

Digital, Culture, Media and Sport Committee

Oral evidence: Fake News, HC 363

Wednesday 21 March 2018

Ordered by the House of Commons to be published on 21 March 2018.

Watch the meeting

Members present: Damian Collins (Chair); Julie Elliott; Simon Hart; Julian Knight; Ian C. Lucas; Christian Matheson; Brendan O'Hara; Rebecca Pow; Jo Stevens.

Questions 1187-1270

Witness

[I](#): Sandy Parakilas, former Facebook operations manager. [Via video-link].

Examination of witness

Witness: Sandy Parakilas.

Q1187 **Chair:** Good afternoon, and welcome to this further session of the Digital, Culture, Media and Sport Select Committee on our inquiry into disinformation and fake news. We are delighted to welcome Sandy Parakilas to give evidence this afternoon. He is doing so by video link from San Francisco. If for any reason there is a technical glitch in the transmission, we will call a brief pause in the proceedings while that is corrected, but hopefully that will not be necessary.

Sandy, for the benefit of the record and the Committee, would you give us a brief description of your role at Facebook and how long you were working there for?

Sandy Parakilas: I worked at Facebook in 2011 and 2012 for a total of 16 months. I was a platform operations manager, and the responsibilities that I had were over policy and compliance for Facebook apps and data protection, protecting the data of users who use Facebook apps. Those were my primary responsibilities.

Q1188 **Chair:** There has been considerable interest in the last few days in particular, but it was also of interest to the Committee when we took evidence from Facebook at our hearing in Washington last month, over the safeguards in place that protect Facebook users' data. Perhaps you could explain a little bit about the way those safeguards worked when you were at Facebook.

Sandy Parakilas: Perhaps I can start by giving a brief description of how Facebook Platform, which is what apps use, works, because it would be helpful in understanding this. When you connect to an app, you being a user of Facebook, and that app is connected to Facebook there are a number of categories of these apps, including games, surveys and various other types. Facebook asks you, the user, for permission to give the developer, the person who made the app, certain kinds of information from your Facebook account, and once you agree Facebook passes that data from Facebook servers to the developer. You then give the developer access to your name, a list of the pages that you have liked and access to your photos, for example.

The important thing to note here is that once the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data. To prevent abuse of the data once developers had it, Facebook created a set of platform policies—rules, essentially—that forbade certain kinds of activity, for example selling data or passing data to an ad network or a data broker.

However, Facebook had very few ways of either discovering abuse once data had been passed or enforcing on abuse once it was discovered. In the event that Facebook received a report of a data violation, it could do one of four things: it could call up the developer and demand to know



HOUSE OF COMMONS

what they were doing with the data; it could demand an audit of the developer's application, their data storage, and that was a right that was granted to Facebook in these policies, the platform policies; it could delete the app and potentially ban the developer from using Facebook Platform or even using other Facebook products such as advertising; or it could sue the developer and pursue that app. Those are the only four things that Facebook could do once it had determined that the developer had been in breach of those policies.

In terms of the frequency of the use of those four means, I can tell you that in my experience, during my 16 months in that role at Facebook, I do not remember a single physical audit of a developer's storage. I do not remember that happening once. There were only a handful of lawsuits and bans. Those were both quite rare. Mostly what I did was call developers and threaten to do other things, basically saying that they needed to follow the policies. That was effectively the main enforcing mechanism during my time.

The other thing to note is that Facebook had relatively low detection of policy violations and most of the reports that it got about policy violations were either from the press or from other developers who were competitors of a particular company and they would call up or talk to someone at Facebook and say, "I think this person is doing X, Y and Z," and they were doing that largely for competitive reasons.

Q1189 Chair: What more do you think Facebook could have done at that time to track what was happening to user data that had been given to developers?

Sandy Parakilas: I think one of the key things to understand is that if you do not have access to the developer's data storage, which you would not have unless you sued them or they granted it to you willingly, then you cannot really see what data they have, because what is exposed to the public view is not indicative.

I will give you an example. If you think about Cambridge Analytica, there was allegedly Facebook data that was passed to Cambridge Analytica. Cambridge Analytica then allegedly used that Facebook data and other data to create user profiles, which included things like estimates of how people would vote on particular issues, and those voter profiles did not include the source data. They were informed by the source data, but they did not include the source data. Even if you had some kind of digital watermark in the data, by the time you get to the next step you would no longer easily be able to tell where the data had come from.

It gets even more difficult because then those voter profiles are not what is exposed to the public; those voter profiles were then allegedly used to purchase Facebook and other advertising. What is visible to the public is an ad with targeting that is also not visible to the public. There are many, many steps between the receipt of data and what you can actually see without some legal avenue to get into the source files of a particular



HOUSE OF COMMONS

developer. It is very hard, and I would argue that the real challenge here is that Facebook was allowing developers to access the data of people who had not explicitly authorised that friend permission.

Q1190 **Chair:** Exactly. Once the data has gone, once the developer has been granted access to the data, the benefit they get from that is theirs forever, really? There is effectively practically nothing you can do to recover the data, and even if you could the developer would continue to benefit from having had access to that data?

Sandy Parakilas: It is incredibly difficult. Frankly, even if you do conduct a physical audit, it is very difficult to prove that the developer has not hidden the data on some secret hard drive in their closet or something. You are basically reliant on their word.

Q1191 **Chair:** Did people raise concerns at the time that Facebook user data was not safe and that it could be gathered by developers in this way?

Sandy Parakilas: Yes. I was one of the people raising concerns. There was a lot of press at the time suggesting that this was potentially violating people's privacy and that there were some real concerns here. It was a known issue. What has changed is that people now realise how many things you can do with large amounts of data and so now they are connecting those two dots and we have the current scandal.

Q1192 **Chair:** How did you raise those concerns within the company?

Sandy Parakilas: One of the things I did was make a map of the various data vulnerabilities of Facebook Platform, which was the only way you could get data on Facebook users out of Facebook other than using ad targeting, which does not give you the data per se. I made a map of all the vulnerabilities, I included lists of bad actors and potential bad actors, which included foreign-state actors, data brokers, I said, "Listen, here are some of the things that Facebook are doing, and here are some of the areas where the company is still exposed and user data is still at risk," and I shared that around with a number of people in the company at the time.

Q1193 **Chair:** Are some of the people you shared that with still at the company today? Are there people at the company today who would have been well aware of the concerns that you raised?

Sandy Parakilas: Yes, some of the executives I shared the presentation with are still at the company today.

Q1194 **Chair:** Are you able to say who?

Sandy Parakilas: It was senior executives in charge of Facebook Platform and people in charge of privacy.

Q1195 **Chair:** Yes, but you cannot name who they were?

Sandy Parakilas: I can follow up with you after if that is a specific—



HOUSE OF COMMONS

Q1196 **Chair:** Do you think Mark Zuckerberg would have been aware of the concerns that you and others were raising?

Sandy Parakilas: I do not know that Mark Zuckerberg would have been aware specifically of what I said, but I think it was known and understood both internally and externally that there was risk with respect to the way that Facebook Platform was handling data. There were concerns from the press and the public. I do not think it was a secret that this was a problem.

Q1197 **Chair:** Yes, although Facebook users were probably not aware?

Sandy Parakilas: I think the problem is that Facebook users may have understood in theory that there were privacy concerns but they did not know how much of their data was being sent to developers whom they had no relationship with. Keep in mind that in the case of the survey that Aleksandr Kogan gave, he only got 270,000 people to download his another place, but because he had friend permissions he got Facebook data on, I believe, either 30 million or 50 million additional people who were friends of those 270,000. If you do the maths, the average Facebook user has something like 200 friends; 270,000 times 200 gets 50 million.

Q1198 **Chair:** Do you still have the map document that you described? Is that something you could share with the Committee?

Sandy Parakilas: No, I do not.

Q1199 **Chair:** In terms of the warnings that were given, was there a written document and presentation that was shown to people, or was it just something that people discussed?

Sandy Parakilas: It was a PowerPoint presentation.

Q1200 **Chair:** Thank you. Also, you said that when you were there you were involved in a few cases of action being taken against developers for breaching Facebook's terms for using data. In those cases were Facebook users notified that their data had been inappropriately accessed, used and exploited by a developer?

Sandy Parakilas: No, not to my knowledge.

Q1201 **Chair:** There was no policy of informing Facebook users that their data had been breached in some way?

Sandy Parakilas: Not to my knowledge. I do not believe that there was.

Q1202 **Chair:** Finally from me, before I bring in other members of the Committee, you touched earlier on the friend permission, and one of the things that concerned us about Aleksandr Kogan's work was that he was able to access friends' data, not just the people who completed the survey. Could you just explain a little bit more about how that permission worked?



HOUSE OF COMMONS

Sandy Parakilas: Friend permissions were a set of permissions on the platform that were active from 2010 until 2014, when the company turned them off, although some apps continued to have access to those permissions into 2015. The best way to describe it is that they give the developer the ability to access data related to the user's friends. I will give you an example. If person A agrees to use an app that asks for friend permission and person A is friends in Facebook with person B, then the app developer gets not only the data that person A agreed to give, but the data for person B, subject to the constraints of the permissions that person A agreed to on behalf of person B. I know that is complicated, but basically what it means is that if I use a Facebook app and I agree to give permission for my friends' data, and if you are one of my friends, the developer gets your data as well.

There are a couple of important constraints to understand. I do not remember the specifics, but there was language in Facebook's terms that definitely described this process, and Facebook has relied on that to say that people had given consent to the terms. Then, separately, they were settings that would enable you to turn off the ability of a friend to give your data on your behalf. The concern I had with both of those is that, first, no one reads the terms and, secondly, the setting was opt-in, meaning that you had to know that the setting existed, go to it and change the setting. I am pretty sure that if you talk to virtually all of the 50 million people who were impacted by this Cambridge Analytica issue, I am quite certain that none, or very few, would have any idea that their data had been shared with Kogan, let alone with Cambridge Analytica.

Q1203 Chair: Was this a continuous flow of data? Once you had completed the survey and given permission for your data to be accessed, and that of your friends, that was not just the data that was accumulated up to that point but any future data that was accumulated as well?

Sandy Parakilas: There were different permissions that enabled different access points. I do not remember all of the technical specifics here, so I do not want to give an incredibly specific answer, but for some period of time on Facebook Platform you were able as a developer to pool data at multiple times moving forward, and that makes sense, in the sense that you can imagine—I do not know if any of you played Farmville or used one of the other Facebook apps that were really popular in 2010, 2011 and 2012—they would need to see your friends and see some of your social activity to be able to inform some of the things that were happening in the app. It provided functionality to developers, but it could also be abused.

Chair: Let me bring in Chris Matheson.

Q1204 Christian Matheson: Thank you, Chair. Hello Sandy; I do not know if it is good morning or good afternoon there, but it is good to speak to you. In your time there, or to the best of your knowledge, has Facebook ever been hacked successfully?



Sandy Parakilas: I didn't work on security, which was a different team, which was focused on technical security, so I don't think I am really qualified to answer that question.

Q1205 **Christian Matheson:** Are you aware of any attempted hackings.

Sandy Parakilas: I am not aware of technical data breaches, meaning systems being compromised.

Q1206 **Christian Matheson:** I am guessing they have very strong security provisions in place to prevent hacking.

Sandy Parakilas: The security team at Facebook is very, very good. They have very, very good engineers working on technical security, and it is a best-in-class company for technical security. However, the concern I had was that they had built this platform that would allow people to get all of this data on people who had not really explicitly authorised—and it was personally identifiable data—it had your name in some cases and your email address in some cases, and in some cases it could include your private messages. It was really personal data, and they basically allowed that to leave Facebook's servers intentionally, and then there were not any controls once the data had left to ensure that it was being used in an appropriate way. That was my concern.

Q1207 **Christian Matheson:** You have almost anticipated my next question, because privacy and security are not the same things but they have a similar aspect to them, and it seems that you are telling the Committee that they take security very seriously, defending their own servers from external encroachment and attack, but that privacy is not given necessarily the same priority, or they do not seem to have an understanding that it has the same priority. Is that fair?

Sandy Parakilas: Yes, I think that is fair. If what you are saying is that they take the technical security of their systems very seriously, then yes, they absolutely do. And then you are also saying that they do not take seriously ensuring that people's data is protected overall, including outside their systems, and I would agree that they do not take that seriously enough.

Q1208 **Julian Knight:** Sandy, it is very interesting evidence that you have given to date, and I think that was a very telling point that you made at the end there: effectively, the dichotomy between their approach to preventing hacking, preventing a technical breach, and their approach to the data and the use of that data when it is acquired by a third party. Do you think that this looseness of personal data was almost seen as a unique selling point of Facebook, something that was actually a part of their marketing strategy?

Sandy Parakilas: The way I would characterise it is that the unofficial motto of Facebook is, "Move fast and break things". Most of the goals of the company were around growth in the number of people who use the service. At the time on the platform team it was about growth in apps,



HOUSE OF COMMONS

growth in developers. It was very focused on either building things very quickly, getting lots of people to use the service, or getting developers to build lots of applications that would then get lots of people to use the service.

I think it is worth bearing in mind that some of the most popular apps had hundreds of millions of users. They had huge scale. I cannot remember specific apps, but I believe that some of those apps asked for friend permissions, so a huge amount of data was being pooled out of Facebook as a result. The volume of data that was being pooled as a result of that permission was a concern to me. I am not sure I answered your question exactly.

Q1209 Julian Knight: No, I think you have answered it mainly. It seems to me that the analogy would be almost like a frontier town in the wild west and this idea of, "Build it; knock it down again; build it again; build it better; bring in this growth," all focused on that. Would that be a fair analogy for the way in which Facebook has approached data?

Sandy Parakilas: I think that in its approach to regulating data the wild west is an appropriate analogy. Going back to your original question, you asked, "Was it a selling point?" I would describe it more as the ability to access a tremendous amount of data was a selling point to developers and Facebook wanted a lot of developers to build a lot of applications because they would draw more people to use Facebook more and more. Developers would for free build features that Facebook did not have itself, and the way that it got developers to want to go through Facebook was, first, they would give the huge audience of Facebook to the developer so you could get a lot of users very quickly and, secondly, you could get a ton of data from Facebook to build your application and understand those users.

Q1210 Julian Knight: Were developers using this data exclusively to target advertising?

Sandy Parakilas: That is a great question. There were a number of rules in the policies that dealt with attempting to prevent developers from using the data targeting advertising. An ad network could not be a developer; developers were not allowed to pass data to ad networks. There were a number of rules that stated quite explicitly that you could not use data from Facebook Platform for the purpose of targeting ads.

However, as I said earlier, there was very little detection or enforcement, and it is very difficult to tell how an ad is being targeted, particularly if data is taken, then joined with other data, manipulated in some way and then used in some other platform to target ads. Without a physical audit, which you would probably need a lawsuit to get, it would be very difficult to understand if that has happened or not.

Q1211 Julian Knight: My impression is that there may have been effectively a rule that said that this was not to be used in order to target advertising



HOUSE OF COMMONS

but you are saying in the reality that effectively that was a rule that was never really particularly enforced. Is that right?

Sandy Parakilas: I would not say it was never enforced, but I do not remember during my tenure a specific instance of it being enforced. It may very well have been enforced a year before, after or at the same time that I was there, but it was entirely reliant on the rule. There was very little way to tell if someone was in fact taking this data from Facebook Platform and using it for a bad purpose. They would have to get a report sometime and then respond to that report.

Q1212 **Julian Knight:** My final question is this: In an ideal world, bearing in mind that this is a business that is trying to grow and provide what it believes to be a service that people want in many respects, what do you think Facebook should have done in order to better safeguard data?

Sandy Parakilas: The first thing that they needed to do, which they finally did in 2014, is turn off friend permissions. You can now no longer get data from someone who has not explicitly authorised the application. That is a good thing. I think the practices of Facebook in that period, 2010 to 2014, were in my opinion far outside the bounds of what should have been allowed. I believe the company's practices in Facebook Platform specifically have become much better. Since I have not worked in the company for a number of years, I cannot speak to what the issues are now in terms of the structure of the platform, but what I will say is that I was very disappointed to see that they allowed the Cambridge Analytica situation to play out for more than two years after they had evidently received certification from Cambridge Analytica and Kogan that the data had been deleted despite multiple media reports saying that Cambridge Analytica was using Facebook data, which they did not follow up. That is a really big concern to me.

I guess my concern is mostly around the enforcement front and the auditing front. If they are allowing data to be passed to third parties—sensitive, personally identifiable data—they must have much stronger enforcement to ensure that developers do not use that data. I think it must be much more proactive about suing developers if they are going to continue to allow this to happen and it must be much more proactive about auditing and using procedures to actually go in to check and inspect what developers are doing with that data.

Q1213 **Brendan O'Hara:** I have just a couple of questions. Going back to something you mentioned earlier about data brokers, what are data brokers, how do they operate, and what was their relationship with Facebook?

Sandy Parakilas: That is a great question. Data brokers are firms that aggregate sets of data and sell that data, and in many cases they are aggregating personally identifiable information, so it is actually your name, your address and other information about you, the individual. It is



HOUSE OF COMMONS

very different in the US from in Europe. It is a much, much less regulated industry in the US.

The second part of your question was about their relationship with Facebook. Facebook has always tried very hard to prevent its data from ending up in the hands of data brokers, and it has quite a number of rules in place to ensure that third-party developers on Facebook Platform do not pass the data to data brokers, but again it is the same problem: they are simply reliant on a rule, and on the threat of a potential lawsuit, and I do not think that is sufficient. I think the real problem is that they allow all of this personally identifiable data to pass out of their servers into the hands of a very highly varied set of people. Anyone can create a Facebook app—there is no background check creating a Facebook app—so it is hard to imagine that some of that data did not end up with data brokers.

Q1214 Brendan O'Hara: I am struggling to understand why Facebook would then allow such vast amounts of their data to be transferred to developers who would then give access to the data brokers. Is that right?

Sandy Parakilas: Again, Facebook did not want the data to go to data brokers, but I think their primary motive was that they wanted to motivate a huge ecosystem of apps as quickly as possible, and the fastest way to do that was to allow access to a large amount of data. That was the primary selling point of Facebook. They had the best and the most personal data of anyone. Again, their model is “move fast and break things”, the goal was to grow the platform as quickly as possible, and data was one of the key ways to do that.

Q1215 Brendan O'Hara: But they must have known that personal data would end up in the hands of data brokers if they did not have these safeguards or these security protections in place?

Sandy Parakilas: They do. There were people in the company like me who were saying, “This data could go to data brokers.” I said that multiple times. I think it was a risk that they were willing to take.

Q1216 Brendan O'Hara: You talked earlier about friend permission. When they changed friend permission in 2014, was that done as a crisis of conscience? Was it a moral or purely commercial decision?

Sandy Parakilas: I think your question was about changing permissions.

Q1217 Brendan O'Hara: Yes. You said that Facebook in 2014 no longer allowed friend permission. Was the reason for the change a moral decision, a crisis of conscience, or was it a commercial decision?

Sandy Parakilas: I was not there when that change happened, so I can only speculate but, based on conversations that I had while I was at the company, I think it was actually a number of things. The primary motivation was likely that Facebook apps were in the process of moving away from web to mobile devices as people moved from web to mobile



devices and the problem for Facebook was that on the web they controlled the payment mechanism, they took 30% of the payments, so it was a real business for Facebook, but on mobile they did not control the payment mechanisms—they were controlled by Apple and Google—so they could not make any money. Suddenly the upside of building this business and letting people build all these apps and taking 30% of payments they were charging went away, the upside was much, much reduced, so then the downside of the risk of data exposure was not worth the upside. I do not know, but I suspect that was the calculus.

Q1218 Brendan O'Hara: Moving on to Cambridge Analytica, when did Facebook know that data had been passed to Cambridge Analytica?

Sandy Parakilas: Again, I was not there when any of this happened, but to my understanding they knew when there was a *Guardian* article in December 2015 that described how Cambridge Analytica was using believed Facebook data on the Ted Cruz campaign. Based on what I read in the press, it sounds like at that point Facebook reached out to Kogan, who developed the app, and Cambridge Analytica and demanded that both delete the data and then at some point they got some kind of a certification saying that the data had been deleted and both those entities agreed and certified that the data had been deleted. I also believe that shortly thereafter they deleted Kogan's app so that it was no longer a Facebook app. So they knew in December 2015.

The concern that I have, other than the fact that it took them that long to figure out that this was going on after detection, was that over the next two and a half years, from December 2015 until last Friday, there were numerous media reports that described how Cambridge Analytica was using huge amounts of Facebook data to do a variety of things. News reports were claiming that Facebook knew that they had had a conversation with Cambridge Analytica and demanded that data be deleted. There was a two and a half year period when they had an understanding that data had been deleted, they were hearing in the press that it had not been deleted, but as far as anyone can tell they took no action whatsoever during those two and a half years. They did not sue the developer, to my knowledge, and they did not conduct any kind of audit. That, to me, is a very long period of time to not take any action.

Q1219 Brendan O'Hara: Given that they had lost control of the data, what other remedies were open to them, other than asking or insisting that it be deleted? What else could they have reasonably done in those two and a half years?

Sandy Parakilas: I think they could have filed a lawsuit to enforce on the fact that these two companies had signed a certification saying they had deleted data but they had not deleted data. I am not a lawyer, and I am certainly not an expert in UK data protection law, but, considering that Cambridge Analytica had signed a certification saying the data had been deleted, presumably they could have involved law enforcement to help them enforce.



HOUSE OF COMMONS

Q1220 **Brendan O'Hara:** Do you think that Facebook accepted what they were told by Cambridge Analytica; that they had deleted their data? Do you think that they went through the two and a half years believing that it was no longer a problem?

Sandy Parakilas: I do not know what they knew or did not know. My perspective is that they should have taken action, considering the fact that there were multiple significant press reports about Cambridge Analytica's activity during that two and a half years.

Q1221 **Brendan O'Hara:** Are you aware of any attempt by Facebook over those two and a half years to inform their users that their data had been compromised?

Sandy Parakilas: I can only speak to the period of time that I was at the company. Again, I do not recall any proactive notification of Facebook users relating to the passage of data to parties that were not authorised or use of data that was not authorised. I do not remember any proactive notification. I was not working at the company during any of this period, but I do not believe that Facebook notified users about what happened with Cambridge Analytica, and nor have they done so to this day. That is my understanding.

Q1222 **Brendan O'Hara:** Finally, do you think that the Cambridge Analytica incident was a data breach on behalf of Facebook, or was it a failure of procedure and a failure of their own rules and due diligence?

Sandy Parakilas: I cannot give a legal opinion on whether there was a data breach. I think that from the perspective of a user of Facebook, the effect is the same as a data breach, and in fact I would say that this is in some ways worse than a data breach, because the users had no idea that their data was compromised in the same way as it would have been during a technical data breach and Facebook was aware that this had happened, did not notify anyone, should have been aware that it was continuing to happen and, again, did not notify anyone, to the best of my knowledge. I think that whether it is a data breach or not is not really the point; the effect of this on users was the same as a data breach and should be treated as such.

Q1223 **Chair:** Sandy, from what you have said it would seem clear that while we have been focusing this week on the data breach with Cambridge Analytica, there have been probably many such data breaches involving other companies and other developers in the past. Would that be your view?

Sandy Parakilas: There are most certainly a number of reports of similar kinds of activity, and I think one of the challenges is that, in my experience, Facebook rarely, if ever, investigated to the point where the absolute truth was understood.

Q1224 **Chair:** For the benefit of the record, could you cite some of those particular reports that you are referring to?



HOUSE OF COMMONS

Sandy Parakilas: This is an allegation, because Facebook never understood exactly what happened. It is an allegation; I cannot say this was a data breach or even—I would not characterise this as a breach, but let me explain what happened in this particular example, and then we can talk about what it means.

There was a company called Klout that was allegedly using third-party permissions, friend permissions, to create profiles, some of which were children. You would go to the private web page, and you could see a profile of someone with their name, and I believe their photo, but that person had not created that profile, and in some cases those profiles were children. Those children's profiles were discovered by their parents and their parents were the ones who authorised the Klout Facebook app to access Facebook data.

This caused a report in *The New York Times* that raised a fair amount of concern that Klout was getting access to the data of children and using that data to create profiles of these people without the children's consent. What happened was that this report in *The New York Times* alerted Facebook that this was going on. I called the leadership of Klout, I said, "Are you violating Facebook's policies?" and they said, "No, we are not." I reiterated what the policies were and said, "You absolutely have to follow these policies." They said, "Yes, we absolutely will," and that was the end of the call. They had stopped doing the ghost profile feature either right before or right after that—I am not sure—but around the time they disabled that feature they continued to access Facebook data and they continued to be a Facebook app. There was no affirmative action taken, to my knowledge, by Facebook as a result of that.

Was there misuse of Facebook Platform? There may well have been. However, Facebook did not investigate deeply enough to determine exactly whether misuse took place.

Q1225 **Chair:** Did you recommend to Facebook that they should investigate? What were you able to suggest should be done after you had had your call with Klout?

Sandy Parakilas: In that specific instance, I do not recall if I made a recommendation about Klout. In general, I asked for more audits of developers and a more aggressive enforcement regime.

Q1226 **Chair:** What was their response when you asked for that?

Sandy Parakilas: Essentially, they did not want to do that.

Q1227 **Chair:** Why not?

Sandy Parakilas: I did not get a specific response, but I believe that the company felt that it would be in a worse legal position if it investigated and understood the extent of abuse, and it did not. That was the impression I got.



Q1228 **Chair:** Why? Because people might say Facebook had some liability for allowing this to happen?

Sandy Parakilas: Again, I do not remember the specific language that was used, but the impression that I got was that if Facebook did an investigation and received information that showed that policies were being broken and potentially laws were being broken, then Facebook was liable. However, if Facebook did not know what was happening, they could claim that they did not know, they were simply a platform and what third parties do on their platform is not something that you could sue Facebook for.

Q1229 **Chair:** From what you are saying, it sounds like they turned a blind eye because they did not want to find out the truth.

Sandy Parakilas: That was my impression, yes.

Q1230 **Chair:** You mentioned as well that there are some Facebook apps that have hundreds of millions of users. We have focused on Aleksandr Kogan's surveys, but that is tiny in comparison to the data gathering that other developers are doing?

Sandy Parakilas: Yes. I should add that there was one additional concern that may have caused the shutdown of friend permissions in 2014. There was concern inside Facebook then that other developers were building their own social networks because they had accessed so much friend data that they could see most of the social graph of Facebook.

Q1231 **Chair:** It was done not to protect users but to protect themselves?

Sandy Parakilas: Again, I was not there for the decision that was made, so I cannot speak to how that decision was arrived at, but I believe it was some combination of risk calculation because of the user protection issues and business rationale.

Q1232 **Simon Hart:** You probably read or heard earlier in the week that Facebook gained access to Cambridge Analytica's office, I think on Monday evening, when all of this was beginning to catch fire. Is there any reason why you think that was possible? What was the relationship, in your estimation, between Facebook and Cambridge Analytica that enabled them to gain access, albeit for a short time, rather than Facebook and a whole host of other organisations that might have been equally concerned?

Sandy Parakilas: I cannot speak to the specifics of the Facebook/Cambridge Analytica relationship. I can say that Facebook has an audit right for its platform policies. If a company is a developer on Facebook, they agree to Facebook's platform policies and those policies give Facebook the right to audit the app, and I believe that also gives them the right to audit the data storage of the company.



HOUSE OF COMMONS

I think the key thing to note here is that, to my knowledge, Cambridge Analytica was not a Facebook developer. I may be wrong—I am not sure—but in this case Kogan was the developer; Cambridge Analytica was a fourth party, where data was passed from Kogan to Cambridge. I suspect that what gave them the right or the leverage to go into their office was this legal certification that Cambridge and Facebook signed after it became known that they had accessed the data in violation of the policy.

Q1233 Simon Hart: Is that different from suggesting or implying—well, I am; you are not—that there might have been either some historical commercial or some current commercial relationship between the two companies that facilitated that access, or do you think it was simply because of the legal and contractual arrangements that you referred to?

Sandy Parakilas: I do not know what the commercial relationship was. However, I find it hard to believe that Facebook did not know that Cambridge Analytica was working with the Trump campaign. The Trump campaign was spending tens of millions of dollars on Facebook ads. I cannot speak to what the commercial relationship was, but they clearly were involved in more developments of Facebook advertising.

Q1234 Simon Hart: When you heard that Facebook, or auditors appointed by Facebook, were knocking on the door of Cambridge Analytica on Monday and demanding access, what was your initial impression? What did you think was going on?

Sandy Parakilas: My first impression was that this is two and a half years too late. Why did this not happen when they learned that this was going on? That was my first impression. Again, I cannot speak to what the relationship was between Cambridge and Facebook and the Trump campaign—I have no detail of that whatsoever—but, from the perspective of someone who worked on these issues a few years before this happened, it was shocking to me that they waited this long to take the step that they should have taken all along, which is: if they had the right authority to enforce, actually go in and enforce.

Q1235 Simon Hart: Can I just go back to a question you were answering earlier about other organisations? We have dealt extensively with Facebook and Cambridge Analytica and the relationship or otherwise of those two organisations. There are of course numerous other organisations, often quite small companies, in and around the business of elections and referendums that also boast that they are able to target and micro-target voter groups to the benefit of whoever is the paying client. I know you started to answer this, but do you think there is sufficient evidence out there to suggest that there are other companies, without the brand recognition of Cambridge Analytica, which presumably has acquired data from somewhere, that may have acquired data illegally from Facebook and that may have been used it in an attempt to impact the outcome on elections in the UK and further afield?



HOUSE OF COMMONS

Sandy Parakilas: That seems very likely. The amount of data that was passed out of Facebook Platform between 2010 and 2014 is just vast. There were, in my memory, hundreds of thousands of apps on the platform while I was there. According to some research in *The Atlantic Monthly* that was cited over the last weekend, 11% of Facebook apps around in 2011 were using some form of friend permissions. I do not know if you can extrapolate directly from hundreds of thousands of apps times 11%, but you are likely talking about tens of thousands of apps that garner access friend permissions, and some of those apps had tens or hundreds of millions of users. There is a vast trove of data that has been passed out into the world.

Q1236 **Simon Hart:** You might not have been following this as closely as we have, but is there any suggestion that the players in the EU referendum campaign in the UK might have been accessing this data in the manner that you describe?

Sandy Parakilas: I have no information about how that data was used. I always assumed that there was some sort of black market for some of this data that Facebook and others could not see, but I have no insight into how that black market works or when it was used in elections generally or in UK elections. Unfortunately, I cannot answer that.

Q1237 **Simon Hart:** But there are a lot of organisations that are out there constantly trying to persuade us that they have micro-targeting ability that would help one political party or movement. That is quite a common feature of UK politics these days. I suppose my question is this: where are they getting their data from?

Sandy Parakilas: Facebook is certainly not the only source. There is a huge market for data. What was unique about Facebook was its vast scale and the volume of very accurate personally identifiable information, but there are many, many sources for personally identifiable data on people, and if you have the money to pay you can start building a very comprehensive dataset quite quickly. If you are willing to bend the rules and break the law, you may be able to acquire data from additional sources, one of which might be Facebook.

Q1238 **Ian C. Lucas:** Sandy, you just said that the Trump campaign was spending tens of millions of dollars on Facebook ads. Isn't it the case that Facebook itself is making huge amounts of money from political advertising and targeted political advertising? Is that true?

Sandy Parakilas: Yes, tens of millions of dollars—I do not know the exact number, but it was reported in the high tens of millions of dollars over the course of the 2016 campaign. That money is paid directly to Facebook.

Q1239 **Ian C. Lucas:** But Facebook also markets itself in politics to political parties and political campaigns to micro-target voters. That is true, isn't it?



Sandy Parakilas: It is. One of the key things to remember here is that the intent of Facebook Platform was never to target ads. It was explicitly not for that. The problem was that there were not reasonable controls in place to ensure that did not happen. There are multiple ways that you can target advertisements on Facebook—Facebook has very, very big data that you can use in a compliant way through their ad tools—but what Cambridge Analytica was allegedly doing, or trying to do, was create external profiles, allegedly using Facebook data and other data of individual voters, and then building custom lists, what Facebook call custom audiences, where you have specific Facebook users that you want to target and then you can build these custom lists and target specific ads at subsets of these users that you create yourself.

Q1240 **Ian C. Lucas:** But what I do not understand is what the difference is between what Cambridge Analytica was doing and what Facebook does with the data that it has itself. Doesn't Facebook also target individuals for political parties for political advantage?

Sandy Parakilas: I think the question is: did Facebook micro-target users—

Ian C. Lucas: Yes, in political campaigns, when it sold advertising to political parties and to candidates, wasn't it itself targeting voters and micro-targeting?

Sandy Parakilas: Yes, that is a feature of digital advertising. What Facebook, Google and other big tech companies sell—their pitch to advertisers—is that you can get very, very specific audiences.

Q1241 **Ian C. Lucas:** Facebook are identifying individuals on the basis of their own records, and they are targeting advertisements at those individuals for political purposes?

Sandy Parakilas: Yes. I think that is just a standard feature of advertising, and digital advertising just makes the targeting more fine-grain. Where you would find an ad at a football match where you can get millions and millions of users and you do not know who those users are but you know they are people who like football, on digital platforms like Facebook you can buy men between the ages of 24 and 30 who live in specific towns, and if you want to target them with political ads you can, because the platform enables that.

Ian C. Lucas: Do you know if Facebook builds political profiles for its own business purposes to target particular groups?

Sandy Parakilas: I do not know the answer. I have seen some pitches that they have made to political campaigns where they tout the benefits of their data for electioneering advertising.

Q1242 **Ian C. Lucas:** I have had one made to me, before the last general election. So Facebook themselves build political profiles for the purposes of campaign ads?



HOUSE OF COMMONS

Sandy Parakilas: I cannot answer that, because I do not know if that is exactly true, but they certainly tout their ability to help election candidates through their tools.

Q1243 **Ian C. Lucas:** But you also said that you yourself have heard, and not just from me, that they had built a profile—

Sandy Parakilas: Yes, they aggressively market themselves as having really good data, I believe, about the potential voting preferences of users on Facebook. I guess if you are saying political profiles, if you go into your Facebook ad settings I believe that you can see your party preference, at least in the US. I do not know if that exists in the UK, and I am not sure I would qualify that as a political profile, in the sense that, to my knowledge, they do not break out specific issues, at least from what I have seen, which was my own profile, they said, “You are likely to go for this party.”

Q1244 **Ian C. Lucas:** Did they get it right for you?

Sandy Parakilas: They did.

Q1245 **Ian C. Lucas:** How do dark ads work on Facebook?

Sandy Parakilas: Posts are simply when you type in the box at the top of the page of the app, you post and your friends can see it. A dark post is a post that does not go to your friends or followers or a particular page; it is a post that is only to users who you target, and the main purpose of dark posts is to address many different iterations of ad content. A political campaign may run tens or hundreds of thousands, or even millions, of different versions of an ad, so dark posts are one way to put those advertisements in front of different users via paying and seeing that it performs better.

Q1246 **Chair:** Can I just ask one or two further questions on targeting? You said that there are lots of different ways that an advertiser can target people using Facebook tools, and you said that a company such as Cambridge Analytica may be creating external profiles of Facebook users. Can it then target those exact same people through Facebook’s targeting tools?

Sandy Parakilas: To my understanding, what is alleged of Cambridge Analytica is that they acquired through illicit means a large amount of Facebook Platform data, which is the same data that Facebook uses to ad-target, but it just pipes out through a different exit, so to speak. They mixed that with data from other sources and then used all of that information to create voting profiles where they estimated how individuals may vote and then—again, allegedly—took those pieces of information about individuals and created lists and those lists were used to target ads by the campaign.

Q1247 **Chair:** I suppose what I am getting at is this: would Facebook let you target advertising at individual Facebook users rather than just categories of people?



HOUSE OF COMMONS

Sandy Parakilas: Yes; well, not one person, but you can create a list of all of these individuals to be targeted, and if there is a match, if Facebook can find that person based on an email address, for example, then they will show that person, as well as everyone else on the list, the ad that you want.

Q1248 **Chair:** I think in my constituency, if I wanted to target—you might think that the way Facebook advertising works is that I could target an advert at women aged between 30 and 40 who live in Folkestone, but actually you can do something much more specific than that; I could give Facebook a list of the users I wanted to target, the individual people, and I could just target them?

Sandy Parakilas: Yes, you could make a very specific list. I do not remember the lower limit—at some point it was no fewer than 20 people; that may have changed—but you can say, “I want to target this list of people and only this list of people,” and it will target any of the people that it can find on Facebook.

Q1249 **Chair:** I understand that you can target people by things they like. I support Manchester United Football Club. If I wanted to target Manchester United fans on Facebook with an advert, presumably I could buy that as an audience; would Facebook help me identify people that had shown that they had an interest in that football club?

Sandy Parakilas: Yes, through Facebook’s advertising tools you can buy ads targeting people by their interests.

Q1250 **Chair:** Can you also target people based on language and words that they use in their posts or in their messages on Messenger?

Sandy Parakilas: To my knowledge, not specifically. I do not believe you can target people who use a specific phrase. However, information may include related data they deal in relation to things people have said, although I am not fully confident how that works, so I do not want to expand further on that.

Q1251 **Chair:** Just so that I am clear, you said Facebook have data based on things people have said?

Sandy Parakilas: Yes. If you have written posts on Facebook, which most people on Facebook have, then they have the data of what you have said.

Q1252 **Chair:** If they have the data, presumably you can target based on that data?

Sandy Parakilas: I am not confident enough to explain how that works to give an answer here. To my knowledge, you cannot explicitly target someone based on something they explicitly said. You cannot do that. That data would need to be used in a more general way in targeting, but I am not 100% sure.



HOUSE OF COMMONS

Q1253 **Chair:** Just as an example, if someone is posting a lot of favourable comments about Donald Trump, say, would Facebook effectively have a dataset of those people, and in theory if you were the Trump campaign you may say, "I want to target messages at people who are already well disposed towards the candidate, and I can identify that as an audience on Facebook"?

Sandy Parakilas: Facebook makes a determination if you are interested in a particular keyword. So "Donald Trump" may be a keyword, and there is a variety of data that helps them figure out if you are interested in Donald Trump, and that data may include stuff that you write on Facebook. However, I do not know the technical details enough to speak to how that works.

Q1254 **Chair:** What if I was interested in immigration as a political issue? Would Facebook be able to identify people who are interested in immigration?

Sandy Parakilas: If that is a keyword, then yes. It likely is, but I am not 100% sure.

Q1255 **Chair:** It is quite interesting, because you start to get into potentially quite sensitive, quite hot political topics. Potentially, Facebook creates data groups around people that have an interest in those topics, and advertisers could advertise to those people?

Sandy Parakilas: Yes. It is interest-based. You can target people based on things that they have expressed an interest in, whether it is liking a page or picking some other action that shows you are engaged with that particular topic. Then you can also have multiple interests, so you can target people who are interested in any number of identifiable interests.

Q1256 **Chair:** Yes, but do they audit those lists of interests? Someone may have quite unpleasant interests. Someone may be a racist and engage in racist discussions all the time. Would they actually say, "We will create a dataset around those people," which in theory people could advertise to?

Sandy Parakilas: Yes. There was controversy a few months ago when Facebook was determined to be servicing interests around some very offensive phrases. Those were phrases that those people had used in their Facebook profiles, so Facebook evidently pulled that information in and serviced that as a potentially targetable interest. After it was called out, Facebook have said they are making some changes. I am not clear on exactly what these are, but they are probably putting some checks in place to ensure that the names of interests that are used exclude certain categories.

Q1257 **Chair:** It is interesting, because I do not know if you are familiar with an organisation called Britain First, which has recently been banned from Facebook, after quite a lengthy campaign where Facebook refused to do that, but from what you are saying it sounds like an organisation like that, which holds extreme views, could not just create a platform for themselves on Facebook, but actually use Facebook to help identify and



HOUSE OF COMMONS

reach out to people who shared similar opinions.

Sandy Parakilas: I think that is possible. You can use targeting to find people who are interested in any number of things, and some of those things may be unpleasant.

Q1258 **Jo Stevens:** We have asked Mark Zuckerberg to come and give evidence to our Committee, Sandy. What would you recommend that we ask him, if he decides to accept our offer?

Sandy Parakilas: I want to provide some potential questions for you. I want to follow up offline, if that is the best way.

Q1259 **Jo Stevens:** That would be very good. Thank you. What more do you think Facebook could do to prevent foreign interference in elections in the US, in the UK and other countries?

Sandy Parakilas: There are people in the group that I work with, the Center for Humane Technology, who are more expert in the subject matter than I am. We would be happy to talk further about that issue if that is something that you guys want to talk about. I do not want to speak to it specifically now, because I would prefer to ask someone who is an expert in that specifically, if that is fine.

Q1260 **Jo Stevens:** Okay. Just staying on the foreign interference point and what we have been discussing about Cambridge Analytica, do you think that those people whose data has been breached, or used in a way that it should not have been, should each be informed that that has happened, and if you think they should be informed, is there a technical way that that can be achieved?

Sandy Parakilas: They should absolutely be informed. I do not see why Facebook would not be able to figure out either who was immediately impacted or a very close estimate of who was impacted on, because they have the logs that the app cultivated and they should be able to determine who the friends of the app users are and determine the data that was passed over.

Q1261 **Christian Matheson:** Sandy, we have had some regulatory action this week from the UK data commissioner. We will not go into the details of that, but what powers have you seen regulators use, and what powers should they have, to be able to look freely at the data that is held by big companies, to look behind the curtain, to go into companies and see how they are protecting users' data? How do you think that should work, and what experience have you had of seeing it work?

Sandy Parakilas: On enforcement, at Facebook to my knowledge there was no physical audit of any developer—I cannot speak to how that works. But I think your question is more about how regulators could audit technology companies, and my perspective on this is that there are a number of privacy issues that need to be thought through to do this correctly. That said, if you think about how we think about financial regulations and the level of auditing and scrutiny that the finances of



HOUSE OF COMMONS

companies receive, we should probably be applying that same kind of thinking to some of the non-financial aspects of technology companies to ensure that the information that they are providing is correct and to ensure that when issues such as this happen people are notified appropriately and that their security mechanisms are reasonable.

Q1262 Christian Matheson: You are suggesting that that puts the onus back on the developers or the platforms to notify the data protection regulatory authorities, as opposed to the regulator having the ability to go in themselves and carry out audits, or should it be a bit of both?

Sandy Parakilas: Unfortunately, I do not think I am close enough to UK law to be able to answer that one.

Q1263 Christian Matheson: What has been your experience in the USA?

Sandy Parakilas: We do not have an information commissioner in the US.

Q1264 Christian Matheson: There are no regulatory authorities that can go in and check what is happening to personal data held in the United States?

Sandy Parakilas: To my knowledge there is no comprehensive data protection law in the US.

Q1265 Christian Matheson: If we are talking about personal data that is held by an American company on servers that are based in the United States but that is personal data about somebody who is in a different country, for example the UK, then the regime under which that data would be managed would be the data protection regime of the United States?

Sandy Parakilas: I do not think I would be able to answer the question. I am probably not the right person to ask data protection legal questions.

Q1266 Julie Elliott: Thank you for the evidence you have given this afternoon. You have very clearly explained to us how this all works. Do you think Facebook realises the size of the problem it has here?

Sandy Parakilas: No. I think if they realised the size of the problem they would have taken some action between December 2015 and last Friday in respect of Cambridge Analytica, and I do not think they would have built their platform as they did.

Q1267 Julie Elliott: Do you think in the last week it is beginning to dawn on them that they have an enormous problem?

Sandy Parakilas: Yes, I believe they are now starting to understand how big a deal this is.

Q1268 Julie Elliott: What challenges do you think what you have outlined, the way this works, poses to democracy in your country and in our country, or do you think it is posing a challenge?

Sandy Parakilas: I think it is creating huge challenges for democracy, and I think it is not a Facebook-specific problem; there are issues with



HOUSE OF COMMONS

the amount of data that private companies and organisations have about individuals and the ways that technology is built such that people can be manipulated using that data. I think that is the problem, and Facebook is one part of it, but it is only one part of this. There are many, many aspects.

Q1269 **Chair:** Thank you. I think that brings the formal questions to a close. I wonder if I may just ask whether there are any recommendations you might make to the Committee about reforms in the way social media works to help further protect the interests of users.

Sandy Parakilas: Yes, and that is also something I would love to follow up on, definitely, because the organisation that I work with, the Center for Humane Technology, has a number of thoughts about this. I would love to provide that in a written form.

Q1270 **Chair:** Great. In that case, on behalf of the Committee, thank you very much for your evidence.

Sandy Parakilas: Thank you.