HOUSE OF COMMONS

Digital, Culture, Media and Sport International Grand Committee

Oral evidence: Disinformation and 'fake news', HC 363

Tuesday 27 November 2018

Ordered by the House of Commons to be published on 27 November 2018.

Watch the meeting

Members present: Damian Collins (Chair); Clive Efford; Julie Elliott; Paul Farrelly; Julian Knight; Ian C. Lucas; Brendan O'Hara; Rebecca Pow; Jo Stevens; Giles Watling.

Members from overseas Parliaments present: Leopoldo Moreau (Argentina), Alessandro Molon (Brazil), Bob Zimmer (Canada), Nathaniel Erskine-Smith (Canada), Charlie Angus (Canada), Catherine Morin-Desailly (France), Eamon Ryan (Republic of Ireland), Pritam Singh (Singapore), Edwin Tong (Singapore), and Sun Xueling (Singapore).

Questions 4274 - 4382

Witnesses

I: Elizabeth Denham, Information Commissioner, Information Commissioner's Office, and Steve Wood, Deputy Commissioner (policy), Information Commissioner's Office.

II: Ashkan Soltani, tech expert.

Written evidence from witnesses:

– Elizabeth Denham, Information Commissioner

Examination of witnesses

Witnesses: Elizabeth Denham and Steve Wood.

Chair: Good afternoon. Thank you to Elizabeth Denham and Steve Wood for joining us from the Information Commissioner's office. Elizabeth, I know you have given evidence to our Committee and the Canadian Committee before. This is probably the first time that you have done so in the same room at the same time, but hopefully we can make good use of that. I know that colleagues have questions both about your work here in the UK and your recent report to the Committee and to the House, and our colleagues from Canada and Singapore have questions for you as well.

Q4274 **Ian C. Lucas:** Hello again. When we last spoke, we had a conversation about when a data breach happens, and I think you mentioned that the law had recently changed in the UK to there being more obligations on businesses to report data breaches than there were previously. In the old scenario, before the legislation earlier this year, did you receive data breach reports from businesses on a periodic basis—from time to time?

Elizabeth Denham: We did receive data breach notices, especially from the health sector in the United Kingdom, and we would receive voluntary notices of significant breaches as good practice, but there was not a legal requirement to notify our office of significant breaches until 25 May this year.

Q4275 **Ian C. Lucas:** Did you ever receive any reports of data breaches from commercial organisations, rather than from hospitals or anything like that, on a voluntary basis?

Elizabeth Denham: Yes, we did. Particularly financial services—banks and other financial services organisations—would advise us of breaches, especially when a large number of consumers were affected by a breach.

Q4276 **Ian C. Lucas:** Do you know whether you ever received a report of a data breach from Facebook?

Elizabeth Denham: I am not aware of any breach notice that we had received, particularly from a technology company, but not from Facebook. But now, under the general data protection regulation, there is a requirement for all companies to report significant breaches, as well as public bodies.

Q4277 **Ian C. Lucas:** When we last met, I asked you a question about the GSR breach in 2015. I asked you who knew about the data breach within Facebook. You replied in your written response—thank you very much for that—which I am going to read out, actually. There is a particular sentence that I am going to ask you about. You said, "We do not hold evidence that Mark Zuckerberg was aware of concerns about GSR in 2015, however that isn't to say that he wasn't aware." I find that quite an interesting response. I spoke to Facebook this morning, along with my colleagues, and they suggested that Mr Zuckerberg first knew about this in 2018.

Have you any information that he knew before then?

Elizabeth Denham: We have searched the records that we have received from Facebook through our information notices throughout the investigation. We have issued three information notices to Facebook for various evidence. We know that there is a long chain of recipients to email, that shows that people knew about the breach, but we do not have Mr Zuckerberg's email on those documents. That is not to say that he did not know—I cannot theorise about that—but obviously senior people in the organisation were aware of that breach in 2014-15.

Q4278 **Ian C. Lucas:** That is in the United States.

Elizabeth Denham: In the United States. The focus of our investigation is really about holding the corporation—the organisation—accountable for data breaches and contraventions of the law. We are not focusing on individuals; we are focusing on the corporation.

Q4279 **Ian C. Lucas:** I asked Facebook this morning about their business model. I have concerns about the way that app developers seem to be sharing information with Facebook, almost as a matter of course. I asked for a single example of a case where Facebook had withdrawn services to a business because of a breach, and they could not provide me with one. Does that surprise you?

Elizabeth Denham: I was following Mr Allan's evidence this morning. Earlier this year—2018—Facebook reported that 200 apps had been suspended from the platform, and they carried out some investigations. Some apps were then allowed back on the platform. Our office has been following, investigating and looking at various apps that were associated with the Psychometrics Centre at Cambridge University. We have been following the data on some of those issues, but of course our office cannot investigate every app on the platform. We are really focusing on political campaigning and the apps associated with the GSR breach and the Psychometrics Centre.

Q4280 **Ian C. Lucas:** When you say 200 were suspended, when was that? Was that recently?

Elizabeth Denham: It was over the summer—after the revelations.

Q4281 **Ian C. Lucas:** After the revelations, they said they were going to carry out an audit, didn't they? So you are not aware of any case before the revelations?

Elizabeth Denham: I am not aware of any case before the revelations. I am just reporting back what Facebook told us in the summer of 2018, when there was a suspension of 200 apps. What happened after that is a question for Facebook.

Q4282 **Ian C. Lucas:** So they have not provided you with any cases?

Elizabeth Denham: As I say, we are looking at some applications associated with the Psychometrics Centre.

Q4283 **Clive Efford:** Following on from my colleagues' questions about GSR, the evidence we have seen suggests that Facebook is run by one person at the top—Mr Zuckerberg. You said in your response to us that people in the policy team at Facebook were aware, as well as Facebook's external counsel. Would you say it is unlikely that Mr Zuckerberg wouldn't know? Did you discover that the way that the company is run is similar to what I just suggested, which therefore makes it very likely that he did know what was going on?

Elizabeth Denham: I cannot say whether he knew what was going on. I can say that, in our experience, it is important that we are able to connect to senior officials in the US at headquarters. That is the way we were able to move forward in a more timely way with our investigation. I was able to speak with and connect with the chief operating officer, Ms Sandberg. That helped our investigation.

Q4284 **Chair:** Charlie Angus.

Charlie Angus: It is a real pleasure to be here in the UK with you, Ms Denham. You used to come to the Committee in Canada when you were the acting representative on privacy issues. I would like to begin by talking about the Canadian perspective on this, which is Christopher Wylie, Zack Massingham and Jeff Silvester—the Canadian connection to the Cambridge Analytica scandal. One of the things that was really striking about what Christopher Wylie said is that SCL found it convenient to set up a number of players in different jurisdictions. It was easier for a number of reasons for them to run these campaigns.

We found when we began our investigation—originally looking into the breach—that we had two guys above an optometrists shop in Victoria who suddenly came into all this money and may have undermined the Brexit vote, but were beyond the jurisdiction of Britain because they were in Canada. We subpoenaed them and forced the production of documents. That raises the question of the adequacy of tools for dealing with data mercenaries who are set up outside the jurisdictions in which they operate.

Can you give us any specifics that you think we should address or anything we may have missed? Despite the best efforts of our Parliament—we are willing to go into the corners with these guys—we still could not get answers from AggregateIQ at the end of the day about their corporate structure and how they were set up with SCL. We could go only so far. What tools do we need to be able to constrain or hold to account data mercenaries who are outside the jurisdictions in which they are operating?

Elizabeth Denham: I think that with digital campaigning, big-data politics, big-data commerce and the fact that personal data is the asset that is driving the internet, it is extremely important that data protection regulators have the ability to reach beyond their borders—extraterritorial reach. In the UK and the EU, we are now able to follow the data in that way. But it is also very, very important that we have strong enforcement

powers to compel documentation and to reach into the cloud, in a digital search. That is very important.

During this investigation, which is probably the largest data protection investigation we have ever undertaken, certainly in Europe, we were able to seize documents and evidence. We were able to get 700 terabytes of data from Cambridge Analytica, which we are crunching through and forensically examining. We were also able to work with our colleagues in other jurisdictions, including our Canadian colleagues. We are also collaborating with law enforcement agencies in the US, the UK and beyond. What is really important is that there are nine jurisdictions in this room, all concerned about protecting personal data, especially in the context of elections, campaigns and referendums but even beyond that, which means that we must have the tools to work together, to collaborate and co-operate, because this is truly a global issue. That is a strong recommendation.

Steve Wood: Just to add a bit to what the Commissioner said, it is really important that international regulatory co-operation networks are strengthened. Around the world, we are still observing that data protection authorities can perhaps have weak or limited powers, which gives them the legal basis to co-operate and share information with their counterparts internationally. In the longer term, we probably need to look at things like multilateral treaties. We really have some quite strong reciprocal enforcement mechanisms there to really make the extraterritorial scope of our laws, as they change, work in practice.

We are still at a relatively early stage as data protection regulators, in learning to co-operate around the world and because data has no borders now, this is a really urgent task. From the UK perspective, we are now chairing the International Conference of Data Protection and Privacy Commissioners, to try to lead that work and get some more global solutions, but it is going to take time. Lots of different countries need to join this work.

Charlie Angus: Thank you. I have two more questions on that, which have to do with the need to ensure that our regulators have the tools and the teeth. I think it was in 2008 or 2009, when you were the acting Canadian Privacy Commissioner, that you launched what I understand was the first investigation into Facebook, on their loosey-goosey approach to privacy controls. I believe that if they had followed your findings and your rulings we would never had the Cambridge Analytica scandal.

That was 10 years ago. You did not have the order-making powers to make them comply, but even if you had, it seems that Facebook has a sense that laws are something they will consider if it works, and if it doesn't they will find a way to explain it away or ignore it. In light of what we have dealt with now, you were very prescient back then. Do you think that we could have avoided a lot of this stuff if Facebook had shown some corporate responsibility back when you issued your report?

Elizabeth Denham: As you reminded me, it was 10 years ago that the report was issued by the Canadian Privacy Commissioner's office. That report laid bare the business model of Facebook and explained how the advertising model and third-party applications worked—the openness of the sharing of data with friends and friends of friends. But at that time, and still today, the federal privacy commissioner in Canada does not have order-making or enforcement power. Any finding has to be enforced by a federal court.

I feel that Facebook has looked at the Canadian finding and the Canadian and Irish recommendations more as advice. The message I heard from Facebook this morning was that unless there is a legal order compelling a change in their business model and their practice, they are not going to do it. That is a serious statement, but it means that we have to have strong laws and we have to have enforcement tools to move online platforms in the right direction, so that they take people with them in the services they offer.

Charlie Angus: When you were in Canada, you did not have the order-making powers you do now, and you have issued a substantial fine against Facebook. Perhaps I did not hear Mr Allan correctly, but it seems that he still feels that your findings of 2009 are advisory, because it is on principle 1, about the platform that was constructed to harvest data from friends without consent. He says that it is all there in the terms of service agreement and he said that this morning. So, is Facebook telling us that they believe that they can write terms of service agreements that override the laws of many different countries, because that to me is very disturbing?

Are you finding that, in the appeal that Facebook is making, they are misrepresenting your findings publicly, because I would find that very disturbing? If we are going to have corporate accountability, will we still see this culture of corporate immaturity such that they do not think that they need to be truthful, or do you feel that they are being accurate in how they represent their challenge to you? And do you think that they respect the necessity to respect the law about these issues of consent?

Elizabeth Denham: After a nine-month investigation, we issued a fine in October of this year. It was the maximum fine that was available to us under the previous regime and I stand by the findings and the enforcement action by my office. That said, any organisation—any company—has the right of appeal. But I was really disappointed by Facebook's statement in the context of the appeal, because I do think that they misrepresented the fact of our finding and the rationale for issuing that fine.

The statement that Facebook published last week said that our investigation found no evidence to suggest that the information of Facebook's 1 million UK users was ever shared between Dr Kogan and Cambridge Analytica or used by affiliates in the Brexit referendum. That was in Facebook's statement, and that much is correct about our investigation.

But our fine was not about whether or not UK users' data was shared in this way. We fined Facebook because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of friends, and friends of friends—and then Facebook failed to keep the information safe. So, in UK terms, that is principle 1 and principle 7 breaches.

That is pretty basic data protection 101; that is about notice and transparency and control. It is not a case of no harm, no foul. Companies are responsible for proactively protecting personal information and that's been the case in the UK for thirty years. Dr Kogan and Cambridge Analytica is just one example of what Facebook allowed to happen and what we are talking about here is up to 87 million Facebook users' data, represented in the jurisdictions of those of you around the table.

Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; it is about the release of users' profile information without their knowledge and consent. That is messages and likes; that is their profile.

I guess that, at the end of the day, I am really disappointed that one of the most innovative companies in the world—because great things happen on Facebook—have not replicated their innovation in ways that protect people's privacy online. That is how I would summarise it, Mr Angus.

Q4285 **Chair:** Nathaniel Erskine-Smith.

Nathaniel Erskine-Smith: I want to pick up on Charlie's line of questioning there—it is about the interpretation of the law. I was a bit confused. It is apparent to me that Mr Allan is not a lawyer, because he said to us today that for someone to have signed up for Facebook and agreed to the terms of service and not to have gone into their settings and checked a box to ensure that their information had additional privacy protections—one step and one omission together—meant that there would be meaningful consent for my friends to share my information with any app developer, regardless of purpose. That seems to me to be contrary to any notion of meaningful consent. What do you think about that?

Elizabeth Denham: That is the basis of our fine. We found that there was not consent, there was not meaningful information, there was not meaningful notice, and terms of service cannot trump the law.

Nathaniel Erskine-Smith: You said that it is privacy law 101. Facebook is worth billions and billions of dollars, and can surely hire a lawyer. A lawyer was not here before us today, but why do you think Facebook is still challenging the ruling when the basic premise of meaningful consent is so very obvious to any lawyer who has ever practised privacy law?

Elizabeth Denham: Because the profiling and the use of personal information, complying with meaningful consent and notice, is at tension with its business model. I think there is a way to resolve this. Regulators need to enforce the law; I need to do my job, and that is what I am doing

here. Facebook has the right of appeal, but it should not misrepresent our findings and the basis of our monetary penalty.

Nathaniel Erskine-Smith: From a legislator's point of view, when one is frustrated with the lack of accountability and what seems to me to be Facebook officials coming to the table and apologising only after they have been found out to have made a series of mistakes, it is frustrating and also bizarre that they continue to compound those mistakes and say, "We're sorry, but by the way, we did nothing wrong." It is strange.

With respect to penalties, in the Canadian context, our federal privacy commissioner does not have the power to make orders or to levy fines. I have actually introduced a Bill in Parliament to address that, but you now have powers under GDPR to levy significant fines. I was on a panel recently with the head of public policy at Facebook Canada who said, "Naming and shaming works just fine, and the ombud's role has served us well." What is your view of the ombud's role, versus having significant powers? Do you think companies like Facebook are responsive to naming and shaming, or do you think the power to levy fines is of critical importance?

Elizabeth Denham: You need the whole package. You have to have the ability to issue orders—maybe a "stop processing" order, telling a company it can no longer process personal information for a certain purpose and in a certain way. That is pretty powerful, but having the fines available is a way to focus attention at the board level of an organisation, and really build good data governance.

Q4286 **Jo Stevens:** I just want to go back to a question that I asked you when you came to see us on 6 November, which was about illegal data sharing between Arron Banks' Eldon Insurance and the Leave.EU campaign. In September 2015, Eldon Insurance sent over 300,000 Leave.EU newsletters to Eldon Insurance customers. You issued an information notice to Eldon Insurance in April 2018, and Eldon Insurance told you that it itself had reported that breach to you. I asked you in November when it reported that breach. Can you tell us whether or not you have found out from Eldon Insurance when it reported that breach, and have you had any proof of that, please?

Elizabeth Denham: Eldon Insurance stated in response to our information notice, as you said, that it reported that breach to us when information was shared between Leave.EU and Eldon Insurance. We found no evidence of its report of such a breach, and you know that we have issued fines against Eldon Insurance under the PECR regulation. We continue to investigate data protection issues, and we have announced an audit of Eldon Insurance as well.

Q4287 **Jo Stevens:** And it has not subsequently provided any proof to you to back up its claim.

Elizabeth Denham: It has not.

Q4288 **Chair:** Bob Zimmer.

Bob Zimmer: Thanks again, Ms Denham, for speaking to the Committee for the second time—the first time on this side of the Atlantic. I have one question for you. We are tasked with making laws to get a handle on Facebook and the social media platforms, etc. I am looking for your advice. What would you do if you were in our place? I know it is difficult in your role to say so, but as much as you can say, where would you start with these guys? From my perspective, the risk to democracy is the most important concern. How would you best combat that and what kind of laws would you make? This could be a 2,000-hour conversation, but as briefly as you can, where would you start?

Elizabeth Denham: One of the reasons that we launched the investigation in 2017 was to look at the whole political campaigning ecosystem, who the players in that system are, how data is collected and used, and what the responsibilities are of each of those various actors. Political parties are part of this. Political parties have a lot of data. They purchase data, perhaps from data brokers. They collect it in various ways. So we need to look at political parties as part of this as well, and make sure that they are able to use new digital campaigning techniques to engage voters and, at the same time, comply with the law and be transparent, and give people control about how they use information.

This is not just about social media companies. They are a large part of digital campaigning now. The spend that political parties and campaigns put towards digital campaigning is growing, but before the train leaves the station and even more intrusive techniques are used in our democratic processes, we have to get a handle on this. Electoral laws need to be strengthened and brought into the digital age—election financing, and transparency and imprints in advertising on platforms.

This is not a simple answer, but we need to look at all the existing regulations to make sure they are up to date and fit for purpose, but we also need a code of practice for political parties and campaigns, because they are at the centre of using these services. One of the main recommendations that our office has made in this investigation is for a statutory code of conduct for the use of data in political campaigns. That is important. That might be something, as we develop this code, which might be of interest to other jurisdictions.

Bob Zimmer: This is part B to that question. We just had political parties appear at our Committee in Canada to answer questions. For the most part, political parties follow the rules, because it is in their best interests to do so. They follow the framework as best they can; again, it is in their best interests to do so. My main concern—although that is part of it—is the foreign actors and the people who show up with a Facebook account that is started one week before and is actively campaigning against members of Parliaments sitting around this room, for whatever reason. How do we best get a handle on that? The part outside of the official establishment—how do we get to those bad actors?

Steve Wood: In terms of the context of different actors coming into the political space, not just the main parties, we have seen proposals around

better registration systems for how political adverts are to be organised online and the transparency that follows from that, so that you can actually see who has targeted an advert and who has paid for it. The challenge is to make that work in practice. It is certainly something that we know the Electoral Commission is taking a strong interest in, in the UK. We have seen Facebook roll out this initial programme in the UK. We have certainly seen some evidence that it has already been circumvented in some circumstances.

I think we have to learn how to make this work in practice. It is good to see some proposals coming forward about making this work. Particularly for those actors who perhaps have an interest in not being transparent about who they are, in terms of using the advertising systems on social media platforms, we have to focus on some quite strong governance, which really gets people to engage with a process of identifying who they are, so that that transparency works in practice, and we can follow the money and see the ads.

I think it is a good principle. We are supportive of it and we made a recommendation around that area that it should go forward in our report in July. I think we have to learn from the practice and see how it is working. It is obviously being rolled out in other countries as well, so we look forward to seeing how that works.

Q4289 **Giles Watling:** I would like to move on to the regulation, which we touched on earlier. In your excellent response to us, Ms Denham, you said that you "acknowledge that, without a very substantial injection of resources and headcount, it is unlikely that any regulator would be able to directly handle the volume of individual complaints" and so on. I would like to ask you whether you mean by that, whatever regulations we might like to put in place, that it is almost unenforceable.

Elizabeth Denham: Not at all. My response around internet harms was not necessarily just in the political context. It was about regulating content and conduct online. My point was, if you set up a regulator to take complaints about take-down requests—where somebody saw offensive material online and wanted it taken down and went to a regulator with every single complaint—you would have a regulator dealing with millions of complaints.

Rather than that system, I think the opportunity to think about is regulating the effectiveness of processes that have to be put in place for things like taking down or responding to complaints from individuals. So the regulator is saying, "Are all the processes effective for meeting the public goals and the objectives that are set out by Parliament?". You come up with a standard and the regulator has to go into Facebook, Twitter, Snap and Google and say, "Show me how effective you are and be transparent about the numbers of take-downs and the context of the material," because we are talking about something that could potentially have millions and millions of complaints.

Q4290 **Giles Watling:** So what you are saying is that you are relying on the

companies themselves to do that work.

Elizabeth Denham: But you have a regulator as a backstop that ensures that they are meeting standards that are set in law. That is what we do not have right now. The gap in internet harms is that we do not have anybody who is regulating content and conduct online. We are regulating the use of personal data. We are not looking deeply into content.

Q4291 **Giles Watling:** So that is what you would recommend that we do, and that is what you would recommend we do on a global basis.

Elizabeth Denham: I think that is where the public concern is. The public are really concerned about what happens online and the kind of harms online, and they expect their Parliaments to regulate to protect them from those harms.

Q4292 **Chair:** Edwin Tong.

Edwin Tong: Good afternoon, Ms Denham. Thank you very much for being here and for the note that you sent to the Committee before today. I have a couple of questions that arise from what you have said here. In one of the points you made—I am not sure which page it is on, perhaps the second full page of the note—you say that a co-ordinated approach needs to be taken to internet harms. By that, I take it you mean that we need not only regulation and legislation, like you spoke about a short while ago, but a range of other measures, such as media literacy, improving standards of journalism, making sure that schools teach our children the right approach to being more discerning online, and so on. Would I be correct?

Elizabeth Denham: I think it is complicated to say how we are going to address the kind of harms that the public are concerned about—everything from misinformation to disinformation to opaque advertising in the political arena to kids spending too much time online to data privacy; all those issues. But digital literacy and digital media are really important, and they make us all a little bit more diligent in how we read things online and understand them. We also need transparency and more regulation. There are so many different aspects to this. When you look at the political context, which has been the focus of our investigation, we have some very specific recommendations.

Edwin Tong: I understand. So what you're saying is that there is no single, silver bullet, but there has to be a suite of measures to tackle this problem. Is that correct?

Elizabeth Denham: You said it very well. I think there are many actors in this space, including citizens, the education system, the social media companies and Parliament.

Edwin Tong: On the question of legislation, your report mentions that there are still a number of internet harms that do not appear to be fully addressed by current law and regulation. You cite the fact that harmful conduct online, which currently might be legal, needs to be dealt with. Can you elaborate on that?

Elizabeth Denham: Obviously, countries have defined illegal online conduct. The issue is how that is enforced. How quickly do social media companies and online platforms remove, and deal with, illegal content? The gap is actually in content that is legal but might be offensive to certain individuals—kids are a good example. The public are looking for legislators to find the right regulatory approach that deals with online harm but also protects freedom of expression and innovation and balances those processes.

Edwin Tong: Would you seek regulation to protect, say, children and the general public from content that could be seditious or incite hatred?

Elizabeth Denham: That is correct. Although it is complicated and complex to come up with the rules that will balance all these interests, our research shows that the public expect Parliament and legislators to do that.

Edwin Tong: The sense is that some kind of legislation needs to be enacted to deal with those online harms and to define the parameters. To borrow your language, you say that online non-criminal harms could be as significant as criminal harms because of the scale of potential activities. I think you mean the proliferation of material on the internet—the quick spread of such information online. Is that right?

Elizabeth Denham: That is exactly right. We are especially concerned about children and vulnerable adults.

Steve Wood: On preparing to think about legislating in this area, it is probably the biggest gap because it is the most complex area—the intersection with freedom of expression. The public have a wide spectrum of views on what they find upsetting and on what information should be removed. We have to learn how to have quite deep dialogue with the public. We have to come up with some ways to research—probably concepts like citizens' juries—to come up with some sophisticated ways to balance these issues and get the decisions right. On the issue of harms that might build up over time and have an impact on people's mental health, we must factor in the longer-term effects of various internet harms, but we have to learn and have all the evidence and research to back up taking that approach.

Edwin Tong: Those objectives have to be balanced by the speed at which you can address the harms that are being spread. I imagine that strong, quick levers are needed to stop and stem the spread. You would also need to be very clear about the kind of information—society may differ on that, so each Parliament has to look at it from the perspective of what society needs to be protected against.

Steve Wood: Certainly, from the perspective of the public, they expect something to happen fairly quickly when they see concerning or upsetting material. You are right: we have to learn from the companies responding how the levers can work in practice, and we have to learn about the checks by the regulator to look at the overall systems that they are using.

If those need to be adjusted, or if their criteria are not right, that overall system approach has to be adjusted quickly to reflect the concerns.

Q4293 **Julian Knight:** You have been very helpful to the Committee during the course of the inquiry, Ms Denham. You have been very open both in public and in private. I thank your organisation for the way it has interacted with the Committee.

I have a few questions to put to you. A £500,000 fine for Facebook—that is probably its sandwich bill for a week. It is almost the definition of a drop in the ocean. What more can you do? Does it need to be something that is really fundamental and hits them very, very hard indeed in the pocket, like the sort of super-fine that we have seen from the EU in the past for American institutions? Do you feel frustrated about the level of fines you are able to issue? What are your thoughts about the fines you are issuing?

Elizabeth Denham: The £500,000 fine that we issued against Facebook was the maximum fine available to us in the previous regime. Because the contraventions happened before 25 May 2018, £500,000 was the maximum. I have been clear that had the maximum fines now available under the GDPR been available to us, we would have issued a much more significant fine to Facebook.

Q4294 **Julian Knight:** Would you have issued the maximum fine?

Elizabeth Denham: A much more significant fine. It is a bit hypothetical, because that wasn't available to us. We now have up to 4% of global turnover, as do the other EU data protection regulators. That is a significant fine for a company, and it would have an impact on its bottom line. I also think that our findings and the fine that we issued are important, because we found their business practices and the way applications interact with data on the platform to have contravened data protection law. That is a big statement and a big finding.

Q4295 **Julian Knight:** Are you looking at Facebook right now, in terms of potential contraventions after the new regime came in?

Elizabeth Denham: We are, and as you know, with the GDPR, the new legal arrangements are that the Irish data protection commissioner is the lead authority for Facebook, because Facebook Europe is based in Ireland. We are working with our Irish colleagues. We have referred matters of an ongoing nature and concerns that we have about Facebook right now on to our Irish colleagues. As a competent authority, we are available to help them with that.

Q4296 **Julian Knight:** Given Ireland's record with firms locating there basically to avoid tax, do you think they will be as firm as they ought to be in pursuing Facebook and ensuring that these potentially current transgressions are properly punished in a way that the public has confidence in?

Elizabeth Denham: There are several investigations ongoing under the lead of the Irish data protection commissioner, who I have great confidence in, as well as other regulators in the EU. We are joined

together in a social media working group, because there are so many issues when it comes to some of these tech giants.

Q4297 **Julian Knight:** The new regime promised to really punish these firms when they transgress in this way, but it doesn't look to me as if it has a great deal of teeth because of the issue of Ireland being in charge of the process. You are not going in and saying, "Hang on a minute. You are trading in the UK. Therefore you should be facing maximum fines if you are transgressing."

Steve Wood: Certainly we have observed closely how the Irish commissioner's office has increased its resources over the last few years to prepare for GDPR. It has doubled the staff and is hiring technologists to get ready for this challenge. The other thing, just to build on what the commissioner talked about, is that if the Irish data protection authority has a case that affects data subjects across Europe, it will probably have to prepare a draft decision in that situation. It can then essentially be called into the European system as part of the mechanisms under the GDPR. There will be an overall decision if the other European data protection don't agree with that draft decision put forward by the Irish, in that instance. It can be a Europe-wide decision as part of the mechanism. There are some balances and checks to make sure it addresses the concerns of Europeans.

Q4298 **Julian Knight:** Can you recommend that they fine the maximum amount?

Steve Wood: Part of the discussion will be whether the GDPR has been applied correctly in that situation.

Q4299 **Chair:** Sun Xueling.

Sun Xueling: You have mentioned that regulations should be a backstop to regulate content and conduct. Would you agree, then, that there is a need for a framework to bind tech companies and regulators to collectively address this information and online falsehoods?

Elizabeth Denham: A collective action between regulators and companies?

Sun Xueling: A framework to bind tech companies and regulators together.

Elizabeth Denham: I believe that the time for self-regulation in this context is over. My recommendation to the Committee for consideration is that, because of the public concern about these internet harms around content and conduct online, Parliament needs to define the outcomes. There needs to be a set of standards that are agreed and a regulator has to be equipped with the right powers to be able to review the activities of the companies.

The complexities of the different platforms is something to take into account. Snap is different and has different operating processes to Facebook or to Google. That is why I think the platforms have to have some overall standards that they have to comply with, but they have to be

judged in the context of who they are serving. With a platform that is operating and serving kids, for example, there would be some different requirements.

To be clear, I am not advocating for a self-regulatory model. I am advocating for a strong regulatory backdrop to a set of standards.

Q4300 **Chair:** Pritam Singh.

Pritam Singh: The realm of fake news and disinformation is not just the domain of opaque social media companies. In this social media age, marked by technological innovation, it can be argued that opaque Governments precipitate the formation of a vacuum, which is then abused by peddlers of disinformation and fake news. Given your experience, what advice would you give Governments in general and opaque Governments in particular around the world that seek to move in the direction of open government? Secondly, and closely associated, how does open government better inoculate a citizenry against disinformation and fake news?

Steve Wood: That is a question we are quite happy to answer as well because the other piece of legislation we are responsible for as a regulator is the Freedom of Information Act in the UK. Governments setting an example of putting as much factual information into the public domain to support and inform debate so that that provides a rich seam of information, which can support debate, and Governments showing the way by being open and proactively responding to freedom of information requests that citizens may make, and that being part of a fact-checking process, is probably another part of the jigsaw that can set an important standard. As we have discussed already today, it is another lever that can help improve the environment. I think if a Government are legislating in this area, a good way for the Government to set the standard is to show how they themselves are being open. That also means embracing new technologies and it is about open data and very much explaining how data can be used to understand the workings of the Government and making that available to civil society and so on. Governments certainly have a role to play in that wider debate, as one part of the jigsaw.

Pritam Singh: You spoke about fact-checking. That is one of the recommendations that our Select Committee in Singapore looked into. It is not so simple, because there are questions about who finances and funds it, and questions of that nature. If you have the Government funding it, there are questions about an obvious conflict of interest there.

What advice would you give to countries that are considering fact-checking platforms, particularly small countries such as Singapore, where the media landscape or media companies—I wouldn't say don't have deep pockets, because some media companies do, but where there is obviously a conflicted party driving that fact-checking process? There are contradictions.

Steve Wood: You are certainly right that it is a balance. Equally, you do not want to have a Ministry of Truth and an overarching body that decides the factual basis that people might seek to complain about. Certainly, having a strong regime for the regulation of national statistics, which we have in the UK, is a good basis to start. There are some core areas where data is particularly quoted as a central area of national debate. It is also about having a strong, vigorous civil society of fact-checking groups, as well as starting to pioneer some ways to do that and to use large datasets. Fact-checking can often be complicated, with big claims. I guess the UK, like a lot of other countries, is finding its way, but I think at the core there has always been a bedrock. I am thinking particularly of official statistics; there is a high degree of confidence in that area, which the UK has led strongly on.

Q4301 **Chair:** Nathan.

Nathaniel Erskine-Smith: You mentioned that the public's concern is additional regulation of content. I asked Facebook, because they supported an Act dealing with tackling content. If it is a legal liability for Facebook when they do not take down content in relation to child exploitation, it seems to me a short step to imposing legal liability for failing to take down hate speech and other horrible illegal content. It would not be you regulating that; it would be some sort of agile judicial oversight, in co-ordination either with the companies themselves or with another regulator.

You have spoken to regulating the effectiveness of processes and to transparency, but I have not heard anything today about algorithmic transparency and auditing algorithms. I raise that point because Richard Allan said something at the end of his session that I wish we had explored a little more. He said that where content is right up against the line, but where they deem it not to be hateful and they do not take it down, their algorithm has a perverse effect. Because that content is divisive and is designed to get a reaction, the algorithm actually increases traffic for it. They are looking at not rewarding that content that pushes up against the line of hate. It seems obvious for a company to do that if it cares about the public interest. Would the ability to audit algorithms reside in your office? Is that the appropriate place? Could you speak to the importance of algorithmic transparency and auditing algorithms in a human rights context?

Elizabeth Denham: Under the GDPR, there are enhanced requirements for explainability in algorithms in the context of personal data. If a company or an organisation is making a decision that is basically done by machines, it has to be explainable and it is challengeable. As another part of the work we do, we are going to be auditing algorithms for issues of fairness, data protection, bias—all those issues. So we are going to be in the space of looking at algorithms and looking at transparency, but you are talking about algorithms used to deliver content. That is associated with us, but it is not right in our space.

I think the challenge for all of us is that data protection is horizontal—it runs across digital advertising and digital campaigning. The use of personal data is part of all this. We are not an expert content regulator, but nobody is. It is about whether or not a country or a jurisdiction thinks about sharing the load between existing regulators and finding some kind of collaboration, or creating another regulator. But you have to be careful that that does not crowd out the existing space, because that creates confusion for individuals and confusion for companies.

Nathaniel Erskine-Smith: It seems to me that we have traditional regulation of content in relation to editors. We hold editors accountable, but as editors are replaced by algorithms, for some reason we have failed to hold accountable those algorithms and the companies that are making billions of dollars in profit from them—in part, at least.

Q4302 **Ian C. Lucas:** I have a couple of brief follow-up questions—on GSR again, I am afraid. First, I think you said in your evidence that within Facebook they were first aware of this in 2014. Is that correct?

Elizabeth Denham: I would have to go back and look at the report.

Q4303 **Ian C. Lucas:** I am asking because some of the evidence that we have had says that the awareness within Facebook was because of a news report in December 2015. Are you aware of their having any awareness before 2015?

Elizabeth Denham: I would have to write to you, Mr Lucas. I do not have the report in front of me.

Q4304 **Ian C. Lucas:** That is fine. Connected with that, you referred to a number of "senior managers"—I think that was the wording used. Can you name them?

Elizabeth Denham: We can write to you with those names. What we have written so far describes the types of positions and titles.

Q4305 **Ian C. Lucas:** We are discovering that the Facebook management structure is somewhat delphic. The best way for us to be clear about chains of responsibility is to have the names. If you could write to us with the names, I would be very grateful.

Elizabeth Denham: I will write.

Q4306 **Chair:** Charlie.

Charlie Angus: I just want to follow up on my colleague's question about algorithms. I ask you because you come from a Canadian context, where we have no digital committee in Parliament. The usual job of the Ethics Committee is smut and corruption, dodgy lobbying meetings and loopholes, and it is something I understand. I got 52% in grade 10 math. I don't know what an algorithm is, and yet I am being asked more and more to look at the ethics of algorithms in terms of public policy. As much as we look to our regulators to understand this, as parliamentarians we are setting public policy based on how Governments will deliver services and how all manner of things will be. To keep an eye on the public policy issue

of ethical accountability for algorithms, whether it is a standing committee or a one-off study, what would you recommend?

Elizabeth Denham: I think it is a critically important area of study for legislators. In the UK, House of Lords and Commons Committees have been examining the impact of algorithms on society across all sectors, public and private. The impact of AI on future employment, jobs, self-driving cars and robotics are critically important areas. In Canada, absolutely there should be a standing committee and various studies, because with the focus on digital innovation in AI, the public policy that goes along with that and the digital ethics are critically important.

Q4307 **Rebecca Pow:** Do you think that a Committee like this, going forward, could be valuable in informing how we go about regulation on a worldwide scale? It is clear to me, talking to all these different countries that are doing a great deal of work individually, that this is much more than an individual country issue, and we need to align.

Elizabeth Denham: I am really pleased to speak to this Committee. We have nine jurisdictions here, representing 450 million people, looking at issues related to internet harms and electoral interference, which are issues of widespread concern to your citizens. Ideally, there would be some kind of international instrument or agreement, with a set of principles that your democracies could agree to. That will be some time away, I suspect, because domestically you have different constitutions, cultures and laws, but I think you all share some things in common, and we have these big internet companies working in this space and delivering services globally.

The answer is yes—working together is very positive for your citizens. When one jurisdiction goes out with a new solution—such as France coming forward with judicial decisions around taking down disinformation, Germany's approach, the UK having been strong in examining these issues and bringing regulators together, and the European Commission having the voluntary code; there have been a lot of initiatives—getting the jurisdictions together to look at the best approach is very positive.

Q4308 **Chair:** When you gave evidence to the Committee earlier this month, we talked a little bit about your discovery of Russian IP addresses remotely accessing the data collected from the This Is Your Digital Life app, or whatever it was called—the precursor to the Cambridge Analytica data-gathering app. Can you tell us any more about those investigations into the Russian IP addresses and where they may have come from?

Elizabeth Denham: We have reported to the National Crime Agency those IP addresses that resolved to Russia, and we have been working with it on that issue. It is not for us to chase down what is going to happen and what has happened at the other end. We continue to work with law enforcement on that. I have no further update other than what I said in our private session earlier.

Q4309 **Chair:** Would you expect that investigation to be concluded when the NCA completes its investigation and takes whatever action it needs to take?

Elizabeth Denham: I expect: what I do not know is whether the results of that investigation will be shared with parliamentarians, or with some parliamentarians. You probably know that process better than I do.

Q4310 **Chair:** If the National Crime Agency decides that there has not been criminal activity and decides not to take any further action, would you be able to report back to the House in more detail once the NCA's investigation is completed?

Elizabeth Denham: I will get back to you on that. I need to check with the NCA and the NCSC.

Q4311 **Chair:** I want to follow up on Ian Lucas's question about senior executives at Facebook who were aware of the Cambridge Analytica data breach. I appreciate that you are going to write to us with names, but from your investigations, do you feel that Facebook has a process in place to notify the senior team of issues like this? Is there a clear reporting path? Are there clearly executives to whom this sort of information is reported and who, it is expected, may in turn report it to others within the company?

Elizabeth Denham: I believe that most of the decisions are made by headquarters. That has been my experience in working with Facebook. Certainly, as I have said, the way we have been able to move our investigation forward is by connecting with headquarters and not necessarily with the European representatives, although we are working with them as well. That is as much as I can say.

Q4312 **Chair:** Would it be fair to assume, in that case, that when you talk about senior executives at the company who are aware of the data breach, they would be senior executives in Menlo Park rather than just here in the UK or in Europe?

Elizabeth Denham: I expect, for significant data issues and data breaches, that that would be the case.

Steve Wood: We would expect the situation to have improved since some of the historical events that you are looking at. The requirement under GDPR is for organisations to appoint a data protection officer when they have a risky profile in terms of the types of data processing that they do. That has to report to board level in organisations, so there are some strong drivers there, particularly looking ahead at how internet companies should have the right sort of governance in place for these things to be escalated. It is important to look to the future in what should be done.

Q4313 **Chair:** I think I can infer from what you said that you do not feel that in 2014 or 2015 they necessarily had those structures in place.

Elizabeth Denham: I know it has improved since then. The company has changed significantly since 2013-2014, and it has certainly changed since 2008-2009.

Q4314 **Chair:** Would it be fair to say that from your investigations, you do not believe that there is a clear reporting structure to board level for data breach issues and data privacy issues?

Elizabeth Denham: There is now—it is legally required—a straight reporting structure all the way to the board level.

Q4315 **Chair:** But you don't think there was then?

Elizabeth Denham: I don't think it was in place in 2013-14.

Q4316 **Chair:** Do you not think that that is extraordinary, given that in late 2011 the Federal Trade Commission ruled against Facebook for a lot of the reasons that you set out earlier—they were not protecting users' data, and apps were able to gain as much access to user data as they liked, seemingly without any restraint? That complaint had already been made in 2011 and the company was required by the FTC to put those policies in place. It does seem quite shocking that potentially three years later they still had not put those systems in place.

Elizabeth Denham: I think that Facebook continues to mature as a company. I think the pressure that sessions like this and the Committee's work, and investigations by the FTC, by our office, by Europe, by Ireland—we need to keep that pressure up. As I said, I am very disappointed that Facebook, being such an innovative company, could not have put more focus, attention and resources into protecting people's data.

Q4317 **Chair:** It just doesn't seem like they took much notice of the FTC's report.

Elizabeth Denham: As you know, the FTC is having another look at its consent decree. It will take some time but it will be reporting on it as well.

Q4318 **Chair:** You said earlier on, when talking about how users should give informed consent to the use of their data, that with regards to the data gathered by Aleksandr Kogan for Cambridge Analytica this was—in your words—just one example. How many examples have you seen of breaches in the user data policy?

Steve Wood: Obviously, we have very much focused on that one area in our investigation. We mentioned earlier that we heard the news that Facebook had suspended the 200 apps as well. We are aware that it is a widespread problem. We have really tried to focus in and narrow in on the areas where we can really make a difference, which is why we focused on Facebook at a platform level, to ultimately reach that finding. We have issued the adjudication, which has led to the fine.

Q4319 **Chair:** Are there any other examples you have investigated?

Steve Wood: As the Commissioner mentioned earlier, we have still got ongoing interests in other apps connected to the Psychometrics Centre in Cambridge. That is an ongoing area of interest.

Q4320 **Chair:** These are apps that are not currently known about? Is it not in the public domain that this is being investigated?

Elizabeth Denham: That is right, but in terms of Facebook, we have looked at it in different contexts. We intervened on the merger between WhatsApp and Facebook because the reason for that merger was increased sharing of data. We actually worked with WhatsApp and

Facebook and have an undertaking by WhatsApp that they will not share information with Facebook until they can show that their plans comply with the GDPR. We have looked at Facebook in other contexts but I think your question is really focused on apps.

Q4321 **Chair:** One of the concerns that we have—and this came up in the questioning earlier and I think certainly comes out of the papers from Six4Three that the Committee has been given—is whether the problem of widespread access to user friend data, without the knowledge of the users, was so commonplace that it might not necessarily appear to be a problem to Facebook.

Elizabeth Denham: That could be the case and we are interested in the Six4Three evidence. We knew about the company and they were unable to share that information with our office, because of the seal by the court. I am interested. If we are legally able to look at that data, we will look at it. That might be important to the litigation that we are going to have with Facebook, because at the hearing before the tribunal there is a potential of new evidence being submitted, in the context of that hearing, if it is relevant.

Q4322 **Chair:** So you believe that the unsealing of that evidence could be important to your current investigation into Facebook?

Elizabeth Denham: We do not know what the evidence says but it could be, because it could go to decisions that were made in 2013-2014. We have not seen the evidence, obviously.

Q4323 **Chair:** But you said that you had approached Six4Three yourself to ask whether you could have access to that?

Elizabeth Denham: We had a conversation with Six4Three. We talked to their lawyers who at the time, because of the sealing of the records, were unable to share the evidence in the email with our office. This was some months ago.

Q4324 **Chair:** I certainly think that the evidence contained within those sealed documents would be of considerable interest to the Information Commissioner's Office, as it would be to us as well. Finally, on Cambridge Analytica, do you believe that the database collected by Cambridge Analytica and the tools that they acquired are being used by other companies today? Do you believe that they are effectively trading under a different name?

Elizabeth Denham: We are actively monitoring the former directors or the directors of the company and any spin-off companies that come out of it. We are actively monitoring that. We have the ability to follow the data. We are still crunching through 700 terabytes of data, so we are discovering more about Cambridge Analytica as time goes by. As you know, we are in court on a criminal matter with Cambridge Analytica in January, so we continue to pursue that.

Q4325 **Chair:** Has the ICO looked into the company Emerdata, which the Committee has taken an interest in before?

Elizabeth Denham: Yes, that is an active line of inquiry.

Q4326 **Chair:** In terms of whether Emerdata is being used as the vehicle for Cambridge Analytica?

Elizabeth Denham: Yes.

Chair: I think that concludes the questions we have for this session. Once again, Elizabeth Denham and Steve Wood thank you very much for joining us today.

Examination of Witness

Witness: Ashkan Soltani.

Q4327 **Chair:** We will start the final part of our session. Ashkan, I know you were probably monitoring the session we had this morning with Facebook. Obviously, the work of the FTC, and the FTC report in 2011, was something we asked a number of questions about. Perhaps you could just share with the Committee your thoughts and insights on the evidence session you heard this morning, and how Facebook's interpretation of the FTC's ruling, and how it has tried to comply with it, sits with your own views on this matter.

Ashkan Soltani: Thank you for having me. I will just give a quick background. I was a primary technologist at the Federal Trade Commission and worked on the Facebook investigation in 2010-11. I was later the chief technologist at the FTC in 2014. I also worked briefly in the last White House—the Obama White House—at the Office of Science and Technology Policy. I most recently helped to write the California consumer privacy law that just passed in June. My opinions here are solely my own and, given the nature of the FTC investigation, they will be based only on publicly-available information. I also want to apologise for my attire. I was not planning to testify today, so I did not bring appropriate clothes. Fortunately, I was able to borrow a blazer.

I want to make three quick comments based on the comments from this morning, related to what I have observed in my work, both as an independent researcher and what is public in the FTC settlement. At the very beginning of the hearing, around 11 minutes in, Mr Allan corrected one of the comments from you all, specifically that apps in version 1 of the API did not have unfiltered access to personal information. In fact, that is false. In the 2011 FTC settlement, the FTC alleged that if a user had an app installed, it had access to nearly all of the user's profile information, even if that information was set to private. I think there is some sleight of hand with regards to V1, but this was early V1 and I believe it was only addressed after the settlement.

Additionally, in the same complaint, the FTC found that Facebook misrepresented their claims regarding their app oversight programme, specifically Facebook's verified apps programme, which was a detailed review designed to offer extra assurances to help users identify applications they can trust. The FTC found that that review was actually

non-existent and the company was not doing anything to oversee those apps. Again, that is in the complaint.

Additionally, there were some statements made that the apps would only have access to information if a user installed them and consented to that access. I helped *The New York Times* in their investigation and verification of the whitelisted apps programme and I have some tweets in that regard that show the screenshots of this access. Specifically, apps were able to circumvent users' privacy settings or platform settings, and access friends' information as well as users' information, such as birthday and political affiliation, even when the user disabled the platform. Those are the pre-installed apps.

Additionally, through a Facebook programme called instant personalisation, some apps such as Yelp and Rotten Tomatoes would automatically get access to users' personal information, even without the user installing them. So, simply by being a Facebook user and visiting the Yelp website, Facebook would transmit to Yelp your home town, your location, your preferences, etc. So those are some discrepancies, I think.

The timelines vary, but this—in my opinion—was V1, if they are considering the changes in 2014 as V2. In short, I found that time and time again Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements. This architecture means that if a bad actor gets a hold of these tokens, such as in the case of Pinterest, there is very little the user can do to prevent their information from being accessed. Facebook prioritises these developers over their users.

I think it was best laid out in Mr Allan's "win-win-win" comments, that "the platform enables things we are not going to do and they are going to do". Right? Facebook gets more engagement from the platform; Facebook users do things that Facebook does not normally provide; and developers get access to a large consumer base. Right?

Another way to describe this is that Facebook pays app developers to build apps for them using the personal information of their users. Right? So, if I am a company and I want to have an app like FarmVille, or a third-party Blackberry client written for me, I would have to pay hundreds of thousands of dollars in development time to have that app built. But Facebook says instead, "Developers, please come and spend your engineering hours and time in exchange for access to user data". And I think that kind of summarises the core issue.

Additionally, from my experience I do not think Facebook is able to govern itself in this area. From my observations of public data as well as my conversations with multiple stakeholders inside the company, my understanding is that senior leadership simply does not prioritise these issues seriously and they will continue to do the bare minimum necessary to pass through the compliance regimes, but will absolutely continue to make these mistakes as their priority is monetisation of user data.

Thank you for your time and for having me here.

Q4328 **Chair:** Thank you very much for that statement. From what you said, it sounds pretty clear that what Facebook said to the Committee—what Richard Allan said to the Committee—was not true, and that users had no real control at this time over how their data was being used, and even when they tried to enable their privacy settings to protect their data, developers were able to get around that without the user knowing.

Ashkan Soltani: Right. And not even get around that—they always just had access to it.

Q4329 **Chair:** Right. And from what you have said, this is effectively a commercial decision by Facebook, doing a deal with the developers in order to encourage them to build on the platform.

Ashkan Soltani: Correct.

Q4330 **Chair:** Charlie Angus, would you like to come in?

Charlie Angus: Thank you. I guess my concern is, because you said you were worried about their ability to self-police regarding these mistakes, that this is a company that we have been told made $18 billion in the first quarter this year—this is a very, very focused and driven corporation. The fact that it is ignoring its obligations cannot, to me, be seen as a mistake any more. The fact that its senior representatives spoke to a parliamentary Committee—which I believe, as we have it in Canada, is testifying as under oath—

Chair: Correct.

Charlie Angus—and misrepresented basic facts is a contempt of our legal parliamentary system. Also, if we cannot trust them to follow the law, we have bigger issues.

I want to ask you questions about your regulatory position. We see in Canada a real unwillingness of Facebook to show up to talk to regulators, but an incredible willingness to go behind the scenes to lobby, to hang out with Ministers and to do all manner of favours to get a free pass on legislation.

In your experience in the United States, it seems that Facebook spends an enormous amount of money lobbying legislators so that they do not actually have to talk to legislators about their legal obligations. How would you characterise the corporate culture of Facebook when it comes to the rule of law and the rule of obligations to the democratic jurisdictions that they work in?

Ashkan Soltani: I think your observations are exactly correct. In the lead up to the passing of the California Consumer Privacy Act, Facebook came out publicly in support it but was in fact still lobbying behind the scenes against it. We have seen that time and again.

This is currently the first time I have seen in the US when the Administration, Congress and the companies are all aligned to pass federal

privacy legislation, primarily to pre-empt the California law and to potentially give them carve-outs from GDPR, because the conservative Administration feels like it might be oppressive to business. My understanding is that Facebook is very involved in that process.

Q4331 **Ian C. Lucas:** When the Cambridge Analytica-GSR scandal first broke in 2018—the big part of it—there was a lot of publicity out there saying how dreadful it was, and Mark Zuckerberg appeared before a couple of committees in sackcloth and ashes saying how dreadful it was. Ever since then, our Committee has been trying to get to the bottom of this data transference issue, and I have come to the conclusion that the transfer of data is the modus operandi of Facebook. Far from thinking it is wrong, it is actually what they do. Is that accurate?

Ashkan Soltani: I think that is right. The platform, as you describe it, is simply designed as an API for third parties—advertisers and app developers—to reach consumers and to collect information from them. That two-way transfer of serving content and collecting information is the business model of the platform. It essentially is the platform.

The reason why it is beneficial to them for it to be a web platform is that, when you visit a website with your web browser, your privacy is more protected. Your web browser only reveals certain categories of information that you explicitly disclose to the site, such the IP address or the webpage you came from, which is required. You guys have a strong cookie law; you know how that works.

On the Facebook platform, app developers receive a great deal more information, such as your friend graph and your hometown—information that Facebook chose to make public. Count 1, I believe, of the FTC settlement was that Facebook changed the rules in 2009. Prior to those changes, information that was public was public only to Facebook, meaning that you needed a Facebook account to use the platform. They made those changes to make that information public to any website, including platform apps, in order, I believe, to allow app developers to get more information and to incentivise the creation of apps on their platform.

Q4332 **Ian C. Lucas:** So the exchange of information is not seen as wrong within Facebook but as what they do?

Ashkan Soltani: Absolutely. I interpreted their statements on what is wrong as information going to the wrong actor, not that the transfer was wrong. As we know, the issue is essentially like inviting a friend to a party. If they bring all their friends and you do not monitor the door, you inevitably have a terrible party. I think that is essentially what they meant as wrong.

Q4333 **Clive Efford:** I just wanted to clarify something. You are saying that what Richard Allan said to us was in certain aspects categorically wrong. Do you think that he knew that he was telling us things that were incorrect?

Ashkan Soltani: It is a very nuanced technical issue, so if you describe V1 of the API as something from, say, 2012, after the Facebook

settlement, to 2014, and you exclude whitelisted apps and instant personalisation, then his statements are generally true. But if you include all the carve-outs, and we know the carve-outs to be significant—we know the carve-outs of the whitelisted apps and of API access to be significant—then it was deceitful. It was in fact misrepresenting what the platform can do. As recently as June 2018, using the Blackberry token that *The New York Times* was testing with, which was provided to me, I was able to access user data in lieu of a user's platform settings. That was as recently as this year that these problems existed, but again the description there was that it was for a whitelisted partner or a "soft landing", which I believe was the term they wanted to use for the API transition. There were all these caveats, so the question is, do the exceptions swallow the rule? It is false to make statements to say, categorically, that this information is unavailable when in fact it is.

Q4334 **Clive Efford:** He is a Member of this Parliament—he is a Member of the House of Lords—and it is quite a thing if he has come here and knowingly misinformed this Committee. Are you saying that it is possible that he might not have known what he was saying but should have done if he was coming before this Committee?

Ashkan Soltani: Right, or it is possible that he was trying to generalise and not to be specific about all the hedge cases and exceptions that are present on the platform.

Q4335 **Chair:** Nathan.

Nathaniel Erskine-Smith: You mentioned that Facebook will do the bare minimum. We were in Washington in October of last year, and we asked Facebook as part of our study of commercial sector privacy legislation—we were looking for recommendations—"Would you propose additional rules?", or, "Are you open to new regulation?", and they indicated that the answer was no. Today, they are saying, "We're open to regulation", "We want more regulation", and, "We want you to regulate us—wouldn't that be great?" It is funny how quickly the tune changes once their bottom line is threatened.

I want to be clear specifically about the questions that Ms Stevens was asking Richard Allan. Her concern was, as I understood it, if I use an application, my friends' information is shared regardless of their privacy settings. Richard Allan said, "No, no, that's not the case. They could go in and they could check a box." Are you saying that there is confusion there, that that is not the case?

Ashkan Soltani: There is also confusion there. In the whitelisted apps story that *The New York Times* ran in June, the story about Blackberry, in that case those apps would, for example, have access to friends' information. I actually tweeted a screenshot—

Nathaniel Erskine-Smith: Regardless of what anyone clicked?

Ashkan Soltani: Even if you explicitly went to the platform settings and said, "Do not share my platform." Additionally, in the findings of the FTC,

on testing from 2010 to 2012, the FTC found that if you, for example, marked individual status updates as private, those status updates were shared with apps, or if you marked individual profiles on this as private, those were also shared with apps.

Nathaniel Erskine-Smith: The notices they were sending—to Canadians at least, and maybe others with respect to the Cambridge Analytica information—were that even private messages may have been shared. We didn't get any confirmation from Facebook Canada—the extent of the notices was "may have been", which was striking as well. You were at the FTC during the investigation of Facebook.

Ashkan Soltani: I was, yes.

Nathaniel Erskine-Smith: Was there any indication at the time—I am less familiar with the Facebook consent decree—about the extensive and unrestricted, or fairly unrestricted, sharing of friends' data with developers and app developers? Was that part of the settlement in any way? Was that flagged for them at the time by the FTC? Was that a concern of the FTC?

Ashkan Soltani: The complaint alleged misrepresentation of what Facebook stated in their privacy policy as well as what the platform privacy controls would do. It was not specific to friends' information at that time; it was just all information, including friends' information. In 2013 or 2014, Facebook, in a blog post from Zuck himself, stated, "Your information will not be accessible to apps your friends install." That was in 2014—they made a statement on their blog and then they updated the privacy policy. But based on the *New York Times* reporting and my testing, that was still accessible to certain apps—at least the white-listed apps that we tested.

Q4336 **Paul Farrelly:** Mr Soltani, I was not expecting you to be here, and you clearly were not. I am curious what prompted you to sit in front of all the people here.

Chair: Just to be clear, he walked in freely off the street. We didn't send the Serjeant at Arms to arrest him or anything like that.

Paul Farrelly: What prompted you to come and sit on your own in front of everyone here to give evidence about Facebook? What are your core concerns?

Ashkan Soltani: I was also primary researcher for the *Wall Street Journal* "What They Know" privacy series. I have worked on this issue for the last decade, highlighting the contrasts between statements the companies make and their actual practices. My graduate research was essentially this—highlighting these differences—and I have been working to help structure and pass privacy legislation to address this concern. I was listening to the hearing this morning. I did the same for the congressional hearings in the US. When companies make technically nuanced and perhaps deceitful statements, it kind of gets under my skin.

My role is primarily as a technologist. A lot of what I do is trying to understand technical issues and explain them to policy makers and journalists. Time and again, companies exploit these very technical nuances. This is an incredibly technically adept Committee, but companies still are able to exploit nuances in understanding and make these statements. With the exception of actual audit and investigation, there is very little that you all and the public can do to challenge these statements. That is basically why I came. On these specific issues, I have actually physically tested—or visually tested—them myself, so I know them to be true.

Q4337 **Paul Farrelly:** You used the word "deceitful". We have seen some documents. We have had much to-ing and fro-ing between ourselves and Facebook. From what we have seen, you could use the word "obtrusive" to describe the company, or the word "rapacious". You could use the word "amoral" sometimes, or the words "cavalier" or "contemptuous". How would you best describe the culture at Facebook as you found it?

Ashkan Soltani: I think it is best encapsulated by Mr Zuckerberg's first appearance in the US Senate and then later in the House. The Senate hearing, where he testified most recently, almost seemed like a game of tennis—"You ask me a question and I'm going to answer you in a way that you can't challenge, and I'm going to win that rally." There is that contemptuousness—that ability to feel like the company knows more than all of you and all the policy makers. You might have seen the announcement recently that Facebook is going to create a "Supreme Court" to deal with fake news. Imagine the level of confidence one must have to say, "I've studied this issue for two years and I now feel qualified to create a Supreme Court to deal with fake news issues." On the one hand it speaks to the power of Facebook as a platform, and on the other it speaks to the contempt that the company—at least the senior leadership of the company—has for an existing democratic process and multiple regulatory frameworks.

Q4338 **Paul Farrelly:** Do you think it has grown too big to care? It is so set in its ways—why should it change? It has been phenomenally successful, and the answer, if not to engage in a tennis match, is simply to send in expensive lawyers.

Ashkan Soltani: Yes. If laws are mandated, I think that they will comply with those laws. I think they have a lot of influence, both politically and economically. In the US, a lot of the reticence to pass strong policy has been about killing the golden goose; it is a leading sector in the US economy and there is a lot of worry that regulation will hamper that. I think that is short-sighted. For me, the policy debate is similar to the environmental policy debate 50 years ago, where there was worry about clamping down on companies for emissions and for environmental harm. We found that, actually, by doing so, we incentivised a great deal of innovation around solar energy or renewable fuels. The same is true of this industry. Smart legislation will incentivise innovation in encryption and in privacy protective technologies that allow us to use these services

without suffering harms not just from the companies themselves but from breach and bad actors.

Folks are familiar with usability testing, which is a common term in this space. Platforms employ usability testing to see how their platforms are used. I have been trying to promote the idea of "abusability testing". Platforms invest resources into seeing how their platforms can be abused to harm consumers. I think that smart policy would incentivise that kind of investment, as we have seen that kind of incentivising around cyber security in the last 10 years.

Q4339 **Paul Farrelly:** Richard Allan, who came before us this morning, is a former MP. I have not met anyone who dislikes him. I like him—he is the likeable face of Facebook. His successor as the Member of Parliament for Sheffield Hallam, Nick Clegg, is just about to move to California. He was an MP and became the Deputy Prime Minister. They have bought a former Deputy Prime Minister of the United Kingdom. I just wonder what that says about Facebook.

Chair: Or Nick Clegg.

Paul Farrelly: Can you see whether, after all the recent scandals, whether it has really changed its ways? Is there any evidence?

Ashkan Soltani: I think that there is some evidence that the company is investing in the area. It is not clear whether it is investing enough. They are clearly investing on the lobbying and policy side. A good data point, particularly around the fake news issue, is in the issues and stories surrounding the departure of Alex Stamos, the former CISO. To understand the company culture with Ms Sandberg and Mr Zuckerberg versus, say, the security team, it is problematic to treat it as a monolithic organisation. For example, my understanding is that there are current and former stakeholders at the company that were very invested in these issues, and in fact, the only reason that we know about the fake news issues and the tampering was because of the security and trust and safety teams that essentially—contrary to the senior leadership's will—publicised some hints of it very early on. There are people at the company who care about these issues and there is some investment, but the fact that Alex Stamos just left, or was pushed out, speaks to what their priorities are. They do not currently have a chief information security officer.

Q4340 **Paul Farrelly:** I asked Richard Allan earlier to what extent he believed that Facebook had complied with the FTC orders and he said—I paraphrase—that to his knowledge, fully. Is that your view? The FTC is now looking again.

Ashkan Soltani: The question was whether?

Paul Farrelly: Facebook had complied with the orders given to it by the FTC.

Ashkan Soltani: Have they complied or are they in violation?

Paul Farrelly: Either.

Ashkan Soltani: My personal opinion is that they are in violation of the consent decree. That is my personal opinion. The FTC has publicly confirmed that it is investigating the company. The thing to remember about US regulatory regimes, particularly under privacy, is that essentially, the two hooks are "unfair" or "deceptive". Unfairness is usually a difficult hurdle for privacy-related issues, so it primarily comes down to whether the agency thinks the company made deceptive statements that were in violation of the consent decree with regard to its practices. I am hopeful that around these whitelisted apps and the oversight of apps, particularly the monitoring of API and the knowledge it had regarding what app tokens and app developers were accessing the API, the agency will find that that was negligent. But again, it is purely the fact that the company made statements that it was doing this. Essentially, under the US regime, the more a company says it takes privacy seriously and takes steps to protect privacy, the more hooks the FTC has. If a company says, "We do our best, but we really don't do much," the FTC really does not have a lot of hooks for going after them. It is a little bit different. It is a market policy, essentially.

Q4341 **Paul Farrelly:** So the email evidence that we have, which is also lodged and sealed with the court, may be highly relevant to FTC inquiries?

Ashkan Soltani: I think that would be critical, particularly if there were senior leadership who were aware of the issues and chose not to prioritise them. That would be very telling.

Q4342 **Jo Stevens:** Can I just go back to Richard Allan's evidence and my question to him this morning? I was very specific in asking him whether, if I had set privacy controls, Facebook could override them without my knowing about it, in terms of allowing access to my information through apps and friends, etc. From what you have said in your evidence just now, I am interested in for how long a period that overriding would have been happening. How far back was it, and until how recently, in the worst case scenario?

Ashkan Soltani: There are multiple privacy controls on the platform. Individual profile elements and status updates have individual privacy controls. Then you have a global platform privacy control, where you can turn off app access. In the 2009 to 2012 period, I don't believe platform controls existed at that time point, and the per status update or per profile element privacy controls did not do anything for apps. So if you set your status update to private, an app that you installed would have access to that information even if it were set to private. I believe, subsequent to the FTC order, the company began adding platform controls as well as ensuring that if you set a profile status update to private, an app would not have access to it. However, certain whitelisted apps and apps such as instant personalisation still had access to those in lieu of those settings. That was after 2012. From the testing that I did most recently in 2018, whitelisted apps—the apps we tested for were BlackBerry at the time, but I believe there are other apps that will be highlighted—had access to consumers' information even if they had platform settings turned to off. They had access to friends information as well, so timeline-wise, 2014 is

when Mr Zuckerberg announced that apps would no longer have access to your friends information. There was a grace period of, I think, a year in which they allowed that setting, and then they also gave certain apps a small grace period. Then they allowed whitelisted apps to completely override that setting altogether.

Q4343 **Jo Stevens:** So we are effectively talking about, in the case of whitelisted apps, potentially nine years—nearly a decade—when they have been able to access—

Ashkan Soltani: Friends' information.

Jo Stevens—friends' information, overriding the privacy settings?

Ashkan Soltani: That's right; I believe so, yes.

Q4344 **Jo Stevens:** Right. So that is not accidental, but privacy violation by design, isn't it?

Ashkan Soltani: I think so. The argument I have heard the company make is, "We're allowing app developers to develop apps for us that we would not otherwise make." The statement I have heard is, "We wouldn't build a BlackBerry app. We are not going to invest the resources. There are just not enough BlackBerry users,"—sorry, Canada—"so instead we will let the platform have administrative access to user information as if they were us, and thereby override user settings."

Jo Stevens: Thank you, that is really helpful.

Q4345 **Brendan O'Hara:** There is enormous frustration around this table at what we heard this morning. Certainly for the UK Committee, this was our third attempt to speak to Facebook about this. From your viewing of it this morning, what do you think Facebook wanted to get out of today?

Ashkan Soltani: If I had to summarise, it seemed like it was hopefully to appease you all and not have to call Mr Zuckerberg to testify.

Q4346 **Brendan O'Hara:** And do you think, if you were Mr Zuckerberg, having tuned in, you would be quite happy with what was achieved today?

Ashkan Soltani: I think so. Their tone was, "This is what we do." With the statement about win-win-win, a lot of the undertone of that was that, "This is our business model. Essentially, the exchange of personal information and the use of our platform by third parties is by design, and this is how we make money."

Again, to the earlier question of how I would describe it, there was a question in the Senate hearing in the US where Mr Zuckerberg responded, "Senator, we run ads." Some of you might remember that quote about how they make money. They were like, "You give your product away for free, so how do you make money?", and Zuckerberg responded, "Senator, we run ads." I think the tone was similar—like, "You all need to understand that this platform is monetised by the exchange of personal information, and that's how the platform works, and that's how it's going

to work." I think that was the message—the undertone—of Mr Allan's comments today.

Q4347 **Brendan O'Hara:** And therefore any change to that model of how the business works will be fiercely resisted.

Ashkan Soltani: He also said that this morning when he said, "We will follow the rules as you pass them, if you pass new laws," but he raised his hands and said, "But it's going to have consequences." I thought, again, that was almost like saying, "You might hurt the golden goose. There's a lot of money in this ecosystem." That was a warning.

Q4348 **Brendan O'Hara:** Would it be fair to say that you think Richard Allan was the right person for Facebook to have sent here from their perspective?

Ashkan Soltani: I think so. You all know him. You all trust him.

Chair: I think we will stick with the first one.

Ashkan Soltani: If it were me—I am not sure, but from my understanding of the company—if I were to invite one person, it would be Ms Sandberg. My understanding is that a lot of these decisions are hers. She is the one who makes the monetisation calls and makes the priorities, and that is who I would want to see up here testifying on these business decisions, and specifically on the monetisations and the decisions of what to prioritise.

Q4349 **Brendan O'Hara:** It seems to me, over the months that we have been investigating and speaking directly to Facebook representatives, that everyone knows a bit, but most folk know enough to get by without ever being able to implicate their boss or their company. Is there an individual at Facebook who knows everything?

Ashkan Soltani: Probably not. One of the comments I made earlier regarding— One of the reasons I do not believe the company is able to regulate itself is that for a lot of this period, from say 2010 to 2016 or maybe 2015, the model was "Move fast and break things".

From the technical implementations that I saw regarding the whitelisted partners—the whitelisted apps—they were incredibly hacky and thrown together very haphazardly. It seemed as if a business development person and an engineer implemented a feature quickly. For example, in order to whitelist an app, all they did was say it was pre-installed for all users. That was the workaround, instead of creating a new oversight regime or a new API specifically for those apps. They essentially just added a flag to the database that said it is a pre-installed app, so it gets permissions by default, so it can skip over the consent process.

That is very hacky. That is not very straightforward. That makes it very hard to regulate and it makes it hard to oversee internally. As a result, there are engineers just running in the direction set for them—that leadership has set—and I am not sure that leadership is giving guidance to say, "No, you know what? This is a priority. User privacy is a priority," or, "Data use is a priority."

Q4350 **Brendan O'Hara:** So it is almost like an internal wild west at Facebook.

Ashkan Soltani: I have been told that 2015 and 2016 are worse, right? There are really early news stories about how interns would do these hackathons, which are coding, programming sprints, with someone coming in and programming for a certain length of time. There were news stories about how an intern could come in for a summer hackathon and make changes to the live platform. At that time, the platform was only hundreds of millions of users—it wasn't billions of users. But a user without oversight, without change control and without governance making a change to a code that affects millions of people—that speaks to the culture that was present at the time. That is probably changing, given all the pressure, but it is important to note the roots of the company as the wild wild west.

Q4351 **Brendan O'Hara:** Given that there are representatives of 400 million people sitting around this table, where should we be looking for the unambiguous truth about what Facebook are doing, how they are doing it and how they plan to proceed in the future?

Ashkan Soltani: At least in the UK, you guys are in Europe and I think you have audit rights. The DPAs can do audits of companies. I have worked as a technologist who for that period has seen a great portion of the source code of the company and how the company operates. Even at that time, when it was a tenth of the complexity it is today, it was incredibly difficult to discern how the company was operating. At least you have the ability to go in and challenge the company, as you have done before. The key is to have a compliance regime that has requirements of the company and is verified externally.

One of the other recent news stories has been around the oversight regime that the company employs. Essentially, they have to seek a consent decree and require that the company hire auditors that they pay for, that then do privacy assessments that are self-attested, and that the company then signs off on. Having an auditor you pay, who lives in-house with you and who you control, is not a sufficient auditing scheme. Having a DPA and having the company essentially make attestations and demonstrate to the DPA that they are in compliance with whatever regime you set, is perhaps something you might consider. That is what we do with utilities over time. It is what we do with any large institution. With airlines, we have safety standards they have to meet and then have to demonstrate with an outside auditor.

Q4352 **Chair:** Charlie Angus.

Charlie Angus: I really thank you for this. I may be going off form here in the Committee, but I think I will ask my question to the Chair, as a guest.

I have been a Member of Parliament for 15 years. I have been in all manner of Committee hearings and I have seen positive, negative and reluctant. I have never been in a set of hearings where getting basic answers from people who know better has been so difficult. I have never

been in Committee hearings where people have had to watch testimony that gives us live messages saying, "They're not telling you the truth." I find that very concerning.

Part of my concern is that they know we are generalists. My main job, as a Member of Parliament, is getting Mrs O'Grady's heat turned back on in her flat in the winter. If I do that, I have done my job. So we have to ask extremely precise questions, but the more precise questions we ask, the further away we get from the source, because we get dragged further and further down the well. I put it to you, Chair, that Facebook sent someone very knowledgeable to everyone around this room. I didn't know who Mr Allan was; I didn't know that he was a British parliamentarian. The words we are dealing with were always on their turf, but they today sent someone on our turf, which is the turf of Parliament.

When I see our witness use the words "contempt" and "deceitful", I find that very, very disturbing. So I put it to you, Chair, as I would if we were in the Canadian Parliament, that, given the gravity of the situation and the extraordinary efforts of legislators from around the world who came here, if Mr Allan misrepresented facts, if we were misled—I am not all that concerned about whether it was this point of a detail or that point of a detail; perhaps Mr Soltani could give us the specifics on that—they are now on our turf, and if they are showing contempt and deceit to our Parliaments, that is worth considering and making a finding. I put that to you Chair.

Q4353 **Chair:** That is duly noted. We have recorded what was said, and based on the evidence that we have just heard, we are certainly in a position to follow up on that and go back to Facebook to ask them to explain the discrepancies in the evidence that we have heard. I think we could certainly take that further with regard to Richard Allan's evidence and the misleading nature of some of the answers that he has given.

It also underlines how important it is for us to gain access to written documents and materials from within the company, because then we will have the unambiguous truth. That is why we went to such lengths last week to secure these documents. I must admit that the picture that that paints is much closer to what Mr Soltani has told us than to what Richard Allan had to say this morning.

Ashkan Soltani: I think that is a very astute observation, but one of the challenges in this space with regard to our terms and their terms is that we now have terms that did not exist before—status updates, apps, APIs. Because it is so technical and so nuanced, there is a difficulty in making things crystal clear. Remember, it is not like the life cycle of software is fixed in time now. Code is constantly updated, so you can say "What was your app doing yesterday?" but there were probably three different code updates yesterday. Over the course of the day, it might have done three different things.

Part of the key here, in addition to discovery and having a great deal of documents and auditing, is to have technical resources on hand to you all.

I am sure you do already, but it is about having more technologists—I am biased because I am a technologist—to sit with you, analyse those documents and ask those questions directly. Prior to 2010, the FTC did not have technologists; they would hire experts when a case went to court, but for most matters they did not have in-house technologists. They brought on technologists like myself to help them investigate these matters. I think Congress in the US now has a technical fellowship programme, which is critical to ensuring that when questions are answered precisely, you can get into the technical realm and ask very specific questions that only have one right answer, which they can demonstrate through API documentation, for example.

Chair: I agree with all of that, but part of the problem is that they deliberately send witnesses who are not technically capable of answering those questions and who have plausible deniability. We have seen that time and again throughout this inquiry, where a Facebook witness has not told the truth and we have been told later that they were not sighted on the evidence that they needed to do that.

Q4354 **Giles Watling:** To go back over something that Mr O'Hara touched on earlier, I am interested in the governance side of this. I am looking at it from the outside and going away from specifics here, but it strikes me that this thing has run away. It looks like a feudal autocracy that no one man can control, so us trying to nail down one guy is kind of meaningless, because it has just grown and grown. Would that be an accurate assessment of the situation?

Ashkan Soltani: I think there are unilateral decisions on the platform that have been made. For example, it was not fully implemented but there was a unilateral decision around data brokers: one guy, or maybe the policy team, decided that data purchased from data brokers or data sent to data brokers does not meld with the platform's vision. That was partially a business decision, and I think it was partially an optics and policy decision. Yes, it has grown quite huge, but the majority of shares is maintained by one guy and the policy team is still able to make unilateral decisions, as long as those decisions fall within the bottom line of the way the company monitors—

Q4355 **Giles Watling:** So in your considered opinion, Mr Soltani, we are chasing the right guy here.

Ashkan Soltani: If it were me, I would probably bring in Sheryl Sandberg. You probably wouldn't be able to get him, but— I would see if I could bring in one of the two former CTOs. I would get Alex Stamos or Joe Sullivan up here. They are going to be locked down with lawyers, but they know the technical side of things very well, and the business decisions made by Sheryl—I think those would help. So maybe three guys, or three guys and a woman.

Q4356 **Giles Watling:** That is really interesting to know. Thank you for those names—that helps hugely. With your background in privacy and ID, do you think there is another big breach of data privacy coming up that we

need to be looking out for?

Ashkan Soltani: Inevitably. The question is always, when is the next Exxon Valdez that is large enough to cause a response? We still haven't seen one. Even the last Facebook breach—the token breach—wasn't enough to tip the scales. You could access users' profiles using this token. It wasn't a Cambridge Analytica-type breach; it was a full website breach that was knowingly exploited. Either it becomes the status quo, which would be really sad, or hopefully one will finally cause people to act. Most likely, if I had to venture a guess, in the US—do you guys know the video privacy law in the US?

Giles Watling *indicated dissent.*

Ashkan Soltani: The VPPA was brought about because Members of Congress had their information affected. When there is a privacy scandal in one of the regulatory agencies or oversight bodies, I think that is when we will see a response. There hasn't been one large enough yet over the last 12 years to have anyone act. In the US, we will probably get a privacy law in the next Congress—that is my guess—and it will be some combination of an Honest Ads Act and a light-consent privacy law that pre-empts the state laws. Because of the pressure, it will be a lighter-touch law than the California law.

Q4357 **Giles Watling:** In the meantime, you think it will be pretty much a case of caveat emptor?

Ashkan Soltani: I think so.

Giles Watling: Thank you, Mr Soltani, for being a surprise guest at the party.

Ashkan Soltani: Thank you for having me.

Q4358 **Rebecca Pow:** I have a very small question that touches on something that my colleague from Singapore mentioned this morning. Lord Allan admitted openly that Facebook had made mistakes—he was quite open about that—particularly in taking down hate mail, but he was still convinced that Facebook is the right body to be in charge of taking down hate crimes. I wonder what your views are on that.

Ashkan Soltani: I think it is incredibly challenging. One of the questions is about business models, and the business models have two components. The business model is to monetise data, as we have discussed here, but the company line is to connect people—Facebook's mission is to connect people. One question is, should we be that connected? There is a great deal of tolerance in the world because there is practical obscurity. You and I might have very different views, but I'm not exposed to all your views so I might not have an opinion about them, and nor do I feel like I need to impose mine on you. Facebook is actively connecting people for the purpose of driving engagement, and what drives more engagement than controversial content? This business model of connecting people and driving engagement from controversial content has caused a lot of contention on the platform. That is something we should question.

Technically, the person to best filter that content is the platform, I think, but I am not sure the policy decisions about how to filter content should be made by the platform since its incentives are to drive engagement and connect people who would otherwise not have been connected.

Q4359 **Rebecca Pow:** You could semi-solve their problems by employing a great many more people looking for this.

Ashkan Soltani: But I think articulation of the policy is critical. Rather than selective enforcement of the policy, they should articulate the specific policies. The big thing in the US is the Honest Ads Act—this was discussed in this Committee—and political advertising having to be registered and disclosed so there is some transparency around it. Then the question becomes, what is political advertising? There are issue-based ads, for example. If you advertise about a woman's issue or a health issue, that becomes non-political. It becomes an issue and not necessarily subject. Having some kind of democratically elected body decide what the policies should be—as most of society has functioned until now—and then have a company follow those polices seems like the smart idea to me.

Q4360 **Ian C. Lucas:** Can I ask you about the FTC? You worked for the FTC. There was some questioning in the Senate about the FTC and the GSR breach that I would like to ask you about. You may have heard me discussing with the Information Commissioner the reporting of data breaches.

Ashkan Soltani: I did.

Q4361 **Ian C. Lucas:** In the UK at that time, there was no requirement for the data breach to be reported to the Information Commissioner. What was the legal position in the United States?

Ashkan Soltani: I don't think there is a federal data breach reporting requirement, but California has a data breach reporting requirement. It has a particular standard for what constitutes a data breach, but California law requires that companies disclose data breaches.

Q4362 **Ian C. Lucas:** There was an interesting question by Senator Nelson to Mark Zuckerberg—he actually appeared before the Senate. The senator asked, "Did anybody notify the FTC?" Mark Zuckerberg said, "No, senator, for the same reason—that we'd considered it a closed case." It appeared that the issue in the mind of the senator arose. You do not know whether there was a federal legal requirement.

Ashkan Soltani: I don't believe there was.

Q4363 **Ian C. Lucas:** Okay. Now, you have also heard me ask about the date of the knowledge of Facebook on the breach, and we are going to get clarification from the Information Commissioner on that. Mr Zuckerberg on a number of occasions said to the Senate that Facebook became aware of the breach in 2015 as a result of a *Guardian* article. We are looking at whether Facebook may have heard about that earlier. Bearing in mind the seriousness of the breach, if Facebook were aware of the breach at an earlier time, what would be the appropriate step for the company to take

in those circumstances?

Ashkan Soltani: I testified to the hearing with Aleksandr Kogan, the developer. The response was that—Mr Zuckerberg's response has been that they sent their lawyers essentially to convince the company to delete all copies of the data and not share that information.

Q4364 **Ian C. Lucas:** This was in 2018.

Ashkan Soltani: I believe so, or maybe 2017. I think that is their response.

Q4365 **Ian C. Lucas:** But in 2015, they say that they did not take any action because they considered it a closed case. What would have been the right approach for Facebook to have taken when they were notified of the data breach? Within that business, what would have been the appropriate step?

Ashkan Soltani: Typically, with a data breach you notify the affected customers and try to ensure an ordered deletion of those records and you look at the downstream dissemination of that information. They would probably have looked to see how that information was used. I believe that they did not consider the first and latter stuff. There was no notification and no downstream investigation. There was simply a request by the accessing party to delete that information and sign a contractual requirement.

Q4366 **Ian C. Lucas:** That step appears to have been in response to the publicity.

Ashkan Soltani: That's right.

Q4367 **Ian C. Lucas:** So there is no evidence of Facebook actually taking any action until there was publicity concerning—

Ashkan Soltani: That's right. The thing to note is that, from the early comments and responses from the company, I do not think the company considered it a breach. They considered it to be a developer with valid access to the API violating the terms of use of that data. They did not consider that a data breach; they considered it a terms of use violation that they investigated. That is a different terminology and a different mindset.

Again, going back to the earlier point, the ecosystem is about the exchange of data. The flow of data in and of itself is not problematic; the use outside of the terms of use is problematic. We have seen this in multiple examples with the company. There was an early case in 2010 where the company sued another company, Power Ventures, for scraping users' information and using it. That was a competitive issue. They did not want this other company to have users' information outside of their platform and their control. They take action and they monitor the platform for abuse where it has a strong business interest, but when it is in line with the business interest, I do not think it necessarily becomes a problem.

Q4368 **Ian C. Lucas:** Thank you very much. Just one final point: Mark

Zuckerberg repeatedly told the Senate that this breach took place in 2015. I think that was in December 2015, so if it took place in 2014, he would have lied to the Senate.

Ashkan Soltani: *indicated assent.*

Q4369 **Paul Farrelly:** Going back to previous evidence, to paraphrase Dr Kogan, he told us that he did not consider that Facebook had any terms or conditions because it never enforced them, so it did not cross his mind.

Ashkan Soltani: That's right.

Q4370 **Paul Farrelly:** The overall tenor—or to use a Californian word, vibe—that I got from this morning was, "We're a social site, so whether you are a developer or a user, it cannot be one-way traffic. You have to give something back to the community, and that means all the personal data that you have, regardless of whether you are paying to run ads, or you are the eyeballs that are there to enable us to sell ads. That's the way we do business, and that's part of the deal." That was the impression that I got from his evidence.

Ashkan Soltani: The hard truth is that on one hand, it is a free service. The comment is, "The service is free for users, Senator; we sell ads. It is a free service. There are not any anti-competition issues, because it is free. You do not need to regulate it. There is no cost; it is free." On one hand, that is the line. On the other hand, there is this assumption that people understand it is a tit-for-tat exchange of personal information, and I am not sure it can be both. It is either free—there is an exchange of information that is non-monetary—or it is an exchange of personal information that is given to the platform, mined, and then resold to or reused by third-party developers to develop apps, or resold to advertisers to advertise with. It is one of those two things.

The California privacy Act was initially similar to GDPR, in that if a user opted out from the sale or sharing of their information, companies were prohibited from denying them access to the site or service. You could opt out, but still use the service. When it went from a ballot initiative to an Assembly Bill, there were some compromises made, and one of the compromises was that companies could charge users who opt out for the service. However, the key provision there that helps is that companies can only charge users the value they extract from their information, and it cannot be usurious or exploitative. That starts putting the onus on companies such as Facebook to articulate what the value of personal information is to users. You can have a free service like the *Washington Post*: "You can have the free version if you let us track you, or you can pay $5 or $9 per month to use the service." That articulation can solve this dilemma, which is "It's a free service, but"—wink, wink—"we believe users understand that we are selling their information, and in fact we are selling it to advertisers and app developers."

Q4371 **Paul Farrelly:** To pick up on your look-forward to an honest ads Act in the States, we have been looking at political advertising, misinformation and manipulation, and the company has said that it is taking steps to drive

that out or see what happens. Our colleagues from Singapore this morning highlighted the unwillingness of Facebook to take down hate speech, which could have had appalling social effects in difficult times, and the answers that came back from Facebook's automated platform when that was reported were very similar to reports I have made of ads that are fraudulent. They come back and they say, "While this ad does not breach our policy"—how can it not? It is fraudulent—"we understand that you do not want to see this, and you will not see this." Lots of other people will still see it, of course. At the end of the day, with that attitude towards complaints, you wonder whether it really will take legal responsibilities and liabilities, and therefore a change in the law, to make Facebook pay more than lip service to complaints in different spheres.

Ashkan Soltani: There are two responses that make me chuckle in this space. I also worked on the White House big data report and the AI report for the last White House. The response to this is that we are just going to create a list of words that we censor for. We are going to create a list of words and we are going to throw AI at the problem and it is going to be solved. My background part of the work was security and anti-spam perimeter protection, and if we know anything about adversarial attacks, it is that adversaries will always find ways to innovate and you need a lot of human investment and control and collaborative filtering, which is what you are describing, to make sure that input from people that have a problem with content is propagated so that other people don't see it. You need a lot more steps there than just paying lip service by creating a list of problematic words in whatever language and this vague notion of AI. The AI assumption is going to cause more problems than it will solve.

Q4372 **Chair:** Bob Zimmer.

Bob Zimmer: It came to me as you were talking that you are obviously an expert in the field. One thing we have asked of different people in Canada or here on foreign influence in elections, which is my big concern, is how you would fix that. The easiest way that I see to tackle it—and it is not easy by any means, but I see it as the only way to really deal with the problem—is to attach an ID to every individual, like in Estonia essentially. So when you are on a platform, it is clear that it is Bob Zimmer and I am buying the ad to run in a campaign, or I am the CEO of company X and I am buying the ad to run. If I am in Russia, and I am Yuri, I still show up on Facebook, because I am Yuri buying an ad to run against Bob Zimmer in Canada. I see that as the only solution. What is your suggestion?

Ashkan Soltani: It is an incredibly difficult problem. I helped to organise a workshop last year on this issue and invited all the platforms as well. It is not just buying. The social problem is, first, the propagation of fake information but, second, the use of fake accounts to propagate opinions or real information that is biased, as well as the convincing of real users to propagate information. The latter two would not be solved by a real ID policy. I have issues with essentially incentivising companies whose business it is to know you to then better know you by verifying your identification. It is a double-edged sword to say that we think fake news is a problem, advertisers, so make sure you get—

Bob Zimmer: Is it something that we need to take up? The classic example is that little blue check mark on Twitter or Facebook. Is it something that the Government have to apply? We have money that has certain things within it to keep it secure so that it cannot be copied easily. Is that something that the Government need to step in and do?

Ashkan Soltani: Identity verification is one proposed solution. I am not a huge fan. I think anonymous and pseudonymous speech is actually important online. I think the key is around engagement in business models, honestly. There are different technical approaches, one of which is that you could consider slow news. The issue is not with hateful speech or fake content on a small scale; it is when it reaches a large audience.

The issue that companies have had is that they say that the volume of content created online is beyond what we could manually filter and curate. One response could be that you curate and filter only the trending articles. You slow things down. If you see things rapidly disseminating that are suspicious, you slow them down and then you have a human verify or fact check. Then you have specific policies and guidelines about how that fact-checking and verification happens and how content gets filtered. You have transparency reports that speak to how that content was filtered and verified and then you have a package. That will solve 90%. We still get spam from time to time. We have not filtered all spam, but we have done a good job of taking out the problematic spam. I think it is the same issue.

There is a third piece, which not a lot of people are talking about, which is that there is the concern of external meddling and external influence by actors to meddle with elections, but the question of the platforms themselves being able to influence elections or influence outcomes is another one. I do not want to sound paranoid. One recent observation I made at a Chatham House-rules conference was that one platform was using automated means to filter content, and as a result was filtering a disproportionate amount of conservative content. There happened to be more conservative fake news ads, so their system was taking them down. As a result, so as not to seem biased, it then promoted more conservative content on its homepage, independent of the actual distribution of conservative versus liberal content.

That subtly influences outcomes, but there is no disclosure requirement and no requirement for companies to describe their algorithmic biases and how they promote content. That is another piece of not just external factors, but the power that search engines and newsfeeds have.

Q4373 **Chair:** Thank you. I have just a couple of questions to finish off. We asked Richard Allan earlier about how the reciprocity policies work on Facebook. He was typically pretty vague about that. From your work with the FTC and the White House, what insights do you have on that? It seems to us like there is a basic deal with developers, which is that they give all their user data in return for accessing Facebook, or for using particular apps on Facebook. There is a data exchange as part of the transaction.

Ashkan Soltani: That is right. We heard some comments about preferred partners—certain partners that give more value. It is true that certain concessions and considerations will be made for companies that will drive a larger amount of content to you or with whom you have some existing business relationship. In the Valley it is often that, if your investor also invests in another set of companies, you give those companies some preferred deals and partnerships. That often involves access to user data.

Q4374 **Chair:** Are whitelisted organisations on Facebook based on that value of exchange? The more valuable you are to Facebook, the more likely you are to be whitelisted?

Ashkan Soltani: I believe so.

Q4375 **Chair:** Do you think that that includes ad buying as well as data exchange?

Ashkan Soltani: I am not sure if it includes value so much. I think that, to some degree, it is about engagement and users; I think the ultimate is how many users and how much engagement something will drive. In the *New York Times*' reporting, there were certain large ad purchasers and automobile industry purchasers that were getting preferred access to the platform. It was not clear whether that was because they had large ad buys and had a lot of money to throw to the platform or because they had a large amount of engagement and users that they could drive to the platform.

At the end of the day, I think it is about relationships and influence. Knowing someone who knows someone on this Committee makes me more likely to be able to come here, right? I think that the same is true for the platform relationships. If my ad guy pays a lot of money to the Facebook sales guy, it is more likely that I will get a meeting with the engineering team to create a custom API for my platform.

Q4376 **Chair:** So there is a value exchange of sorts, because you are saying that companies that end up being whitelisted and having preferential access to data are either potentially giving Facebook a lot of money by buying a lot of ads or they are giving it a lot of data because they are bringing a lot of users with them, which is of huge value to Facebook as well, or they are doing both.

Ashkan Soltani: Right. Or they are dragging a lot of eyeballs—engagement.

Q4377 **Chair:** So there is a commercial value to Facebook of that relationship, and as a consequence of that commercial value, that third party gets preferential access to the site?

Ashkan Soltani: That is right. Just from a simple, really basic numbers game, if you run a website and tomorrow decide you want to create a Facebook app, it's going to cost some amount of dollars, depending on the scale of your app—say $100,000 or $200,000.

It is worth it for you to invest that initial development resource—as well as the ongoing cost of maintaining and hosting that service, to be on the platform—and so you do it. At the very least, that development number is the initial investment, and that is the value exchange for the company.

Q4378 **Chair:** Do you think that what has happened since 2014-15 is that, if you are a big player, you have found the backdoor into the data? You have bypassed the systems, you get full privileged access to all the data because you are a big player and you bring a lot of eyeballs and a lot of data to the party, and you are potentially spending a lot of money?

Ashkan Soltani: It is possible, yes.

Q4379 **Chair:** If you are a relatively small developer, though, you are going to get squeezed out of that market, aren't you?

Ashkan Soltani: That is right; you just follow the standard API and you are restricted from access.

Q4380 **Chair:** Do you think there is a concern, then, that these changes in policy have been detrimental to lots of developers creating apps and tools, which used to run on Facebook successfully, but were effectively pushed off the platform?

Ashkan Soltani: I think that is an important question. For example, to the earlier question about friends of the user's data, we know that there was the initial announcement, there was a grace period and then there was a selective grace period for a set number of companies that had rolling dates, and for some companies it was never cut off. The question is, how were those decisions made? It would be interesting to know. Was there a pattern in who the extension was given to? Most likely, if you are a small app developer, you are not going to get an extension, but if you are a significant player on the platform, either by your users or, perhaps, by your ad spend, you might get preferential access and the delay extended.

Q4381 **Chair:** Given the scale of the business—that it has almost monopolistic powers as a social network—that would seem to be massively anti-competitive. It would be an abuse of power on their part, to behave in that way.

Ashkan Soltani: Absolutely. You guys have not brought up the VPN issue, but that is another area.

Chair: That is another example of privileged access to users' data without their consent.

Ashkan Soltani: That is right.

Chair: Another one.

Ashkan Soltani: That is by Facebook, though. Facebook purchased a VPN provider and they admitted in public statements the fact that they monitored users' use of this VPN, to see which apps are popular with users, in order to acquire those apps or to build a competitor.

Q4382 **Chair:** So many of these issues seem so important to the inquiry we have been running—user data still being acquired without user knowledge or consent on a big scale. There is also this other issue, which has come to our attention, of Facebook's aggressive policies being used to do deals with big commercial partners—people who are valuable to the company—and pushing off smaller developers with much poorer deals and no real opportunity to appeal that. On both of those things, in terms of GDPR and data protection rules, there seems to be a question of the legality of it, because it certainly does not pass the informed consent test. You questioned the commercial practices and the impact that has on developers, if an arbitrary decision is being made that favours them commercially. These are important issues for us and, again, they are important issues behind the reasons why the Six4Three papers need to be in the public domain, so that people can get a much better insight into some of these issues and Facebook can respond to the specifics, rather than our questions.

Ashkan Soltani: I think that is critical, particularly for other regulators, as well.

Chair: Thank you very much. It has been a great way to finish the session. You have provided a lot interesting light on to the fog of Facebook's evidence.

Ashkan Soltani: Thank you so much for having me. I wasn't expecting it.

[Applause.]

Chair: Thank you.