of what they did with it and how they did it. My contention with the Aleksandr Kogan data would be that I think Facebook would never have known about it if it hadn't been for a newspaper article in *The Guardian* in the U.K., which exposed it; and they then followed up on that once they'd been told. I don't think they have any monitoring or auditing of what happens to data acquired by developers.

However, there's another question. Kogan is right to say that, well, the terms and conditions for using the app he created say that he may want to give that data to other people. The question then is why Facebook didn't stop that at the time. Why did they approve it and let him do this? Clearly, Dr. Kogan would have known, and should have known, that to do what he did was a breach of Facebook's rules. I think there's, then, a separate question about the existing U.K. data protection law at the time he did it, which has got quite strong provisions in place to stop people holding political data about people and gathering data to use in political campaigns. I think he should have known that there were certainly serious legal questions about what he was doing.

Hon. Peter Kent: This is a very short question, as my time is almost up.

What is the timeline for your study, your investigation, and do you expect to have any firm, hard conclusions at that outcome? Furthermore, what is the timeline of the Information Commissioner's investigation?

Mr. Damian Collins: In the parliamentary inquiry, we are aiming to report before the summer recess in the U.K., so that is around July 20. That's what we're looking to do. We'll be holding all evidence hearings into June, but then we'll look to bring our findings to a conclusion at that point and produce our first report. As we said, we'll be looking to make concrete conclusions based on what we think happened and based on the evidence we've received. Also, as is normal for select committees in the House of Commons, we'll make policy recommendations to the U.K. government. The government has already given ground on one of the issues we have championed, and that is on additional powers for the Information Commissioner, for her to be able to have no notice period before arriving to take and seize data, so we don't have a repeat of what was a farcical situation where it took her five days to get a warrant to go into Cambridge Analytica. She will have substantially enhanced powers, which will help the conclusion of this investigation and future ones too.

In terms of her work, I believe she's looking to produce a policy report, looking at the general issues of data use in elections, and she's aiming to produce that report by the end of this month. I certainly believe it's her hope that she would have concluded the initial investigations into criminal and civil offences, again, I think probably by July. I know that she's received a lot of new information; therefore, it's possible that it might take longer.

● (0905)

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

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

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

It's a pleasure to have you with our committee today. In my 14 years in Parliament, I've never seen a situation where one of our committees is actually speaking to a committee in the U.K., or in any other jurisdiction, but maybe it is a reflection of the nature of the big data beast that all of us are dealing with, which is very much cross-border and almost beyond the jurisdiction of domestic laws, as they seem to think.

You could probably help us get a better sense of some of the questions that we were left struggling with after AggregateIQ came before us, because they are listed as SCL Canada; Zack Massingham is identified as having the phone for SCL Canada. He says there's no connection between AggregateIQ and SCL. Do you think that's a credible response?

Mr. Damian Collins: The evidence we've received contradicts that. We've been told by Chris Wylie and Brittany Kaiser that, as far as they were concerned, that's what it was. It was SCL Canada, and indeed there are documents that Chris Wylie gave us that show employee lists and directories where SCL Canada is listed. We know there's a huge number of projects that SCL and AIQ worked on together—the staff teams worked together—going back a number of years; and there's a document we published, which Chris Wylie gave us, which is about a project in 2014 done for Ambassador Bolton's super PAC, the campaigns they were supporting in the mid-terms in America that year. Again, there were staff members from SCL, Cambridge Analytica, and AIQ all working on the same projects, including Dr. Kogan as well.

The impression you get is one of a high-level of integration and partnership, and the evidence we had from Chris Vickery, yesterday, looking at these datasets he found on GitLab would, again, suggest that this is an entity of work that is totally integrated.

Mr. Charlie Angus: That's very helpful.

Our concern also, which we couldn't get a clear answer on, was how did this obscure company in Victoria, British Columbia, get every single contract for the leave campaign. That didn't seem credible.

The question is what would be the role of SCL? Can you explain to us how SCL, as the parent company, would have played a role in this and the credibility of AIQ suddenly stepping into the Brexit campaign and getting all those contracts?

Mr. Damian Collins: It's a really interesting question. I thought it was a great question to ask them how they had come to get this contract given that they had no links to the U.K. and were a relatively small company.

There are things we know. Brittany Kaiser told us that there was an initial introduction to Leave.EU—the other campaign, Arron Banks' campaign—to Steve Bannon. They made an introduction through Arron Banks to Cambridge Analytica. Cambridge Analytica were working with Leave.EU from the autumn of 2015 through to the point where Leave.EU didn't get the nomination to be the official campaign. Leave.EU say they never paid Cambridge Analytica for that work they never got, but they had a contractual relationship with them. There are still some questions around that. We know that links between Cambridge Analytica and SCL seemed to continue after the official designation was made. They were involved in supporting Arron Banks' visit to Washington, D.C., before the referendum. There seem to be close links there. Some of the these things are even detailed in Arron Banks' book and he refers to the fact they hired Cambridge Analytica. There seems to be quite a strong relationship there.

With AIQ one of the things we're interested in understanding more about is how the introduction was made of AIQ to Vote Leave when Vote Leave got that official designation. Who was responsible for that introduction? It does seem very strange that you have what, at the time, seemed to be unconnected companies. We know now that the companies, even if they weren't one legal entity, were highly coordinated in the way they worked together and were potentially advising two sides of the same campaign.

● (0910)

Mr. Charlie Angus: That leads me to my next question, because we heard the news that SCL and Cambridge Analytica are closing up shop and how hard it is for them. I'm looking at this new company, Emerdata Limited, which has the same address as SCL. Rebekah Anne Mercer from SCL, Jennifer Mercer from SCL, Julian David Wheatland from SCL, Alexander Tayler, Mr. Nix, are all now working as directors at Emerdata.

Have you looked at any of the role and the work of Emerdata? Is that part of your committee work at all?

Mr. Damian Collins: It's a good question.

We certainly ask questions about Emerdata. As you say, they seem to be completely connected to these other companies. Therefore, if Emerdata is holding information, documents, datasets that are relevant to our inquiry, there's no reason why we couldn't go after that. The same would apply for the Information Commissioner as well. Again, we seem to have a series of entities that are highly interconnected, with the same people, who one would imagine are using some of the tools and information. I've not been there. The office is in Westferry Circus, the one, I think, you're referring to.

I've not been down there but I was told by a journalist in London this morning who has been there that there seems to be no evidence of anyone working at that address at all. Again, the nature of this company, what it is, and what it does, is unclear. But if that company is the legal guardian and owner of data, information, and contracts that are relevant to our inquiry, then it would certainly fall within it.

Mr. Charlie Angus: Thank you.

I received a letter last night from UpGuard. We'll present that letter to the committee today. They are very concerned that this legal decision to shut down Cambridge Analytica could allow them to start erasing and getting rid of data. They're concerned about data that may be on other hosting sites. They're looking to see if there have been any preservation requests for Cambridge Analytica data, or SCL or AggregateIQ, particularly with third-party service providers such as Amazon Web Services.

Have you put any of those data preservation requests in?

Mr. Damian Collins: No. That would probably be for the Information Commissioner to do. I don't know whether she has done that. I did speak to her earlier today and she reassured me that as far as she was concerned, she had all the powers she needed to complete her investigation. I know she has access to and has received a large amount of data, which they are currently working through. You're right to raise these concerns. There may be data that does not yet fall within the scope of the inquiry, and that we don't yet know about or have access to, and that could be destroyed. I don't know if these files are held in the cloud by Amazon as a storage provider or another company. I don't know what the scope is to go back to that company to get the original files if an attempt were made to erase them. That's certainly a question that I will put to the Information Commissioner in the U.K.

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

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

Mr. Raj Saini (Kitchener Centre, Lib.): Hello, Mr. Collins. Thank you very much for being here.

I first want to touch upon some testimony that was given in front of your committee by Mike Schroepfer, the chief technical officer at Facebook. To me it seems that this whole situation began, as you said, with an article in *The Guardian*. Since then Facebook has finally admitted that probably 87 million Facebook profiles were compromised, one million of them in the U.K.

Under questioning regarding the influence on the Brexit referendum, Ms. Elliott said that the campaign was run based on email lists, that it had acquired email lists of people from some source—Mr. Kogan's app. Mr. Schroepfer goes on to say that it could not have been his app, because he didn't acquire an email list. He said that AggregateIQ must have acquired that data from some other source.

Have you investigated what other source that could have been? It seems to me we're all chasing the same data, but the chief technical officer is now saying that it could have been some other data.

Mr. Damian Collins: I think there are a couple of quite important things there.

With regard to the data collected from Dr. Kogan's survey, that would seem to be primarily psychological profiling of people who completed the survey, but then crucially linked to their Facebook profile. I think that's important, because if you then take that data and add it to other datasets they may have acquired, and the email lists that the campaign group itself had acquired, you can then not only merge all those datasets together, but you can also tie it back to the Facebook user profile, which helps you to retarget the individual back through Facebook, where Facebook is effectively acting like a giant telephone exchange, and you're programming the data in, not generically to categories of people, but to named individuals.

Mike Schroepfer was saying that the Kogan datasets wouldn't have included email addresses. That could be right. They could have just found those emails in other ways. But from the evidence that we had yesterday from Chris Vickery, I think it's clear that you can have many different datasets that you process together through your targeting tool and then use that for the basis [*Technical difficulty—Editor*] Facebook.

● (0915)

Mr. Raj Saini: So there is an overlap going on with different datasets?

Mr. Damian Collins: Yes, absolutely.

Mr. Raj Saini: Also, in written testimony, Mike Schroepfer says that they also found “billing and administration connections” between SCL/Cambridge Analytica and AIQ.

Have you done any research into any of these connections?

Mr. Damian Collins: This is one of the issues we want to follow up on with Facebook to see if they can help us.

I wrote to Mark Zuckerberg on Monday with a list of over 40 outstanding questions and issues from the Mike Schroepfer session. That's one of the reasons we want Zuckerberg to come back—there are so many outstanding questions. But this is an important issue.

I know that the Information Commissioner in the U.K. has been in contact with Facebook about her inquiry, but I think this is one of the key issues, not for the Information Commissioner, but for the Electoral Commission and U.K. election law. If there was coordination between different campaigns, that's an issue. And I think we will understand more about the day-to-day coordination between these companies as well.

Mr. Raj Saini: I know that yesterday Mr. Vickery gave you a hard drive. It might be too soon, but have you started the analysis procedure of reviewing what's on the hard drive?

Mr. Damian Collins: We haven't started that process yet. We're putting our apparatus in place to start it. It's a lot of information. I think he said that the compressed files are 19 gigabytes of data, so the whole files will take some time to go through, and we need to get a team of people in place to do that.

I also spoke to the Information Commissioner to let her know that we have this dataset, but as a parliamentary committee, we're keen to go through it ourselves to see what it contains. There may be information that's both relevant to our inquiry and helpful to the Information Commissioner too, but it's going to be quite a task.

Mr. Raj Saini: Are you going to make that information public? Will we have an ability to review the information for the purposes of the work on this committee?

Mr. Damian Collins: Our primary task is to go through the data to see what's there, and then to take advice on what we can publish. There will be things that we want to publish, as a committee, but we want to make sure that in doing so it wouldn't prejudice other investigations that are under way. Although clearly, the people who created this dataset know what's in it, and it was taken down a few days after Chris Vickery discovered it. They will be aware of what it contains.

I need to take advice on it from the U.K. authorities, but we would certainly be very happy to share information. And I think Chris Vickery would also be happy to share it with your committee directly.

Mr. Raj Saini: For my final question, when we look at the number of data profiles accessed by Cambridge Analytica and the worldwide downloads of that survey, it was about 270,000, which led to 87 million profiles being garnered. In Canada, fewer than 300 profiles were accessed, and 621,000 profiles were garnered.

According to Mr. Schroepfer's testimony, he said that 1,040 people had done the survey in the U.K., which led to a million profiles being accessed. To me, mathematically—going on what we heard—that is a very low number.

Is that a number you're confidant with, that one million only?

Mr. Damian Collins: This seems to be just from this app. That's based on the number of people who took the survey, and then an average of the number of friends that people had on Facebook at the time. That multiple gets you to around a million. Of course, there may have been other datasets and sources that were part of the data-gathering exercise as well, and then the targeting exercise that derived from that data.

When Brittany Kaiser gave evidence to us, she said that a good-sized working set of data, if you were going to plan a Facebook campaign, is around 40,000. If you have around 40,000 profiles with good mapping data, understanding who these people are, what motivates them, that's your good working set. Of course, then you can acquire look-alike audiences from Facebook as well, to grow that to help you target a much wider group.

Even if that were the limit of the data they acquired through Dr. Kogan's app, the power of that data is potentially significant.

Kogan also said to us that he didn't think that data, in and of itself, was worth very much, just with the surveying he was doing and the Facebook accounts they were linked to. But, of course, it was never intended to be used in isolation. It was intended to be used as part of a much richer set of data, of which this was going to be an important part.

● (0920)

Mr. Raj Saini: Thank you.

The Chair: Thank you, Mr. Saini.

Next up, for five minutes, is Monsieur Gourde.

[*Translation*]

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

Thank you, Mr. Collins, for taking part in this committee hearing. Your participation is really very important to us. In fact, in this new digital reality, there are many questions and beliefs to elucidate. We are currently experiencing a type of lawless and faithless digital far west.

The company names don't matter much to me. I am more interested in the ways they use our personal data for profiling. In fact I am especially interested in the tactic that involves third party companies in countries where the electoral laws are not the same. We have to deal with that.

Normally, a country's laws control elections well. However, the situation can become problematic if we are dealing with a company in a country where the laws are different. In the current situation, the data are in Facebook, but a company is using Facebook data to do advertising. So they are in two, three, or perhaps even four countries. Even if we legislate in our respective countries, that is Canada, the United Kingdom, the United States and others, those companies can settle in the Cayman Islands or any other tax haven. We have no control on the provenance of the funds or on the amounts spent.

We have to clean all of this up, but in your opinion, where should we start?

[*English*]

Mr. Damian Collins: Well, as you say, it's like the Hydra from Greek mythology, this sort of multi-headed beast. When you cut one head off, another one springs up.

I do think these systems, these companies, have been created to be as difficult to track and follow as possible. If you brought in money and finance there as well.... This is again something we discussed with Chris Vickery yesterday, about the interest these companies seem to have in cryptocurrency. That of course facilitates the movement of money from one place to another, for whatever reason, in a way that's very hard to trace.

I think what we have to try to do, and what we're trying to do with our work, is to strip this back to some basic principles where we know we have jurisdiction. There are laws about the way in which data can be gathered and used in elections. There are laws about the way that referendum campaigns can be funded and around the coordination of different aspects of those campaigns. In terms of data storage and the use of data belonging to the citizens of the country, there are national laws that apply, and national jurisdictions as well.

I think we can go after them. It got us to where that company is based. They are processing data by U.K. citizens. If they are doing so in the U.K. jurisdiction—any data processing—then we have clear jurisdiction there.

As I said at the beginning in response to Mr. Erskine-Smith's question, this is one of the reasons why I think co-operation between our committees and by authorities in different countries is so important. These companies and these investigations cross multiple boundaries. To be successful, I think we need to be as integrated as possible.

[*Translation*]

Mr. Jacques Gourde: If you discover after your investigation that those companies that did profiling did not declare certain funds that were spent during the pre-referendum Brexit campaign, and that those funds may have influenced the results of the vote by a few percentage points, you will probably have some recourse. However, does this call into question the very legitimacy of the referendum results?

● (0925)

[*English*]

Mr. Damian Collins: That's difficult to say. At this moment in time, we need to be able to identify what took place, both the actions of the companies involved and the work of companies such as AIQ in the campaign. The Electoral Commission will determine whether that was done within the rules. We've been seeking to ask questions as well about Russian interference and involvement in elections in the U.K. There has been work done that shows intent and activity from Russia to influence voters in both our last general election and the Brexit referendum. It has been harder to get information of that nature about Facebook, but there's clearly intent there as well.

Those are all really important issues in understanding what's in place. We can then lay it out for people to see. It should inform the way in which we seek to protect our democracy in the future from the interference of bad actors. It's then a debate for our country to say, if we feel and can demonstrate that the level of interference in the referendum was much greater than was previously suspected, does that change people's attitudes or not? The Electoral Commission, of course, can take action against people who committed offences, be it on spending or campaigning, or whatever.

The Chair: Thank you, Mr. Gourde.

Next up is Mr. Baylis for five minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Mr. Collins. I appreciate it very much.

Our concern, obviously, is that we don't want to be part of this international network and have Canadian companies interfering with other jurisdictions' elections. This is very concerning for us. It's also very concerning as we see a pattern flowing out and pointing to Russian interference in a number of elections. I'd like to draw the process as I see it and hear your comments as we go along.

If we start with the Russian government, their second largest oil company, Lukoil, which is presently under U.S. sanctions, has been operating as an arm of the Russian government. We know that Mr. Alekperovis is a former Soviet oil minister. This company somehow has money going to Mr. Aleksandr Kogan. He's the University of Cambridge researcher who has also, to my understanding, received money from the Russian government directly and had discussions with Lukoil.

I'd like to hear your thoughts on this. This person, Aleksandr Kogan, uses the cover of the University of Cambridge to do a little research project. If he were coming out saying, "I'm the Russian government doing a little research project," I'm not so sure many people would have signed up. Do you see Mr. Kogan as a key player?

Mr. Damian Collins: When he gave evidence to our committee, we asked Dr. Kogan questions about his Russian connections. As you say, whilst he was at Cambridge, he also collaborated on a research project at Saint Petersburg University that was funded by the Russian government, and that was into cyberbullying techniques. It wasn't quite—

Mr. Frank Baylis: Yes, but he's being funnelled money from the Russian government. Now, somehow he connects with Mr. Alexander Nix. We've had a number of company names, but we know that Alexander Nix is both the CEO of SCL and Cambridge Analytica. Therefore, let's assume that they are one company.

I know that whenever you seem to ask some questions, he'll say that Cambridge Analytica had nothing to do with Lukoil. However, we know there were links between Lukoil and at least SCL. Is that correct?

Mr. Damian Collins: Yes, that seems to be the case from the information we received, particularly from Chris Wylie.

Mr. Frank Baylis: We can assume, then, that Lukoil is both funding Aleksandr Kogan, with an objective to go and scrape a lot of information, and then discussing at the same time with Alexander Nix, the CEO of both SCL and Cambridge Analytica, how to use that to interfere with elections.

Mr. Damian Collins: Yes. Dr. Kogan's job seems to be data scraping, whether he's doing it for elections or for other commercial work. There is then a question that has been floated by people who gave it to the committee about the significance of Lukoil and the elections work. Is the purpose of the elections work just to get introductions and to develop a relationship with powerful people in certain countries in the hope that commercial work comes later or that big companies will fund other things?

● (0930)

Mr. Frank Baylis: Yes, but it would seem that scraping data from 57 or however many millions of people would not be the business of Lukoil if they were truly just in the oil business. As we know, they are sanctioned for operating as part of the Russian government.

We also know or have proof that the Russians were interfering in the U.S. presidential election of November 8, because Robert Mueller has charged 13 Russians and three Russian entities with purposely interfering in that election. They've been charged in the United States. Before that, we look at Brexit, the same year, but on June 23. This Russian connection has got its hands everywhere and suddenly this little Canadian company called AIQ shows up, whose president or CEO has his cellphone number listed as SCL Canada, and yet has denied knowing anything about it before this committee. Does that make sense?

Mr. Damian Collins: No, it doesn't, and I share your concern. It's been difficult to get straight answers on what SCL Canada is. First it's AIQ, and are they the same thing? They certainly appear to be the same thing—

Mr. Frank Baylis: He had the nerve to tell us that. He found out about this when he read in the paper that his cellphone was listed as SCL.

Mr. Damian Collins: Yes, absolutely, and you'd have to ask, would AIQ have got the work that they did without their relationship with SCL?

Mr. Frank Baylis: Let's talk about that. That's another question, and it brings me to connect the dots of between how Russia, I truly believe, interfered in the U.S. election, as Robert Mueller has found out, and the Brexit vote. It did so purposely by funnelling money to Mr. Aleksandr Kogan in connection with Alexander Nix.

Now, you have a substantial sum of money from VoteLeave. Then you have BeLeave, and we learned that not only did BeLeave not get the money from VoteLeave, but they were contacted—theoretically—independently, and the CEO and COO could not tell us how BeLeave even found out about them. Suddenly they get a phone call and order over a million Canadian dollars' worth of services, and just say someone from VoteLeave will call you up and pay our invoice.

Then you have Veterans for Britain and the Democratic Unionist Party. You have four entities in the Brexit side contracting with this minute little company in Victoria, B.C., and they were unwilling or unable to give us any clarity as to how these people even knew about them, except for the fact that we could find out that the CEO was completely linked with SCL.

Mr. Damian Collins: Yes. That's right. You can see how a link through SCL and Cambridge Analytica can get to these parties in the U.K., and it's hard to see how the Democratic Unionist Party would have decided to pick up the phone to AggregateIQ. It's impossible to see how that could have been the case.

Mr. Frank Baylis: If I could sum it up—

The Chair: Thank you, Mr. Baylis. I'd love to let you keep going, but I would just like to clarify something. We do have the Chair of the U.K. committee for two hours. We're going to try to get to some committee business at the very end, so don't worry, we can get you in.

Thank you.

We'll go up next with Mr. Kent for five minutes.

Hon. Peter Kent: This is a slightly broader question, Mr. Collins. With the GDPR coming into effect now, do those regulations cover some of the matters that your committee is studying, or is it all going forward from today?

Mr. Damian Collins: The GDPR comes into effect on May 25. That's the deadline for the new [*Technical difficulty—Editor*] coming in place. The House of Commons has got the final stages of the bill to implement the GDPR, for instance, next week.

I think it enhances a lot of the data.... A lot of the existing data protection law is already quite helpful for the inquiries that we're pursuing because there are already quite tough restrictions on holding political data about people and who can do it.

I think one of the big questions posed to our inquiry, and why we supported the Information Commissioner's getting these additional powers to support her investigations, is how do we know that a company like Facebook is compliant with GDPR rules? If someone puts in a request to get their data back or to have their data destroyed, how do we know that the request has been complied with? If someone asks for their data back and they want data that's been acquired by Facebook developers, as well, who polices that? The best way we can do that, I think, is to make sure the authorities have got these “no notice” powers just to go in and take data and inspect data where they believe a breach may have occurred. One of the big questions for us when GDPR comes in is, how can we make sure that it's being enforced correctly and that companies are actually doing what they're being asked to do?

● (0935)

Hon. Peter Kent: Will monitoring and enforcement and penalty applications be a result of national parliaments, or will there be an EU super-department that would have that responsibility and would require those resources to monitor?

Mr. Damian Collins: It will be the national authorities who will have the responsibility. The U.K. government policy is to have equivalence in data regulation with the rest of the EU, so even after Brexit we'll be operating on the same rules, but it will be the national authority of the Information Commissioner to enforce those rules.

I think it's also worth mentioning that even though we have European standards for data management through GDPR, there are different requirements in different countries as well, and for different reasons. So Facebook in Germany runs to different rules than Facebook does in the U.K. because it has to comply with German legislation on hate speech, and therefore employs vast numbers of people to take down posts that would be in breach of Germany's data protection laws, and Facebook itself would be penalized if it failed to do that. So even within common European standards, you could still have quite different jurisdictional requirements in different member states.

Hon. Peter Kent: You've cautioned Mr. Zuckerberg that should he come to the U.K., within your jurisdiction, you would in all probability call him. There's a possibility of a subpoena, but in more general terms, will you consider recalling Facebook as your inquiry continues? You're obviously not satisfied with the answers you've received to date.

Mr. Damian Collins: No, that's right, and that's why when I wrote to Mark Zuckerberg on Monday, it wasn't just to formalize the requests and to notify him that we would summon him if he didn't respond but also to set out in writing the questions that remain unanswered from the evidence session we had with Facebook. Some of them are on really serious issues, which we do want answers to.

One of the things we have not talked about so far today is this whole question of dark ads. I asked Mike Schroepfer whether, if someone sets up a Facebook page, and posts dark ads that can only be seen by the people receiving the ads and the person who put them up, and proceeds to put up thousands of these during a campaign, and as soon as the campaign stops, deletes that page and all the content with it, there is any record that it ever existed. He said he didn't know.

If the answer to that question is no, that is really serious. That is a massive breach of our rules, and it gives people massive power to impact what people see during an election campaign. They don't have to declare it and there'd be no record that it ever took place.

Hon. Peter Kent: To Mr. Gourde's question, if the commissioner's findings are that in fact the Brexit vote was stolen, one has the very large question of whether another vote must be held, or could be held. What's the discussion in your parliament about that?

Mr. Damian Collins: Well, I think then people would want to see evidence that that had happened. Ultimately it would be for Parliament to decide whether it wanted another referendum or not. There are people who are calling for that, but that's largely because they just don't like the result of the first one.

I think this would inform a bigger national debate on what to do next, but at the moment I don't think there would be a consensus in favour of a second referendum.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for five minutes is Monsieur Picard.

Mr. Michel Picard (Montarville, Lib.): Merci. I have a very simple question to start. Do you require an MLAT request in order to exchange information based on my colleague's request to have access to the hard drive, or will a simple letter from our chair suffice?

Mr. Damian Collins: I need to take advice from the clerks on that just to see how we can share information and whether we could do that without publishing the material. It may be better for you to request that information directly from Mr. Vickery. He's certainly indicated to us that he'd be willing to share information with you, but perhaps we can continue that discussion after this session.

Mr. Michel Picard: We could.

With respect to your inquiry, apparently companies had access to documents related to Google. Are you aware of any implications for Google?

Mr. Damian Collins: No, we've not had information about Google data, Google information, being used, but we'd certainly be interested in looking at that if there is evidence of it.

Mr. Michel Picard: In a broader approach to the problem, I'll give you an anecdote. In the 1950s in Quebec, there were some priests who said in their speeches that the sky is blue and hell is red. Apparently, they were referring to political parties according to their colour. If this is not fake news, it's at least propaganda.

The issue is freedom of speech. It's not new that we are bombarded with all kinds of fake news and false information. It's a technique used in World War II, and it's been going on for centuries. Although we end up with a situation where my information is used to provide me with all kinds of false information, there's nothing much I can do about it, since anyone can say anything they want. It's for me to believe it or not and make my decision based on my own knowledge.

It might not be moral, it might not be fine to exchange and exploit information in this way, but in the end I cannot do much about it. My problem is not the fact that I'm bombarded with all kinds of false information; my challenge is that I need to find a way to better monitor what people do with my information. Consequently, should I prohibit that and therefore put at risk other companies where the business plan is based on selling information for advertising and so on?

● (0940)

Mr. Damian Collins: There are a number of important points in that. First of all, I would create a distinction between pure fake news and what you might call “hyperpartisan content”. We know, for example, that the Pope didn't endorse Donald Trump. That is clearly someone spreading a known lie, and therefore I put that in a category of bad, harmful content that we want companies like Facebook and Google to act against.

There's then the question of hyperpartisan content, which could be bias or propaganda, as you say. The question is, do people understand why they're receiving it, and can they do anything about receiving it? These problems seem to have gotten worse since Facebook allowed advertising through the newsfeed. You can advertise straight into the newsfeed. I asked Mike Schroepfer this: If you didn't want to receive political ads, can you stop them? The answer is no. You can be targeted with political messaging, and there's nothing you can do to not receive it. You could receive many of these political messages that have been targeted at you based on psychological profiling that's been done—unbeknownst to you—of your interests, fears, and concerns, and you can't stop receiving them.

You may also not know who is sending them to you. What's been exposed in the Internet Research Agency's work is that what you thought could be a community group concerned about an issue you're concerned about is actually someone in St. Petersburg targeting you with propaganda, and you have no way of knowing.

There are questions there about how people can turn off political advertising for the newsfeed if they don't want to receive it, which is a policy issue for Facebook, but also to have more transparency over who is sending you information. If someone in my constituency in the election period got a leaflet from me through the door and they weren't a Conservative voter, they would weigh up what I'd said against the fact that I'm a Conservative. They would consider whether or not to believe it, because they would know that I have a biased political opinion because I'm a politician representing a political party. They could make that judgment based on knowledge. You can't do the same thing with this message on Facebook, because you don't know who is sending it to you.

Also, I don't think enough people understand why they see what they see. They see more of the content they engage with, so what they're seeing doesn't reflect a broad sweep of opinion; they're seeing only the opinions of the people they most agree with, and that's continually reinforced.

The Chair: Thank you, Mr. Picard.

Next up for three minutes is Mr. Angus.

Mr. Charlie Angus: Thank you.

When Facebook came to our committee, I was very surprised that for a corporation this big, we couldn't get straight answers from them either. They became aware of the effect of that Kogan app three years ago, but they proudly announced to us that three weeks ago they told Canadians that their data had been breached. That's a violation of Canadian law. They must have known it was a violation of Canadian law, yet it seemed that Facebook didn't seem to think they were bound by Canadian law until this scandal came to international attention.

In your discussions with Facebook at committee, how have you felt they've seen their role in terms of their obligations to European law, U.K. law, and domestic law?

● (0945)

Mr. Damian Collins: I think it's been a frustrating process dealing with Facebook. When we started our inquiry, we asked them for evidence of Russian interference in the referendum, and they refused to look. They said that unless we could find evidence that there had been, they wouldn't look to check for themselves. The frustration we've had is that if the Facebook ad-checking team allowed ads to be bought using foreign currency from a foreign country in elections in breach of election law—in America certainly, and to a very small extent that happened in the U.K. as well—why weren't they looking there too?

As you rightly say, there was no disclosure to the Information Commissioner in the U.K. of a data breach involving potentially up to a million U.K. citizens. If it hadn't been for the *Guardian* article, I don't think Facebook would have asked any questions themselves about this. All they did then was write to the people concerned and ask them to delete the data. They didn't notify the users who had been affected. Chris Wylie said that even when they were made aware of this, he wasn't contacted by Facebook for six to nine months asking if he'd still got the data and whether he should delete it. When they became aware of the fact that Cambridge Analytica was working on Ted Cruz's campaign and the Trump campaign, and yet they'd potentially have access to this dataset they shouldn't have had, there seems to have been no checking or double-checking to see whether or not they'd actually destroyed the data.

You see a pattern of behaviour that I think looks like a company seeking to turn a blind eye rather than get to the bottom of it.

Mr. Charlie Angus: Well, this is, I think, really concerning. Sandy Parakilas spoke to your committee. I raised some of Sandy Parakilas's concerns with Facebook Canada, and we didn't get a clear answer. He was really concerned about a growing black market in Facebook data, that black market could be used by terror gangs, corrupt people. I mean, the fact that the Kogan app has potentially had such a massive impact means that other breaches could be very serious.

Parakilas said that Facebook told him they didn't want to be looking into this because, he said, “Facebook was in a stronger legal position if it didn’t know” that the abuse was happening. Is that your experience in dealing with Facebook's response to the Kogan breach?

Mr. Damian Collins: Just to give a bit of background on the Kogan breach and Facebook, we took evidence in Washington from Facebook in February. We asked them about whether there had been data breaches, whether Cambridge Analytica had acquired large amounts of Facebook user data, and when there'd last been a breach. We didn't get answers on any of those issues. The company knew about this issue at the time. It didn't disclose it to us. They're not able to explain now why that was the case. With Mike Schroepfer, we asked about that at length when he gave evidence to us last week.

We find all of that deeply concerning, because I think what would have been an honest answer to those questions would have been to say, “Yes, we are aware of breaches by developers. This is what happened. This is the action we took. This is what we do to satisfy ourselves that this has been contained.”

Mark Zuckerberg was asked in Congress about other developers doing similar things. We asked Mike Schroepfer about this last week. There are still no answers from Facebook about that. I think the concern we share is that if it was so easy for Dr. Kogan to do this work, probably lots of other people could have done it too. And who else did it? Did Dr. Kogan work with other people? Did other people share those techniques? Was this practice quite widespread?

It wouldn't at all surprise me, in that regard, that there could be a black market in this sort of user data. I have not seen evidence of it yet myself, but if people like Sandy Parakalis are telling us that a huge amount of data was taken and no one knows what happened to it, then it wouldn't be at all surprising if it were being traded in that way.

The Chair: Thank you, Mr. Angus.

Mr. Collins, we did ask you originally if there was some information that we would need to go in camera for. I have talked to both vice-chairs on the committee. We still want to hold it in public, if that's possible.

Are you okay with that, or would you prefer to go in camera?

Mr. Damian Collins: No, that's fine by me. If at the end there are any issues you want to discuss in camera, I'd be happy to do that as well.

The Chair: Okay. Perfect. We'll continue on, then.

Mr. Baylis, you have seven minutes.

Mr. Frank Baylis: Thank you, Chair.

Thank you, Mr. Collins. I'd like to continue along the line of questioning we were doing before.

First, who was in charge of Leave.EU?

Mr. Damian Collins: That campaign was led by Nigel Farage and supported by Arron Banks, a businessman. Andy Wigmore was the communications director of Leave.EU. There were competing forces in the U.K. seeking to get the nomination for or to be the official designated “no” campaign.

I believe the reason there ended up being these two entities is that Vote Leave seemed to be led by Euro-skeptic politicians in the Conservative Party and the Labour Party, and—

● (0950)

Mr. Frank Baylis: Who was Vote Leave led by?

Mr. Damian Collins: Dominic Cummings was sort of the communications director, but the leading political figures in Vote Leave were Euro-sceptic members of the Conservative party and the Labour party. Boris Johnson and Michael Gove were the political figureheads of Vote Leave when the referendum was called, but the executive leadership, as it were, came from people like Matthew Elliott and Dominic Cummings.

Mr. Frank Baylis: There are a number of names and different groups, but I really think there are three entities here. There are the Russians. There is the Brexit vote—call it Vote Leave, BeLeave, Leave.EU, Veterans for Britain, or DUP. Then you have a group called SCL, and you have Cambridge Analytica and AggregateIQ. So there are three groups.

It's my understanding that Leave.EU began the discussions with SCL and Cambridge Analytica before they won. They had already set in place a series of motions. Is it correct that they had begun these discussions?

Mr. Damian Collins: Yes, and they were more than discussions. We were taught by Brittany Kaiser that Steve Bannon introduced Cambridge Analytica to Arron Banks. That was the connection there. They worked up detailed plans about how Cambridge Analytica would run the referendum campaign for Leave.EU if they got a nomination.

Mr. Frank Baylis: So Leave.EU starts this process, a quite detailed process, to use this company. I'll call it SCL, Cambridge, or AggregateIQ. It's one company. We can say that.

They start this discussion, but Nigel Farage loses out on the official designation, and it drops to Vote Leave.

Suddenly, Vote Leave shows up at SCL, Cambridge Analytica, AggregateIQ—this one company—to request exactly the same services that have been put in place by Leave.EU. Is that correct?

Mr. Damian Collins: Yes, that's correct.

Mr. Frank Baylis: So it would be fair for me to say that Leave.EU and Vote Leave were completely coordinated in using this company to do their dirty work.

Mr. Damian Collins: Well, there you have an area of dispute, a quite violent dispute, between Leave.EU and Vote Leave, who have both been adamant in saying that there was no coordination between them. Indeed, Arron Banks and Dominic Cummings in particular are often trading blows on social media—

Mr. Frank Baylis: I'm sure they are because to my understanding, if they were coordinating, they would have broken UK law.

Mr. Damian Collins: That would be correct.

Mr. Frank Baylis: There are a series of potential, how should I say, coincidences that belie logic and are not reasonable.

We know that Leave.EU starts this process, and they get heavily into it, but they don't get the money. The money goes to Vote Leave, and suddenly, Vote Leave continues the exact same process. They can be in violent disagreement of how it happened, but we do know this has happened.

Then, they off-shore it to a small Canadian company, AggregateIQ, whose CEO was also listed as the CEO of SCL Canada, so it's the same company. Cambridge Analytica is between them, but it's the same company.

They start doing work for Vote Leave. They start doing work nominally for BeLeave, but paid for by Vote Leave, and they don't even deny that anymore. Veterans for Britain shows up; DUP shows up, all for this unknown, small Canadian company offering nothing of unique value. We asked them very clearly whether there was some special skill that would bring them across the ocean to the far end of our country. They said there was nothing special.

That one group is coordinated, and it is my belief that you have to ask a lot of questions to see how your laws were broken, but they were broken. For this group to say they didn't know, and for them to put on a public display of being at odds with each other, is nonsensical because the facts are that they showed up at the same place to request the same services, and they off-shored things. They paid for these services, though, which means to me that you laws were broken—at least in the U.K.

The same thing is true now with the Russians showing up. The Russian government's former oil minister, who's now running Lukoil, is supporting Aleksandr Kogan, and he goes in and scrapes all this data off.

The question I'd like to ask is how did Aleksandr Kogan connect with Alexander Nix, the CEO of this organization? How did the researcher who stole this data...? He he had no right to do it, but let's say what he did: He stole this data. Suddenly, it's handed over to this company that's operating for Vote Leave, BeLeave, Leave.EU, all of these; it's operating for them. Do you know how those two connected?

● (0955)

Mr. Damian Collins: My understanding of that based on Chris Wylie's testimony to us, and also Dr. Kogan's written statement, which we published on our committee's site, is that Cambridge Analytica was working with academics at Cambridge University and through the Psychometrics Centre at the University of Cambridge. That was how the connection to Dr. Kogan was made. He was working there. He was someone they took an interest in. They started working on projects together. Dr. Kogan's company, though, was set up, it would seem, specifically to work on projects with Cambridge Analytica.

I think to your earlier statement as well, we also are interested in pursuing this exact line of questioning. That's why we want to get in Dominic Cummings, Arron Banks, and Andy Wigmore. We're interested in talking to them, too, about these issues to understand the points you have raised about how these relationships started.

Mr. Frank Baylis: Yes. I think you would be well served to start looking at them as one group. They are going to deny that because, if I understand their denials so far, they have not broken the law. The coincidences are beyond just coincidences. They are actively coordinating. The same is true for SCL, Cambridge Analytica, AIQ, or SCL Canada; they are all one organization.

Thank you.

The Chair: Thank you, Mr. Baylis.

Next up is Mr. Gourde, for seven minutes.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

Among the people I know, there are some survey analysts. They are seasoned analysts, people who have experience and are retired. They tell me that Canadian attitudes seem to have changed over the past ten years. In the beginning of the 2000s and until 2010, they could predict people's voting intentions during electoral campaigns relatively reliably. Things changed slowly, that is to say less than 0.25% per day and sometimes they only moved by 0.1 or 0.2% a day.

These analysts now say, however, that since 2011, things fluctuate very quickly. Sometimes, over four or five days, you can see voting intentions change by 0.5% to 0.7% or even 1%. They tell me that that is no doubt due to the quick circulation of information today, and perhaps even to the impact of fake news, especially during the last 10 days of an election campaign, when there is no time left to react to fake news that may have an impact. The authors of that fake news probably target the undecided vote, and since things are circulated on Facebook, this reaches the entire population. Those who have made up their minds probably pay no attention. However, those who have not yet made a decision will pay particular attention to the most recent news sent by a political party or a third party discussing a position or an issue that could influence their voting intentions.

Historically, the media have been somewhat ethical in their treatment of fake news and did not publish it. Traditional media such as newspapers, television and radio generally did not publish or broadcast news they had not checked. However, on Facebook, it is impossible to check the information and it is possible to put out just about any news about anyone. During an election campaign, those rumours find their way around.

Do you think it is possible to find a way of regulating this more quickly a few days before an election, if we notice that a piece of fake news may impact voters' intentions?

[*English*]

Mr. Damian Collins: This is obviously something that people are thinking about at this moment in time. Should we say there is a liability for the big tech platforms to act against known sources of fake news and disinformation, particularly during election periods?

We know that Facebook track their users activity, not just on the site, but on other sites too. I think they have the capability to identify people who are potential sources of fake news and disinformation, and to bar them from the site or to disrupt what they are doing. I think that would be an important step for us to take.

In France, they are discussing having a judge 24-7 that you can go to during an election who will give a ruling on whether something is fake news or not, and whether it should be taken down or not. We could, of course, go the German route, which they use for hate speech, in particular, where there could be heavy fines for organizations involved in the dissemination of disinformation.

I think this is going to be an increasingly important debate. In western countries I think we have been late to the party on this. If you talk to people in eastern European countries and the Baltic states and Ukraine, this has been an issue they have been dealing with for many years—and certainly Russian interference in their politics through disinformation.

We know with the new technologies and the power of augmented reality to create videos of your giving a speech that you have never given in a place that you have never been to, people are going to need trusted new sources. Also, we're going to need to do more, I think, to make it clear to people the trusted sources, the ones that don't have a reputation for spreading disinformation, and to identify and call up those that do.

● (1000)

[*Translation*]

Mr. Jacques Gourde: Thank you very much. Please know that you have the backing and full co-operation of all parties here in Canada if we can assist the United Kingdom. Perhaps we could innovate and develop a common approach or joint legislation to deal with this problem, and may even inspire other countries to follow suit.

I thank you very much.

[*English*]

Mr. Damian Collins: Thank you.

The Chair: Next up, for seven minutes, Mr. Angus.

Mr. Charlie Angus: Thank you very much.

UpGuard, in their analysis of the AIQ datasets, said that AIQ used Amazon web servers.

Have your officials looked into any possible use by Cambridge Analytica or Aggregate of third-party service providers such as Amazon web servers, where maybe unexamined information may still exist?

Mr. Damian Collins: That's not something we've done as a committee. I don't know whether the Information Commissioner has done that either and whether she has made a request of Amazon.

I think you're right to suggest that the third-party hosting platform companies may well be holding important data that could be relevant to those inquiries.

Mr. Charlie Angus: Yes.

UpGuard had identified GitHub, Amazon Web Services, and also Facebook as maybe having relevant data that may need to be be gathered, caught, and preserved in order to be able to find out what's going on, particularly with SCL closing up shop.

Would you have the powers within your committee to order access to that data, or do you go through your privacy commissioner?

Mr. Damian Collins: It depends. We got the GitHub and GitLab data from Chris Vickery. If we want to go in camera at the end of the session, I could probably tell you a little more about the discussion we had with Chris Vickery about that.

We can order papers, documents, records to be supplied to us within the jurisdiction of the U.K. The issue we would have would be seeking to order the production of materials that are being hosted outside the U.K.

The Information Commissioner is probably better placed to do that, as she has the power to work with other law enforcement agencies in other territories, and to work through them in the normal way. I know that the Information Commissioner has been discussing requests for information with Facebook. I don't know whether they've had this conversation with Amazon as well.

Mr. Charlie Angus: One of the things that was surprising was to read in Chris Wylie's comments and testimony about SCL his claim that his predecessor had been killed in, I think, Kenya. He said that people are afraid and intimidated. He said that they work internationally on some very suspect campaigns in order to influence governments and that that's where the real money was.

We found Mr. Massingham to be very reluctant to say anything. Do you think there is any credibility in Mr. Wylie's claims about SCL, that people are afraid of them?

Mr. Damian Collins: Well, I can understand that.

When we spoke with Brittany Kaiser about SCL's work in Nigeria, for example.... Now we know from information that Chris Wylie provided to us that there were very violent films made for that campaign. They seem to have employed a group of consultants to work on the ground who were ex-secret service agents from Israel. We don't know, and no one seems to know very much about, their background or what they were doing, but certainly looking at some of the materials from that campaign, it looked particularly unpleasant.

This is an area that, whilst it gets away from the core bit of our inquiry, I think there are lots of concern that have been raised about the ethics of the work that was being done. Indeed with Cambridge Analytica, Alexander Nix, and the investigation done by *Channel 4 News* in the U.K., the undercover filming where they were talking about hiring sex workers to compromise politicians in different countries to try to influence the results of an election campaign, says a lot about the ethics and practices of a company like that.

● (1005)

Mr. Charlie Angus: Well I'm looking at this Emerdata spreadsheet of their corporate structure, and you say that apparently nobody is at the address. Almost all the SCL main directors are now at Emerdata.

Johnson Chun Shun Ko, who is also a director, is apparently tied with companies connected to the Chinese government, and is also a business partner with Erik Prince, who is well known for international mercenary work.

What do you think the potential is for maintaining quaint little things like democratic elections in our countries when we have very, very powerful companies that are starting to move into this data control? We saw it with SCL; we saw the effects in Brexit. If we see these new companies being formed with connections, whether to the Russians or the Chinese state, or to international mercenaries, what do we have to do to ensure the integrity of our domestic electoral systems?

Mr. Damian Collins: I think we have to recognize this for what it is, which is a new kind of threat.

My concern sometimes is that the work our governments do looking at cybersecurity is to defend institutions and infrastructure from direct cyber-attack. Have we been looking for this more subtle approach of undermining democracy and public confidence in institutions through, not a direct cyber-attack, but by using data information to try to influence the outcome of elections?

There could be different motivations for people doing that. Is the motivation of the company doing that—using, as we've been told, what would be considered weapons-grade information warfare in other countries and our own country—just to make money, or is it about political influence?

For the Russian state, it seems that their modus operandi is to create discord, to turn communities against each other. They may not necessarily have a direct political interest in the outcome, but they want to create as much disruption as possible to undermine people's confidence in democracy.

It could be that these actors may have common but separate interests. I think they've recognized that you can use these tools, particularly on social media, to support these campaigns and also to polarize political debate and opinion. The consequence of that has been, in many countries, particularly in Europe, the collapse of the centre in politics, people pushed increasingly to the margins, and political debate and discourse being increasingly aggressive. I think we have to recognize this as a major threat to democracy.

Mr. Charlie Angus: Thank you.

Finally, if you've read the transcripts of our testimony with Mr. Massingham, I would say that in my 14 years here, I've never seen someone refuse to treat our parliamentary committees with respect and give straight answers.

Do you think it would be worth our while to invite Mr. Massingham back to answer some more questions?

Mr. Damian Collins: Yes, I do. We're in a similar position with Alexander Nix. We want him to come back, because we believe there are serious questions about the honesty of his testimony to the committee, and we want to challenge him on that.

I watched the session that you had with AIQ. Obviously, my dark concern there was with the answers they gave about their co-operation with the Information Commissioner. I think they were completely disingenuous. It's quite clear from the Information Commissioner that they may have responded to letters, but they're not co-operating with her investigation, and are still not. I think it was misleading of them to try to insinuate to your committee that they were.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

Next up is Mr. Erskine-Smith for seven minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much.

While we're on the topic of information commissioners, your information commissioner has significant powers. Ours has very modest powers when it comes to compelling testimony and the production of documents, and certainly can't issue fines or make orders in the same way.

How important do you think it is for an information commissioner in the modern age to have significant new powers to address some of the concerns we've seen with Cambridge Analytica, Facebook, and SCL?

● (1010)

Mr. Damian Collins: I think it's really important that that they have the ability, not just to request documents and information, but to go and take them if the company refuses to provide them. The powers to fine should be significant.

I think we should also discuss whether it should go beyond that, as well. If you're a very wealthy individual like Robert Mercer, you might think that, if the only risk in certain countries is that someone might get a minor fine for a breach in data protection law, you are happy to pay those fines. You will price that into the cost of doing work. Very wealthy people can afford to take those risks. Therefore, it's right that, in national territories, our agencies have the power to find the truth, get the information, know what's going on, and then have the powers to take significant action against companies who are in breach of the law.

Mr. Nathaniel Erskine-Smith: A number of my colleagues have asked about Brexit.

I found it incredibly interesting that Mr. Massingham indicated that he knew at the time that, had the £625,000 come from Vote Leave on behalf of Vote Leave, there would have been an election finance violation at that time.

Did you know that beforehand?

Mr. Damian Collins: If that had been paid by Vote Leave?

Yes, that—

Mr. Nathaniel Erskine-Smith: Yes, there was knowledge amongst the players at the time that, had this happened—paid by Vote Leave as Vote Leave—there would have been an election finance law violation.

I didn't know that we would get an answer from AIQ, that they would confirm they were aware of that at the time.

Mr. Damian Collins: I was surprised by that, too. I thought it was one of the most interesting and significant moments in that testimony. To me, it seems to be a pretty clear violation.

Mr. Nathaniel Erskine-Smith: We've touched on this a little bit. When it comes to a referendum like Brexit, and it's such a close but significant outcome for the country, and if there have been election finance violations that have had an impact on the outcome, it seems to me there would be strong grounds for that referendum to be set aside based on the unwritten principles of your constitution.

What do you think about that?

Mr. Damian Collins: At this moment in time, I think people need to see it laid out in front of them. They need to see the proof and the evidence of what took place, the scale of it, and how many people that may have impacted upon directly. That would then inform a debate about what we should do about it, and the consequences that are clearly greater than just taking action against individuals for breaking the law.

Mr. Nathaniel Erskine-Smith: Of course.

When it comes to co-operation with AIQ, you mentioned that AIQ continues to refuse to co-operate with your Information Commissioner. They've indicated some willingness to attend before your committee, but nothing is confirmed. Given just timing, I mean AIQ is the Canadian player over which we have jurisdiction. You've heard from witnesses who certainly are going to refuse to attend before us, from Kogan to Nix, and hopefully, you get Zuckerberg, but I'm not sure. However, AIQ is the company under our jurisdiction. Do you think it's imperative in terms of timing; at what point should we have them back in your view; and is there anything else we can do to further your investigation, given the timeline where you say you want to conclude this before the summer recess?

Mr. Damian Collins: I think you've got strong grounds to call AIQ back in your own right, obviously, because of the concerns about the testimony they gave. I had hoped we would be able to agree to hear them very soon. I hope that we'd be in a position to announce that next week and they would give evidence to us before the end of this month. That's certainly something we'd like to see happen.

Certainly we're in a position when interviewing witnesses who may not otherwise be able to come to your committee, and there are questions or issues you'd like us to cover off on your behalf, to do so. We'd certainly be very happy to do that.

Mr. Nathaniel Erskine-Smith: Okay. I would appreciate that.

When we had Mr. Vickery before us, he indicated that when he had reviewed the dataset, it was likely that this overlapping and sort of master dataset comprised election lists. He even suggested it had some commercial information from the Koch brothers. He suggested it had the information from Cambridge Analytica and the Facebook breach, and potentially others. He said that this information had certainly been used for election purposes, but he also said it might have been used for commercial purposes as well. I wonder if you have gone down this road in your inquiry. Do you know more than we do whether such information has been used for commercial purposes?

Mr. Damian Collins: We know that he said there were links in the dataset to advertising networks that would therefore be engaged in commercial work. The way he describes the way the dataset is collected, it would certainly have that application. You effectively have a store of information about people that's linked to their profiles. You can add other information to that, which may be more specific to political campaigns, but that information is still going to be very useful for commercial campaigns as well. Also, he sees these datasets as kind of almost living organisms to which you're constantly adding new data information, and you can just call up information and create new datasets and new audience groups out of this market set, whenever you want.

● (1015)

Mr. Nathaniel Erskine-Smith: Yes, and the idea that you would collect information for political purposes and use it for commercial purposes is certainly against our law, and I expect against your law as well.

Mr. Damian Collins: Indeed.

Mr. Nathaniel Erskine-Smith: When it comes to transparency rules in targeting and advertising, and you mentioned this a few times, when it comes to co-operation, certainly we can co-operate on the inquiry itself in terms of getting at the right questions for the right players, and if we've got jurisdiction over certain individuals, we can assist in your inquiry. However, when it comes to the outcomes and the recommendations, do you think there is value in having consistency in rules across jurisdictions, especially when it comes to the transparency of advertising in elections?

Mr. Damian Collins: Yes, I do. There obviously will be different countries that have different rules in place, but I certainly think that rules on transparency would be much effective if they could be enforced across the board. I think there are the same or similar rules in all countries relating to how they use services like Facebook. I see no reason why that shouldn't be the case.

You brought up the case of Germany. That is quite a good example because there may be very specific national reasons why certain rules are in place, and those conditions may not apply in the same way in other countries. But I think some of these basic points about transparency should apply globally.

It's my concern as well about whether there should be political advertising in the newsfeed or on Facebook, or if there is, whether people should have the right to turn it off. I think it's an important point, and that's really about the way the platform works as a whole rather than individual countries.

Mr. Nathaniel Erskine-Smith: I appreciate that, and I look forward to co-operating as we go forward.

Mr. Damian Collins: Absolutely. Thank you.

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

Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

I just have one last question going to the point of Facebook's acknowledgement of having allowed serious privacy breaches. Here I'm referring to Mr. Zuckerberg's apology before congressional committees. When Facebook executives appeared before our committee, they assured us that thousands of employees monitored Facebook looking for disinformation and fake news, and that many thousands more would be hired to address the realities that have been discovered through the Cambridge Analytica scandal, AIQ, and so forth.

However, we reminded Facebook that some Russian disinformation posted a year ago, regarding Canadian troops participating in NATO Operation Reassurance in the Baltic countries was ridiculous. One of the postings suggested to Latvians that Canadian troops would be encouraging homosexuality in the Latvian population. Another said that our Muslim defence minister would be leading a Muslim takeover of Latvia. When I offered to the Canadian CEO of Facebook that those postings were still up and very open and known to folks in Latvia as well to Canadians who might be following Latvian affairs, he expressed surprise and asked for the link to assist Facebook in taking it down.

Have any similar occasions of glaring disinformation come before your committee during your inquiry?

Mr. Damian Collins: I think we have a similar area of concern, which is that when complaints are made to Facebook about content on their site that is misleading or wrong or that might be harmful, the company doesn't always take it down at all, or quickly enough. That would suggest to me that they don't have the resources in place to do that effectively. That is clearly a ground for concern for the future.

I think, as well, that they should not only act more quickly on user referral but also use the tools they have to try to identify for themselves whether content is likely to be problematic or open to challenge, and then investigate it themselves and take it down. We know they can track what users do on and off the site and whom they are engaging with and what they are doing. They do that, they say, for security reasons. I think they could use those techniques to identify the sources of disinformation.

When they are talking about news and fake news, I think they are right about having more transparency over who has posted this information, where they are based, who they are. With political advertising, you have to do that from a page where you verify your location and your identity as part of setting up that page to place ads. I think they are looking to change some of their policies in a way that would be helpful.

But for me this is where you then come back to the question about liability. If we say "We want you to act in this way", and you don't do it, is there a liability in law that can be enforced against them for not doing it?

● (1020)

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Mr. Saini, you have five minutes.

Mr. Raj Saini: Mr. Collins, I want to ask two questions. Specifically, can you comment on why Andy Wigmore of Leave.EU would refer to AIQ as SCL Canada in an interview with Emma Briant, if they weren't referring to themselves in that manner?

Mr. Damian Collins: What you've rightly discovered and highlighted is that this is what the people who worked in this company thought AIQ was. It's not just the view of one person who might have got it wrong; this seems to be a consistent view about what this entity is.

Mr. Raj Saini: I just want to paint a broader picture so you can help the committee understand the effect of this issue on the Brexit campaign. You had a very close election result: 51.9% versus 48.1%, or a less than a 4% difference. It was 3.8%, to be exact. You had 30 million people who cast a vote, so that just happens to be about one million people. You've come out now and said that you're trying to conclude your investigation by July, right?

Since article 50 was triggered a year and a half ago, the departure of the U.K. from the EU will happen at 11 p.m., U.K. time, on Friday, March 29, 2019. That's a little less than a year away. You've had a run-up to that date by companies, corporations, and organizations that are divesting themselves, making manoeuvres, and readjusting their alignment. You have U.K. citizens who live in other parts of the EU, who are also thinking about where they're going to fit within the new relationship.

Your investigation is going to conclude in July. Whatever your recommendations will be, there will probably be further investigations. If it is determined that the Brexit result was compromised, isn't it effectively too late? The momentum, the shift, the resources, the negotiations, everything is working towards this date. With all the energy that's being consumed right now for that date, isn't it effectively too late for this inquiry's conclusions?

Mr. Damian Collins: To be clear, we have looked at issues connected with the referendum because they have been relevant to our inquiry, but we're not investigating the referendum itself. The Electoral Commission is investigating these issues, and the Electoral Commission will be the body that will determine whether it believes laws were broken and, indeed, will recommend what should be done next. In the past, they've imposed fines. People have gone to prison for their breaches of election law. However, that's a matter for the Electoral Commission to determine.

All we can do is to pursue our investigation and lay out the evidence that we've uncovered. Ultimately it will be for Parliament to determine if it feels that there should be a reconsideration of the referendum itself and whether that should be rerun. That would be a decision for Parliament to make.

Mr. Raj Saini: Thank you very much.

The Chair: Thank you, Mr. Saini.

Last up, Mr. Angus has a letter that he would like to present.

Mr. Charlie Angus: I received this letter last night at 11 o'clock, and I haven't had a chance to get it translated into our two official languages. It's very clear to me that we do not present documents unless they're in both official languages, but I would like to present it to the committee so that it can be shared. It was written to Chair Zimmer and Vice-Chair Erskine-Smith, as well as me, from Mike Baukes, co-CEO of UpGuard in Mountain View, California, as well as Greg Pollock, and Jon Hendren, their director of strategy.

I'm not going to read the whole letter, but there are key elements to put on the record, especially as Mr. Collins is here. It says:

> We at UpGuard are reaching out to you, honorable chair and vice chairs of the Standing Committee on Access to Information, Privacy, and Ethics, regarding an important matter of privacy and data integrity affecting not just Canadian citizens, but individuals around the world. The issue of preserving any and all relevant data stored by companies AggregateIQ, Cambridge Analytica, and SCL on the systems of external services, including but not limited to Github, and Amazon Web Services, is a matter of great urgency and public significance.

It goes on to say:

> The news today that Cambridge Analytica and SCL are being dissolved raises a serious concern: is there more data out there, hosted using services such as AWS, that is relevant to inquiries in the US, UK, and Canada into all three companies?
>
> We write to you in the hopes that public servants might immediately put forward data preservation requests to GitHub, Amazon Web Services, Facebook, and other relevant data services, to freeze and preserve the data in any accounts used by AggregateIQ, Cambridge Analytica, and SCL.

It continues:

> We hope these data preservation requests would be made public, as ultimately the directors for all of these companies should be held accountable. We fear that if the proverbial paper trail is wiped, important information could be lost of interest to the relevant international inquiries.
>
> The risk is that one cluster of companies have the keys to all of this data, yet turns a blind eye to all of the egregious uses of their platform without governance nor controls in place for transparency or oversight into their operations. It would compound the potential issues under investigation were this data to now disappear with the dissolution of Cambridge Analytica and SCL

They've listed a series of questions they're asking us to consider, and they would be eager to discuss this matter with any Canadian or international officials.

I will present the letter to the committee, and we can have it properly translated so that everyone has a copy.

● (1025)

The Chair: Okay. Thank you, Mr. Angus.

I would like to ask you, Mr. Collins, to stay on the line to go in camera with us for a few minutes. You had mentioned that you wanted to say a few things in camera.

I want to thank you publicly for appearing before us. It's deeply troubling. The foremost concern to me is our allowing foreign money to influence our elections, with viewers not knowingly being a part of that. That's deeply concerning. Enabling those bad actors to influence our democracy is troubling to all of us here at our committee.

I want to suspend for about five minutes until we clear the room.

Please stay on the line, Mr. Collins.

[*Proceedings continue in camera*]