

# Digital, Culture, Media and Sport Committee

## Oral evidence: Fake News, HC 363

Thursday 26 April 2018

Ordered by the House of Commons to be published on 26 April 2018.

Watch the meeting

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

Questions 2087-2500

### Witness

I: Mike Schroepfer, Chief Technical Officer, Facebook.

Written evidence from witnesses:

– [Facebook](#)

## Examination of witness

Witness: Mike Schroepfer.

Q2087 **Chair:** Good morning 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 very pleased to welcome Mike Schroepfer to give evidence to the Committee today. This follows evidence that we took from Facebook in Washington in February but there has been quite a lot of significant developments since then that have given cause for the Committee to consider other questions we want to put to the company, so we are grateful to have the opportunity to do that today. There is no time limit on this session so I cannot say exactly what time we will finish. I do propose that we will take a short 15-minute break at 1.00 pm if we are still running at that point and then resume shortly after that.

Mr Schroepfer, if I could start the questions. How much money do you think you will spend on your next car?

**Mike Schroepfer:** I am sorry, sir, can you repeat the question? I didn't hear it.

**Chair:** How much money do you think you will spend on your next car?

**Mike Schroepfer:** I don't know.

Q2088 **Chair:** Okay. What is the rough square footage of your home?

**Mike Schroepfer:** I don't know that off the top of my head either.

Q2089 **Chair:** Okay, but Facebook gathers that information about you as a Facebook user, as it does from its other users too.

**Mike Schroepfer:** I doubt Facebook knows the square footage of my home or how much I am going to spend on my next car.

Q2090 **Chair:** But those are categories of user information that Facebook gathers data points on, based on your use of Facebook and the way you use the internet, the other sites you visit.

**Mike Schroepfer:** I want to clarify one thing, Mr Chairman. First of all, may I just say two sentences to introduce—

**Chair:** We will go straight into the questions, if that is okay.

**Mike Schroepfer:** Of course.

**Chair:** Just for the benefit of the people in the room as well, we have received your written statement, which we are grateful for, and the Committee has published that now. It is available online for everybody who wants to see it although, having read the statement, I am pretty sure we will cover off a lot of the subject matter as we go through the



session.

**Mike Schroepfer:** Great.

Q2091 **Chair:** Facebook gathers that information. Those are categories of information that Facebook gathers about Facebook users: how much money you spent on your car or are likely to spend on your next car; how big your home is. Facebook may have a good idea of the answers to those questions even though you were not able to answer them. Why does Facebook gather that data about its users?

**Mike Schroepfer:** I want to clarify one thing. I have looked recently at my ads preferences, which is a feature on Facebook that any one of you or your constituents can use right now to look at the interests that we have understood that you have. That is what we allow advertisers to find and advertise against. In my interests there was nothing about my home or the purchase price of my car or anything even close to that level of detailed information. It said things like I have a liking for coffee, that there are certain events and other things I am interested in; I am interested in new technology; I am interested in travel; I like cats. These are all things that you would find in your interest category. They are things that our advertisers can then advertise against. The key thing is if you do not like those categories, you can change them or delete them if you so choose at any time in the ad preferences. That is the basic way it works with the advertisers.

Q2092 **Chair:** But the ad preferences is based on Facebook's analysis of the things it thinks you are interested in. That would be correct, wouldn't it? You may not be in the market for buying a new car, so there might not be very much information about that, but if you are interested in coffee there will be.

**Mike Schroepfer:** The basis of our service, the thing we provide, is a way for us to provide personalised experiences. Setting aside ads for a second, when I log into Facebook the thing that I get is a personalised news feed. This is updates mostly from my friends but possibly from pages I follow or other things. The whole purpose is to provide the information that is most relevant to me. The feedback we get from people over and over again is that when they find things on Facebook that they are not interested in or are not relevant to them, that is the worst form of experience. The best way to provide them relevant information is to have an idea of the things they are interested in so that we can provide that information for them. As I said, it is a key principle of ours that we are overt with what that information is, those interests, and allow you to control it if you want to change it or delete those things.

Q2093 **Chair:** As well as people's consumer preferences, Facebook seeks to gather information about an individual's political interests and their likelihood to engage in political activity. That is correct, isn't it?

**Mike Schroepfer:** There is a wide of variety of interests that people can participate in on Facebook and politics is one of them.

Q2094 **Chair:** Yes, exactly. If in my ad preferences I said that I did not want to receive political advertising, could you guarantee that I wouldn't?

**Mike Schroepfer:** The way it works is you can decide which interests advertisers would want to use in order to find people who are interested in those topics. Just like there is no way for me to prevent a political advertisement coming on my TV or showing up in a newspaper that I might pick up, even if I have said that I am not interested in politics, for example, political advertisers may choose to try to advertise to everyone in the United States at which point I may see one of those advertisements. We try to use the interests to help advertisers find their audience but there may be places where those advertisers are trying to reach a broad audience even if I have not declared any interest in what they are looking for.

Q2095 **Chair:** If I expressly said I do not want to see political advertising, what you are saying is that you could not guarantee I would not see political advertising in my news feed?

**Mike Schroepfer:** Like most forms of advertising, if there are advertisers who want to reach all people, it is hard to say, "No, you can't reach that particular person".

Q2096 **Chair:** I might buy *The Times* newspaper and there might be an advert in that. I can't control what the advertising is. I might generally expect the advertising is relevant to me as a reader of that paper but I can't control it. Isn't that very different though from your own personal news feed on Facebook where you cannot block a certain category of advertising from reaching you?

**Mike Schroepfer:** I want to clarify one thing. My humble apologies, I forgot one important thing, which is I was referring to the ads preferences that describe the interests that advertisers can use to find you as an audience. There is another feature in the product, which is if you see any advertisement and decide that you don't like it, there is a control to say, "I don't want to see this advertisement" or "I don't want to see anything from this advertiser again". In the US if one of the political parties is advertising to me, I could decide to mute all ads from that particular party, which is a feature you absolutely do not have on a newspaper or television. By doing that and hiding pages and other things, you can control the sorts of ad you would see, even if they were broad-based trying to reach all of the UK or the US.

Q2097 **Chair:** One of the difficulties there, and this is one of the things that we have been looking at in this inquiry, is that political advertising does not necessarily come from registered political parties. It can come from multiple different entities using different pages on Facebook to base their advertising on. If you can't turn off political advertising—you said you can't—even if you block an individual advertiser, it does not mean to say you will not get something very similar from a different entity. You have to be consistently blocking those people. That would be the case,



wouldn't it?

**Mike Schroepfer:** This is one of the places where we are doing a lot of work. As we said in my written statement, we are showing ads transparency here in the UK that will let me see all the other ads from that advertiser. Specific to your question of political ads, we are going to mark all of the political ads prior to the 2019 elections here in the UK. We are going to provide a searchable archive of all of those ads and explain who paid for them and provide a lot more transparency for people who want to understand this. I understand the concerns about giving people control over political advertising. It is an important issue that we are working on.

Q2098 **Chair:** I think we have established that people do not have control over political advertising to the extent that they can stop receiving it. We have certainly established that. If I am an advertiser wishing to target a political audience on Facebook, that is based on their metadata—that is right, isn't it—the data trail that that person has created through using the platform? Is that correct?

**Mike Schroepfer:** Again, I want to clarify one thing. You can mute ads from advertisers on Facebook, which is a feature you do not typically have on most other media.

Q2099 **Chair:** I think we have covered that point. Political advertising can be based partly on people's metadata trail from Facebook itself. You would be looking at what someone is interested in on Facebook, what they do, and from that surmising that person might be receptive to receiving political advertising. Is that correct?

**Mike Schroepfer:** We build a list of interests to try to understand what people are interested in.

Q2100 **Chair:** Yes, I know, but we will stick to politics. Politics is one of those interests; I think we have established that. My activity on Facebook, my metadata from Facebook can be used to put me in a category where I might receive political advertising from an organisation. Would that be correct?

**Mike Schroepfer:** Let me give you an example of interests that people might use for political advertising. One of the key ways that we understand interests is that there are pages on Facebook. These are places where you obtain information from public entities and if you like or follow that page we will use that as a signal that you are interested in that category of topics. If I liked a political issue about immigration or something else, that possibly could be used as a signal to understand that people who are interested in that category of things might want to receive advertising on it.

Q2101 **Chair:** But it would be more than likes, wouldn't it? It could be posts I have put on Facebook about political issues?

**Mike Schroepfer:** We don't scan your posts for advertising data.



Q2102 **Chair:** That would not be part of my metadata profile on Facebook?

**Mike Schroepfer:** I think the easiest way to do this is on a very individual level look at your ad preferences and you can see exactly what we have computed for you as your set of ad preferences. If you or any of your constituents want to look at those you can see—

Q2103 **Chair:** I am talking about you rather than me, in a way. I am talking about what the company does rather than what my personal ad preferences are. You track Facebook IDs of users as they visit other sites that are off Facebook. That could also include political websites I have visited that could be part of my data profile on Facebook. Would that be correct?

**Mike Schroepfer:** The way this works is that any website that wants to include functionality from Facebook or any number of other folks can choose to include features like our “like” button, for example, or “share” button that would allow you to like or share that information. When I visit that page, we would get a log of that visit on to our servers. As an example, on your website, when I looked at my news about my testimony this morning, you have this sort of third-party information from six different companies—Google, LinkedIn, Twitter, Hotjar, Pingdom and Facebook—all on that site and so when a user visits that site their browser will send a cookie, a piece of information, to each one of those third parties.

Q2104 **Chair:** In general, not just thinking of political advertising or political websites, what proportion of websites do you think have Facebook tracking software on them?

**Mike Schroepfer:** I do not have a number for the proportion of the sites that have decided to include some of our software, given how large the internet is. I don’t know.

Q2105 **Chair:** You are probably best placed to give an educated guess. What do you think that would be?

**Mike Schroepfer:** I am an engineer, so I don’t like to speculate on things that I have not studied. I honestly don’t know the proportion offhand.

Q2106 **Chair:** A half, a third?

**Mike Schroepfer:** I would suspect much less.

Q2107 **Chair:** Much less—10%?

**Mike Schroepfer:** Again, I am guessing at a number, which I don’t like to do.

Q2108 **Chair:** I wonder if you could give us a range, that was all. I am not going to hold you to a number but if you could give us a range. It is quite important to your business. I would have thought it is the sort of thing that someone in your position would know.



## HOUSE OF COMMONS

**Mike Schroepfer:** It is not a statistic I have tracked since I can remember working there.

Q2109 **Chair:** Facebook can gather data about people's political preferences and opinions, based on their metadata from the site itself and from tracking the way they visit other sites. You hold that data and that can be of benefit to people who wish to advertise through Facebook. Before we even get to the GDPR rules, given that the current UK data protection rules put very strict restrictions on people holding political data, private companies holding political data, do you think that what Facebook does now is legal?

**Mike Schroepfer:** It is my understanding that what we do is clearly legal. I want to be clear on one thing, especially as part of the GDPR. There are sensitive categories of information that you are not allowed to use and target against and I believe political opinions is one of those. That is actually part of our GDPR set of screens that we are showing to every single European user to let them be aware of that and choose whether they want to opt into that or use that or not. I believe there has to be clear consent to do that.

Q2110 **Chair:** Are you satisfied at the moment that everyone on Facebook that is being targeted for political advertising in Europe—or in the UK rather, to be more specific—has given their express consent that they wish to receive it?

**Mike Schroepfer:** It is my understanding that we are compliant with the law.

Q2111 **Chair:** If I have not only given my consent not to receive, I have actually told you I do not want to receive it and yet I still receive it, do you feel that is legal?

**Mike Schroepfer:** Even if you go into the ads preferences and delete all the information in there and so the only thing the advertiser is using to find you is to say that you are a person in the UK and I want to contact you, just like a TV or a newspaper ad would, I believe that is legal.

Q2112 **Chair:** You met with the UK Information Commissioner this week, didn't you?

**Mike Schroepfer:** We met with her office on Tuesday, that is correct.

Q2113 **Chair:** Did she raise any concerns with you about whether the way Facebook holds political data might be in breach of UK law?

**Mike Schroepfer:** No. We talked extensively about the ongoing investigation with Cambridge Analytica and others and we provided her staff with a variety of details about that.

Q2114 **Chair:** If a political advertiser wishes to upload to a custom audience to Facebook to help target their audience, do you ask them or does Facebook have a way of checking or asking them to confirm that the



## HOUSE OF COMMONS

people within that target audience have given their consent to receive political advertising?

**Mike Schroepfer:** It is a requirement that anyone who is advertising with us using information they have, like a mailing list that they have got through some other means, has legal rights to have that data. It is a certification we ask that the advertisers do with us that the data they are using, the information, for example an e-mail list, is something that they have acquired legally.

Q2115 **Chair:** The onus is on them to make sure that the data is correct and that the consents have been given?

**Mike Schroepfer:** Yes, because the important thing is that we do not actually see the data. When an advertiser decides to use, for example, e-mail, they have a mailing list for people who visited my shop, they have a list of e-mail addresses, we do not get the e-mails in raw form so I do not know what the e-mails are. We get it in a thing called hashed, which means that we can't reverse it. If I had never seen that e-mail before, I can't store it. We throw the data away afterwards because we are not responsible for storing that data. We can't even see the data so we could not validate it if we wanted to and so it is a requirement that the person who has acquired that mailing list confirms that they have the rights to that information.

Q2116 **Chair:** If the same advertiser who has a custom audience asks Facebook to create a lookalike audience as well, could you guarantee that no one who had opted out of political advertising would be included in that lookalike audience?

**Mike Schroepfer:** The controls we have for ads are to allow you to decide the set of interests that you would like us to use in order to have advertisers reach you. You can decide that you would like to no longer receive advertisements from a particular advertiser. If I had chosen that I did not want to receive ads from this advertiser, I would not get this ad even if I had given them my e-mail address through some other means.

Q2117 **Chair:** You said at the beginning that even if you had opted out of political advertising you could still receive it. What I am asking you is if an advertiser came along and said, "I want a Facebook lookalike audience for this custom audience I have created" could you guarantee that someone who had opted out of political advertising would not be included in the lookalike audience because they have already told you they do not want to receive that advertising?

**Mike Schroepfer:** I want to be clear and my humble apologies if I—these are complicated topics and I am sure I was not clear on them. There is not an opt-out for political advertising. What you do have is a set of controls over what interests you would like to use and you can remove all of the interests if that is what you want. It is basic information; age, location, gender is the baseline information that you have as information on Facebook. In that case if an advertiser said, "I would like to reach all



folks in the United Kingdom”, regardless of whether it is a product or a political ad, you would be a candidate for that ad unless you had chosen to say, “I don’t want ads from this advertiser anymore because I don’t like it”.

**Q2118 Chair:** There is the individual advertiser and you don’t like the ad, but what you are saying is there is not an opt-out for categories of advertising. You can remove your preferences, which might make it less likely you would receive it, but there is not an opt-out for political advertising. That is what you said, isn’t it?

**Mike Schroepfer:** There is no specific category-by-category opt-outs. There is a way to control the interests we use. I think it would make it very unlikely that unless the advertiser was trying to reach a very broad audience, for example every citizen in the UK, that you would see that sort of advertising. It is very important that when I mute an ad from that advertiser you no longer see any ads from that advertiser. These are controls that don’t exist on most platforms and certainly not on TV and print. I can also tell Facebook that I just don’t like this ad and we will use that as a signal in our systems to say, “Ads like this aren’t interesting to this person” and we will show fewer of those.

**Q2119 Chair:** A lot of work has been put on the user there. What we are concerned about is that in some of the political campaigns it is not like saying, “I am going to block ads from the Republican Party, from the Democrat Party”. It is thousands and thousands of different pages with thousands and thousands of different messages that people are receiving all the time from multiple different advertisers. That is a pretty weak tool to stop people getting messages they don’t want. What you are saying is that someone can’t even opt out of it. Going back to my earlier question, from what you said as well, even if you had said, “I don’t want to receive political advertising, I have removed that preference from my ad preferences”, Facebook could still sell you through a lookalike audience to a political advertiser. For me, that is the extrapolation of what you said. Is that correct?

**Mike Schroepfer:** I don’t think so. I think the key thing that we are missing in all of this is limited budgets, even for political advertisers, and they want to spend those budgets really well to reach the audiences that are interesting to them. When I, as a user, take all of these things out, the way the advertiser is most likely to find me is a very broad-based campaign, advertising to all users in the UK. That is going to look more similar to a TV campaign or others that are quite expensive per person because by definition I will reach a bunch of people who are not interested or are not even eligible for this particular issue that I am concerned about.

The way our systems work is that we want to provide ads that are most interesting to you, so if there is a broad-based campaign running and there is something that is more local, like a coffee shop around the corner from me, it is much more likely I am going to get that ad than this



## HOUSE OF COMMONS

broad-based campaign because it is much more expensive for that advertiser to deliver that. I agree that there is not one big master control but I can set this set of interests I have. I can tell Facebook, "I don't like this particular ad", even though I am not blocking the advertiser, because maybe the content is not good. We will use that to say we are going to show fewer ads like this.

Through this set of controls you can dramatically reduce that sort of experience. We are motivated to show you the ads that you want to see, so if you do not want to see the political ads you are not going to click on them. You are going to X them out and say, "I don't like these ads" and very quickly you are going to get into an actual product experience that has few to none of those ads on the platform. It is not within our incentive to show you things that you don't like. That is counter to the whole basis of our business.

**Q2120 Chair:** Yes, but the concern we have, particularly looking at political messaging and political campaigns—and this is very different from a lot of the consumer advertising you would find on Facebook—is that people are launching highly specified campaigns. They are creating custom audiences based on people's opinions, their fears. It is based on geographies. It is a tool to target messaging at them and it is augmented by getting lookalike audiences from Facebook to target people with stuff the advertiser thinks they want to see. There is no real protection for a voter against that at all because from what you have said, even if they have opted out of political messaging, they would still receive it and if someone came to you with a custom audience and asked you to create a lookalike audience you would include them in that as well. In very specific political campaigning, this is being used as a really powerful tool to reach people with messaging that they may not want to receive or to try to influence their behaviour.

**Mike Schroepfer:** I appreciate the line of questioning because political advertising is a really important issue. I want to clarify a few things. Once again, what you are raising is this issue of targeting these small audiences or targeting based on interests and you used the word "fears". I want to clarify a couple of things. First of all, we think one of the best tools to work on this problem is to give everyone radical transparency on what is happening here. One of the concerns that has been raised is what if an advertiser is targeting just this segment of the audience. That is why in June you will be able to see for any particular advertiser the entire spectrum of ads they are running at this moment in time and who they are advertising them against. We are going further for political ads because we understand how important it is and we are releasing extensive information about those political ads, including who they were trying to reach, how much they have spent, how many times they were viewed—very detailed information about the political campaigns. This is the work we are doing in time prior to the UK election in 2019.



## HOUSE OF COMMONS

The questions you are raising are important and the way to really answer them is for everyone—you don't have to bring me out here. Anyone who is interested in researching this topic wants to make sure that things are being used appropriately, has the ability to see in real time what is going on and then after the fact if they want to do analysis we can do that through an historical log. The issues you are raising are important and I think getting into the details of how these things are actually working is really critical. I disagree with one point, which is once I remove a bunch of these interests and other things, it is harder for advertisers to target me directly. They have to reach me through some of these broader-based campaigns. That is the basis of these controls.

In general what we find when we work with advertisers, both political and not, is messages that people want to receive, that they like, are the ones that work the best. This is not about fears or profiles of people. This is about that in the commercial sector if you send me a tea ad I am not going to click on it because I am a coffee drinker. In the political sector, there may be issues that I am very passionate about and issues that I am not passionate about. Talking about the issues I am passionate about is probably a better way to engage me and that is the thing that the content of the ad and how people engage with that ad is probably the biggest signal in that. If people run ads and people just look at them but don't engage in any form—they don't click, they don't visit a website to buy a product, they don't visit a coffee shop—those ads are going to be ineffective and expensive.

**Q2121 Chair:** As I say, I think there is a big difference between consumer advertising and political advertising, and I think we have seen that from the content. Just looking at the content that was presented to the United States Congress, content that came from ads run by the Internet Research Agency in St Petersburg, a lot of those were fear-based, highly targeted; they are seeking to influence people's actions and behaviours, making people turn up to fake rallies and demonstrations. This is the reality of how these tools are being used. Transparency is good and what you are suggesting on transparency is helpful but all that means is that the Russians, rather than doing it from an office in St Petersburg, would have to find a different mechanism for running the advertising. The transparency shows you who is doing it but it does not allow you to stop what is happening.

**Mike Schroepfer:** I agree with you on a few things. The first is I agree with you that political ads are in a different category and this is why we are doing a whole bunch of work very specific to political ads. There is transparency work and others. I agree with you 100% that we need to provide tools to protect against bad ads and tools to help everyone, yourself included, understand how these tools are used. I also want to highlight that what happened in 2016 with the Russian Internet Research Agency, the Russian IRA, is awful. It is a terrible idea that a nation state would be using our products to interfere in the elections of a democratic nation. It is against everything we stand for and the key weapon in that



is to find out the actors. The problem here is that they were masquerading as citizens of the US and spreading issues on the site. Being able to identify them and take them down, which we did after the election, and what we are doing now is proactively looking for actors like that on the platform. That is why last month we announced that we had taken down another 270 pages, including an alleged news site based in Russia, because we found detailed technical links between those and removed them from the platform. They can't post organically or advertise. That is an issue that is of great importance too in the ongoing fight against those sort of adversarial actors. I would agree with you.

**Q2122 Chair:** You are quite right that the ads that were found were Russians masquerading as Americans, but not very successfully because they were making payments in roubles to run the advertising, which is in breach of US election law because they were making those payments from Russia. Why didn't the Facebook ad review team spot that at the time and stop the advertising?

**Mike Schroepfer:** We were slow to understand the impact of this at the time.

**Chair:** Yes, about six months after the event or longer, a year after the event.

**Mike Schroepfer:** I understand and I am way more disappointed in this than you are. I am sorry, I shouldn't have said that.

**Chair:** It is a high bar.

**Mike Schroepfer:** You are right. I am sorry, I shouldn't have said that. I just want you to know that it is something that we are working very hard on. It is a critical issue and this is why we are taking proactive enforcement against these.

**Q2123 Chair:** Did the Internet Research Agency use any particular Facebook targeting tools in their advertising?

**Mike Schroepfer:** I don't know specifically what tools they used in the advertising offhand. If it is of interest to you I am sure we can follow up with that information.

**Q2124 Chair:** Yes. I think it is quite important. We have been talking about a number of different tools that political advertisers could use. Did the Russians use those same tools? Did they have a custom audience for state-by-state campaigns or did they use lookalike audiences for Facebook as part of their advertising spend?

**Mike Schroepfer:** Yes. Unfortunately I don't have that because that is with the US election. I came prepared with information for you on particularly Cambridge Analytica and issues here. I did not come with the figures on what tools the IRA used. If it is important, I will be happy to follow up shortly after the Committee.



Q2125 **Chair:** I think it is important to us. We have lots of questions about the other topics we will come on to. These tools could be used across the board. We have been concerned about Russian activity in UK elections, in the referendum, in other elections here. After several times of asking, Facebook did some work looking to identify that, after initially saying they wouldn't. Facebook also said that is not necessarily a complete survey. The reason the IRA case in regards to the American elections is interesting is that it is the most exposed and we want to understand what happened to make it easier to identify similar activity in the UK as well.

**Mike Schroepfer:** Absolutely, and we would be happy to follow up offline. I want to make sure you have all the data you need. I want to clarify one thing. We did look several times to understand connections between the Russian IRA and the Brexit referendum in 2016 that you mentioned. We found \$1 of spend and this is us looking through all the same means that we have been using to find this information proactively. This is the extent of what we found, which is almost nothing. I would be happy to share that.

Q2126 **Chair:** It could have been done in other ways, I think. We don't know that it happened but if it did happen it was done in a different way. We can say that.

**Mike Schroepfer:** I can't prove a negative and the challenge with these things is that we are dealing with adversarial actors. These are paid adversaries in a building who work nine to five, trying to exploit radio, TV, internet, Facebook, all different forms of medium, for whatever their political goals are. I also want to highlight that we have been reacting much more aggressively to this, by both human and technical means, but we treat this as an ongoing issue not something that we have looked at and clarified. There is a day-to-day fight on these things. The key thing here is people trying to create inauthentic identities on Facebook, claiming they are someone other than who they are. To give you a sense of the scale of that problem and the means, while we are in this testimony today it is likely we will be blocking hundreds of thousands of attempts by people around the world to create fake accounts through automated systems. This is literally a day-to-day fight to make sure that people who are trying to abuse the platform are kept off it and to make sure that people use Facebook for what we want it for, which is to share it with our friends.

Q2127 **Chair:** I think that is right. That is why I asked the question about what tools the Internet Research Agency might have used because understanding the tools they have used is vital to understanding how you can disrupt that activity and understand it better. You say you don't know. Are there people at Facebook who would know that? Is that something Facebook knows?

**Mike Schroepfer:** Yes. If the specific ad campaigns are important, I am happy to provide that information. I just don't have it in front of me. The biggest weapon we found in this defence is to find the actor, find the



account and take it down. If they are running hundreds of ads and we can take down the account, we stop all of those and stop all future ads. Whether they are advertising broad, using lookalikes, using interest, it is to some degree the root cause is identifying the actor, someone who might be IRA rather than a legitimate advertiser. All of our energy is focused on how do we consistently identify people like that on the platform, either at registration time or after, and get them off the platform as quickly as possible. This is one of the reasons I do not have that information because our focus and energy is on keeping those people off our platform.

**Q2128 Chair:** In cases like that—and there are similar cases in the UK and we will come on and talk about some of those—would the UK Information Commissioner’s Office have access to the data analytics tools used on Facebook to support targeting to look at whether it breaches the law or how bad actors are doing it?

**Mike Schroepfer:** As we mentioned before, I visited the office personally this week. We are providing them extensive information, including access to senior personnel. We are doing analytics for them to understand issues related to Cambridge Analytica and others. We are also working with your Election Commission on issues related to the election, providing them all the same information. Any time that they need information for their investigations, we are working our hardest to give it to them.

**Q2129 Chair:** I want to ask a couple more questions about the news feed in particular. Do you think there is a case for saying that political advertising should not be in the news feed?

**Mike Schroepfer:** I will tell you the conversation we had, which is that this is not an issue of revenue for us. Political advertising is a very small, low single-digit percentage of our overall advertising. The decisions here have nothing to do with money or revenue. What we do know is that advertising is a critical way to reach audiences and particularly those who don’t have an established name, who are running for a new office and would like to reach people. The combination of being able to reach them organically via pages and via advertising is a powerful tool of free speech. There is a number of challenges that you have raised and there is a number of things we need to do better. Transparency is the most important so we can see that the bulk of this advertising happening is legitimate advertising from legitimate political actors who are trying to reach their constituents. Saying that we would just cut all of them off for access would probably in many ways do harm to people’s ability to reach their audience and constituents.

**Q2130 Chair:** Or you could arrange it differently. When I go on my Gmail account, Google sifts out promotional messaging, messaging from social networks that I am a member of, from my main e-mails. Facebook looked at doing something similar through Explore, putting paid advertising from brands, political organisations in a different feed, not the news feed, and you abandoned that experiment. Why was that?



**Mike Schroepfer:** What we have found time and time again is experiences that are natural and seamless. The basic experience that people have in Facebook is you launch it and go to your news feed. It is the first thing in the product and it is the way that I am able to keep up with my friends and family. My family lives all over the country and are far away from me, so it is a way for me to share with them what is going on with my little kids on a daily basis. That is the best part of Facebook. As I am scrolling through it I will get updates from friends, primarily, but also from pages that I have shown interest in. Putting the advertisements directly in line rather than the disruptive sort of stop your experience, put it over here or make me go to another tab to find those things is something that is a better overall consumer experience.

Q2131 **Chair:** You have made a lot of money out of running ads in the news feed as a company, haven't you? When that change came in it did a lot to grow advertising revenue on Facebook.

**Mike Schroepfer:** This is the basis of when we moved to the mobile platform, mobile is a constrained device so there is not a lot of—

**Chair:** Only so many buttons you can have at the bottom.

**Mike Schroepfer:** The key thing here is when you are doing advertising in mobile it can be very disruptive—I am sure you have used an application that takes over your whole screen and you are hunting around looking for the X to get this thing out of my way before I get to the thing I am actually trying to do; that drives everyone sort of crazy—or you can integrate the advertising into the experience. I am never stopped or disrupted. If I don't like this ad, just a flick of the finger and it has gone. It is scrolled right past me. Just like the story from my friend who posted the third cat video of the day, that goes right past me on the news feed. That detailed integrated experience, where it is not somewhere else and it is not disruptive, is the thing that we have found is a better consumer experience. You are right, it has been good for our business because we have found when we build things that people like and work well our interests are aligned; it is also generally good for our business.

Q2132 **Chair:** From what I have read about, the research that Facebook did on the pilots of Explore was that users did not like the separation, but it could just be that they were not engaging with ads as much because they found they did not need them. They did not miss them from the news feed. They were happy with the content they got from their friends and family and colleagues, the things that they are directly interested in, and they were not necessarily that bothered about receiving pushed promotional advertising.

**Mike Schroepfer:** What we found is that the integrated news feed product is the basis of the products we have built. If you look at many other products that are like ours, they are very similar. I think they have come to similar conclusions about having an integrated place that I launch and scroll and I do not have to think much about navigating



## HOUSE OF COMMONS

around to find all these different things, and I can get updates. That is the basic power of the product. Instead of sifting through a big inbox, I can, with a simple scroll on my cell phone, get quick updates on my brother and my sister and my mum who are all in different places than I am. That ability to connect with people easily is the basis of the product.

**Q2133 Chair:** Facebook, and Mark Zuckerberg in particular, seem to have gone through a Damascene conversion on the issue of fake news over the last few months, from that it was not a problem to now recognising that it is a problem. The reason I am going to ask you about this is that you said that Facebook is the network that connects people around the world, with huge audiences and huge numbers. The combination of the news feed plus targeted advertising has been probably the catalyst for fake news organisations, be they the Russians or people creating click rate spam news or bad actors seeking to influence the outcome of elections. This is the pipe through which the fake news comes and there does not seem to be that much you can do to control it, other than asking users to block out things they do not want to see.

**Mike Schroepfer:** I disagree that there is not much we can do. We are a product that is based on free expression. The basis of the product is I launch it and I can have a box or I can type what I want, I can share a link from any news article or any website I want and I share it with my friends. That is the meat and potatoes of what our product is and we believe very strongly that the individual's right to share what they want is critical to free expression. The evolution that has happened over time is we have realised that, as I think you are asking, that same platform can be abused by bad actors. It can be a nation state; it can be a spammer who is just trying to make money; it can be someone who is trying to spread spam or malware. When I am not here talking to you, my primary job back home is to build our technological systems and to do things like build capabilities that are state of the art around the world and have been immensely successful in reducing the sort of content that is not welcome on Facebook. If we had time, I would love to go into lots of detail on the things we are doing there. I agree that it is a problem and it is something that we are making good progress on but have a lot of work to do.

**Q2134 Chair:** You have probably been aware since you have been in the UK of the issues raised by Martin Lewis about the use of his image and profile by fraudsters seeking to scam people into investing in schemes that they falsely claim he has endorsed. Have you seen anything on that?

**Mike Schroepfer:** I have seen news report on it, yes.

**Q2135 Chair:** He makes two points I want to ask you about, which I think are quite important. First, it is often beholden on him as an individual to complain to Facebook about the adverts but if they are not being served to him, certainly if they are being posted as dark ads, how can someone complain about an ad that they can't see?



## HOUSE OF COMMONS

**Mike Schroepfer:** You have raised a couple of issues there and I think they are critical, so I am going to take each of them. The first is the core issue of fraudulent ads is a problem and it is not welcome on our platform, whether it is this case or others. We have both manual and automated systems to try to detect these systems, but these are people who are financially motivated to try to evade whatever systems we have in place. We use things to classify these ads in a certain way. They will abbreviate the name, so instead of Martin Lewis they will say M Lewis or they will misspell the name slightly such that even when we put in technical measures they will work around it. They keep running ads and they will get blocked and blocked until they figure out they can get one. This is a place where taking down the actor is often the most important thing.

In the case of Mr Lewis, he reported in the order of 50 ads to us. As a result of that we did a more extensive investigation using our technical tools, found thousands of other ads that were a problem, and took all of those down proactively. More importantly, we found the dozens of actors, people who are fraudulently advertising on the platform and took them off the platform. That obviously takes everything they have advertised and prevents them from advertising in the future. I think that is the important thing.

The second issue you raised is also an important one, again about transparency: how does he see these things? This is where in June you will basically be able to see every running ad on the platform. I want to highlight that I think we are trying to catch all of these things proactively. I do not want the onus to be put on people to go and find these things and people reporting. We are trying to get to a mode over time, particularly with technical systems, that can catch this stuff upfront. We want to get to a mode where people reporting bad content of any kind is the sort of defence of last resort and that the vast majority of this stuff is caught upfront by automated systems. I know that is true of authentic accounts, bad content on the platform; 90%-plus of nudity on the platform is flagged and removed by automated systems before any human ever sees it, which was not true five years because we did not have the technical capability. That is the future that I am personally spending my time trying to get us to so that people like Mr Lewis don't have to spend time doing it because our systems do it for him.

Q2136 **Chair:** But Mr Lewis said he does not advertise himself. He does not use any adverts that have his image in. Why doesn't Facebook use the facial recognition technology it already has to identify ads posted by fraudsters using his image to prevent them going up?

**Mike Schroepfer:** The first thing is that we have not had facial recognition enabled in the EU until just recently. It was not even a feature we could offer to our users, so we are just in the process of rolling that out, so we need to do that first to make sure we can offer that feature for consumers. We are investigating ways to do that. It is



challenging to do technically at scale and it is one of the things I am hopeful for in the future that would catch more of these things automatically. Usually what we end up doing is a series of different features would figure out that these ads are bad, so it is not the picture, it is the wording. We will catch classes of ads and say we are pretty sure this is a financial ads and maybe financial ads we should take a little bit more scrutiny on upfront because there is the risk for fraud. This is why, for example, we took a hard look at the hype going around cryptocurrencies and decided that when we started looking at the ads being run there the vast majority of those were not good ads. We just banned the entire category and said, "You can't run cryptocurrency ads because we think the likely harm to the consumer is high there". When we can do things like that, combined with catching the actors—because this is ultimately a person who is running a fraudulent ad and get them off the platform—that is the really effective long-term defence of these things.

Q2137 **Chair:** You can run facial recognition at scale, clearly, as a business?

**Mike Schroepfer:** I am happy to dive into the details on this. I am not sure we have the systems yet to be able to do that, running this across 2 billion people for every single ad that is uploaded, to figure out—

Q2138 **Chair:** But you are running facial recognition across 2 billion users for their pictures and things. The idea is that you have facial recognition software and you could automatically tag on their pictures unless they have opted out of that.

**Mike Schroepfer:** The challenge here, and forgive me if I go into some detail, is that when any of these systems happen and you are trying to match, there is this ad running, is this particular—does it match, the larger the search space you use if you are looking across a large set of people, the more likely you will have a false positive, that two people tend to look the same and you will not be able to make automated decisions that said this is for sure this person. This is why I say that it may be one of the tools but usually what ends up happening is a portfolio of tools. Maybe it is something about the image, maybe the fact that it has Lewis in the name, maybe the fact that it is a financial ad, wording that is consistent with financial ads, and we tend to use a basket of features in this in order to detect these things. You are right, the thrust of this is that we are working hard to provide more technical means that move this from reactive to proactive, which means we catch this stuff at creation time and it does not run on the platform and harm a consumer, which is the most important thing, and it does not put work on anyone else to go and chase these things down.

**Chair:** My concern over this section we have just discussed is that a lot of the tools do seem to work for the advertiser more than work for the consumer.

Q2139 **Simon Hart:** What is Facebook's definition of a political ad and how



## HOUSE OF COMMONS

much money are you spending on this project as a percentage of your annual turnover?

**Mike Schroepfer:** This project to provide the archive of political and social ads? Is that what you are referring to?

**Simon Hart:** The wider description of what you are doing to tackle this problem. Presumably there is a budget and we wondered what it was.

**Mike Schroepfer:** On all of these issues, I don't know the specific budget. Let me explain why I don't, because I don't review dollar figure budgets on a regular basis. We talk about priorities that the teams are working on. I can't remember a meeting in recent memory with our advertising team that was not about protecting ads transparency or political advertisements. The whole focus of that team for quite a while now, the senior leadership team in particular, has been on these issues.

Q2140 **Simon Hart:** Okay, and the definition of a political ad?

**Mike Schroepfer:** There are two categories of this. There is a lot of detail here that I want to make sure I don't get wrong in this proceeding, so if we want detailed information let's follow up in writing. The gist of this is that there are ads run by a candidate, which I think everyone can understand, a political ad run by a candidate for a campaign. The more challenging part of this is issues of political interest during a campaign. I think that honestly the really hard part of this is defining exactly what the scope is of those issues. We have been working with third parties and others to define more public lists of interest in these things and this is the area that if you are interested in getting into the details I would be happy to provide more details on, because it is work in progress on that. It would be easier for us to implement just the first but we have said that as hard as this is, we think it is important, because a lot of the issues the Chairman has raised are not about a candidate running an ad. It is about broader issue ads. Whatever we do we have to figure out a way to correctly encompass that.

Q2141 **Jo Stevens:** Mr Schroepfer, I am going to ask you some questions about Cambridge Analytica and SCL and Facebook and GSR. You will know that we had Dr Aleksandr Kogan give evidence to us on Tuesday. Did Facebook read the GSR app's terms and conditions?

**Mike Schroepfer:** We require that people have terms and conditions and we have an automated check to make sure they are there. At the time, this was in 2014 or maybe earlier, we didn't read all of the terms and conditions.

Q2142 **Jo Stevens:** You didn't read their terms and conditions?

**Mike Schroepfer:** No.

Q2143 **Jo Stevens:** Do you ever read any terms and conditions of developers who puts apps on Facebook?



## HOUSE OF COMMONS

**Mike Schroepfer:** We made a big change. This happened prior to the platform changes we announced in 2014 and the key changes we made there were twofold. One was to significantly reduce developers' access to data, for example friends' data that they could access. The second was to move to a proactive review process where if an app developer wanted access to additional data they would have to go to a review with our teams. Primarily what they are doing is looking at the app, looking at the developer, trying to understand what data that developer is asking for. If I am building a music application it makes sense that I may want to get my likes so I can understand what music I may like but getting my birthday may not be relevant. We would want to make sure what those apps are asking and there is a set of principles we have, the minimum set of data needed to provide the functionality for the consumer. That process is—

Q2144 **Jo Stevens:** Prior to you putting those measures in place, you did not ever read terms and conditions of any developer's apps that were put on Facebook; is that right?

**Mike Schroepfer:** I can't say we never read them. I think it was not a requirement that we read them.

Q2145 **Jo Stevens:** What was the date when Facebook found out that the data from the GSR app was being used in contravention of terms and conditions? Was that before *The Guardian* report in 2015 or after?

**Mike Schroepfer:** My understanding is we found out about this in December 2015 from *The Guardian* report and that is when we initiated our proceedings to contact all the parties and make sure that the data was deleted.

Q2146 **Jo Stevens:** You found out from *The Guardian* report?

**Mike Schroepfer:** That is my understanding.

Q2147 **Jo Stevens:** Do you rely on the press to tell you when there has been compromised data?

**Mike Schroepfer:** No, not at all. That certainly happened in this case. In I believe it was 2011 we had started a specific program to allow people to report any issues they may have with a developer and we would follow up and do that. We had an enforcement team that would regularly be following up on these things. When we made this platform change in 2014 we would regularly be rejecting applications that wanted to be on the platform. I wish we had found this ourselves but it is certainly not the only—we definitely do find these things through other means.

Q2148 **Jo Stevens:** You mentioned having an enforcement team in 2011. How many developers did you take any enforcement action against between 2011 and 2014?

**Mike Schroepfer:** I don't have that data in front of me.



Q2149 **Jo Stevens:** Can you send it to us afterwards?

**Mike Schroepfer:** We will get you the information, yes.

Q2150 **Jo Stevens:** Thank you very much. Why did Facebook threaten to sue *The Guardian* just last month when they had given you advance warning about the story that they were going to publish, when previously you had acted on information that *The Guardian* had given to you to show that GSR had compromised Facebook users' data?

**Mike Schroepfer:** It is my understanding that we were sending them a letter to correct some facts they had in the article and it is a fairly standard legal letter to make sure that we had the facts right in the article as it was published.

Q2151 **Jo Stevens:** Why not just ask them to correct the facts? Why threaten to sue them?

**Mike Schroepfer:** My understanding—I was not involved in the specific issue—is that we do talk to them but we do also, in many cases in the UK, send a letter specifying what it is we want corrected in a story to make sure that the facts are accurate. That is what we have done.

Q2152 **Jo Stevens:** With an accompanying threat of litigation?

**Mike Schroepfer:** The broader issue is that bringing these issues to light is critical. The implication that we are trying to make these things be hidden I think is a fair question and it is not what we intend to do. This is one of the reasons, for example, we initiated a data bounty program just recently where we would pay people money if they told us about data breaches or data misuse of any form so that we can better find these things. We have been doing a similar process with bug bounty programs. I would always prefer that we stop these things in advance or catch them ourselves but the first goal is to protect people so if there is data out there that we do not know about we can't protect it, so we want people to find it.

Q2153 **Jo Stevens:** We are trying to protect freedom of speech here and freedom of speech through accurate newspaper reporting. I am sure you can understand why we think it is bullying to threaten a newspaper with litigation when they are actually pointing out to you faults with your own organisation or its governance.

**Mike Schroepfer:** It is my understanding that we did not threaten to sue, but the broader point is I agree with you that the media is absolutely critical to raise these issues and they and others have raised critical issues. Through bug bounty, through the journalism, through internal systems we need to find these issues. As I talked about before with ads, we think transparency on all these issues is the most important tool in the long run to make sure that everyone agrees that these systems are working in the ways they want. I agree with you that we want independent and vocal journalism.



## HOUSE OF COMMONS

Q2154 **Jo Stevens:** Let's go back to December 2015 when you find out via *The Guardian* that GSR has compromised Facebook users' data. What did you do at that point?

**Mike Schroepfer:** We contacted the parties involved, Mr Kogan, Cambridge Analytica and others, and I believe we went through a process of certifying through them that the data either did not exist or was deleted and had signed-off agreement from them that that was the case.

Q2155 **Jo Stevens:** Who were the others that you mentioned? You mentioned Kogan, Cambridge Analytica and others.

**Mike Schroepfer:** There was Mr Kogan, Cambridge Analytica and I believe there was two other parties involved. I am happy to provide that in private session. I do not know if that information is on public record yet and I know that there is an ongoing—

Q2156 **Jo Stevens:** I would like you to answer the question, please. Who did you contact? Who were the two others?

**Mike Schroepfer:** Immediately after these proceedings I am happy to give you that information. The only reasons I am being careful is I know that your Information Commissioner has an active investigation ongoing and I do not know if the names of all these parties are out there. I want to be deferential to their investigation, but I will provide you the information immediately after in a private non-public session.

Q2157 **Chair:** There is no reason in law why you cannot provide that information now. It is not sub judice. There are no charges being brought by the Information Commissioner. You are free to say that now.

**Mike Schroepfer:** Okay. My understanding is there was a researcher at the University of Toronto and it was Mr Wylie and his company.

Q2158 **Jo Stevens:** How did you ensure that the data had been removed or deleted?

**Mike Schroepfer:** We retained outside counsel and had legal certification that that data was deleted.

Q2159 **Jo Stevens:** That was not just data. Was that derivatives? Did it cover everything? Did you check that everything had been deleted?

**Mike Schroepfer:** They were required to certify that all of the data and its derivatives were deleted.

Q2160 **Jo Stevens:** You took them at their word?

**Mike Schroepfer:** It was a legal certification so, yes.

Q2161 **Jo Stevens:** Does Facebook plan to take legal action against Aleksandr Kogan or against Cambridge Analytica?

**Mike Schroepfer:** I think the key concern that brought all of this to light is recent events where there are the allegations that Cambridge Analytica



## HOUSE OF COMMONS

still had this data and that is the thing that brought all this to light. We had started an investigation and have deferred to your Information Commissioner who is doing an ongoing investigation of them. We want to wait and defer to theirs before we understand what legal action we are going to take against any of the parties.

Q2162 **Jo Stevens:** You have not ruled it out?

**Mike Schroepfer:** We want to basically get to the heart of the matter first before we talk legal issues. Understanding the facts of the situation is the key thing here.

Q2163 **Jo Stevens:** Does the non-disclosure agreement that Facebook has signed with Aleksandr Kogan, which he told us about on Tuesday, prevent you or him from taking legal action in the future?

**Mike Schroepfer:** I am not actually sure. I have not reviewed that document in detail so I am not sure.

Q2164 **Jo Stevens:** Aleksandr Kogan gave us evidence on Tuesday that he had been made to sign a non-disclosure agreement with Facebook and he would not answer our questions because he is under duty under that disclosure agreement. You don't know anything about the agreement?

**Mike Schroepfer:** I will tell you that that was a confidentiality clause that was part of the legal agreement we had certifying that this data was deleted and removed. There is a standard confidentiality clause in it, like in any other contract. We contacted Mr Kogan's lawyers. It was a surprise to me on Tuesday that he felt he could not talk about this, so we clarified yesterday with his legal team that we are happy for him to discuss all the matters involved here.

Q2165 **Jo Stevens:** If he is happy, I am sure you are happy to discuss it as well. What was the date of the agreement?

**Mike Schroepfer:** I don't know the exact date of the agreement. I am happy to talk with my legal team and we can provide the legal agreement in its entirety to you after this proceeding.

Q2166 **Jo Stevens:** I think you are going to be here for quite a while, Mr Schroepfer, so perhaps your colleagues behind you can find out and give you the information so that you can tell us during the hearing today when it was signed, why it was necessary, who was party to the agreement and whether any payment was made to Dr Kogan in order for him to sign the gagging clause, the non-disclosure clause that you have referred to. Perhaps your colleagues could find that out. Thank you.

Q2167 **Chair:** Just on that point, you rightly asked for Facebook to provide that information to us. From what you said, Mr Schroepfer, hearing what you said in this forum, if Aleksandr Kogan wished to provide that information to us there would be no restriction on him doing so. Is that correct?

**Mike Schroepfer:** I want to make two things very crystal clear. I am happy to provide the documents in their entirety to this Committee



## HOUSE OF COMMONS

immediately after these proceedings, and I want to be clear that we contacted Mr Kogan yesterday and I am saying to you today that any thought that there is any confidentiality, we waive any concerns of that. We want to make sure the truth of this matter comes out and Mr Kogan feels free to discuss it. I think he has been very forthright in what he said and we want to make sure that that information gets to you and others.

**Q2168 Jo Stevens:** When you realised about this data compromise and the unlawful use here in the UK of that data, did you inform the Information Commissioner's Office here in the UK?

**Mike Schroepfer:** I don't believe we did.

**Q2169 Jo Stevens:** Why not?

**Mike Schroepfer:** At the time we thought that the matter was resolved. We had received legal certification from all the parties involved that the data was not there again. The issue at hand was a developer had used our platform, collected some data and then resold that data to a third party. That reselling of the data was the issue. We had thought that the matter was resolved.

**Q2170 Jo Stevens:** Facebook felt they had no responsibility to report to the Information Commissioner that it was the fault of the developer. This is the developer that Facebook had not read the terms and conditions of its app that went on to Facebook in the first place, is that right?

**Mike Schroepfer:** We did not inform the Commissioner at the time.

**Q2171 Jo Stevens:** Do you intend to take any legal action against the University of Cambridge?

**Mike Schroepfer:** I am not aware of any pending legal action on any of these matters. The first priority for us is to make sure all the facts of the matter get written out. This is again why I want to defer to your Information Commissioner, the Electoral Commission and others. We want to give them all the data they have. We want to not get in the way of those investigations, so that they can do this. This is why, for example, we had begun an audit with Cambridge Analytica but stood down at the request of your commissioner so they could take precedence. I am not aware of any current plans to do legal proceedings. I think our priority right now is to understand what has happened and to co-operate fully with the Information Commissioner and others.

**Q2172 Jo Stevens:** Were you aware that there were other employees at the University of Cambridge building apps that were similar to the ones built by Aleksandr Kogan?

**Mike Schroepfer:** I do not think so.

**Q2173 Jo Stevens:** You mentioned that you have contacted all the Facebook users whose data was compromised, UK Facebook users.

**Mike Schroepfer:** Yes.

Q2174 **Jo Stevens:** When did that happen?

**Mike Schroepfer:** That has happened over the last few weeks. This is a control that has showed up in the very front of the product at the top of the newsfeed for every single one of the people affected by this across the world, including everyone in the UK who was affected.

Q2175 **Jo Stevens:** It is two and a half years since the breach occurred and you are only now telling the affected users. Why the delay?

**Mike Schroepfer:** As Mark has said himself, in retrospect it was a mistake we did not inform people at the time. This is why we are informing people now and committing to do so in the future.

Q2176 **Jo Stevens:** Why did you not inform them at the time? What was the decision process, who made that decision?

**Mike Schroepfer:** I do not know who made that decision.

Q2177 **Jo Stevens:** You are the Chief Technology Officer, Mr Schroepfer, why don't you know?

**Mike Schroepfer:** I understand. I was not involved in the discussion. I do not know what happened. I am guessing the key thing at the time is the teams were focused on making sure people's data was safe and deleted and not used. That was the priority at the time.

Q2178 **Jo Stevens:** It was a bit late for that, wasn't it? Don't you think? Going on to the ICO and the investigation into Cambridge Analytica, why did Facebook choose Stroz Friedberg as the auditor for Cambridge Analytica?

**Mike Schroepfer:** I do not know the specific selection process for that particular forensic auditor.

Q2179 **Jo Stevens:** Who made the decision?

**Mike Schroepfer:** I believe it was the team investigating the issue.

Q2180 **Jo Stevens:** Who heads that team?

**Mike Schroepfer:** There are several people on the legal team working on this, on the privacy team and on the platform team. I do not know exactly who chose—

Q2181 **Jo Stevens:** Who heads the team, please? Do you know who heads up that team?

**Mike Schroepfer:** Which team? We have multiple teams working on this.

Q2182 **Jo Stevens:** Who has overall responsibility for the people who are doing that investigation?

**Mike Schroepfer:** There is a person on our platform enforcement team who is leading up the audit of all the applications on the platform.

Q2183 **Jo Stevens:** Who is that person?



## HOUSE OF COMMONS

**Mike Schroepfer:** With respect, I prefer not to name people in a public setting. If it is of interest to this Committee I am happy to give it to you after the fact.

Q2184 **Jo Stevens:** This is an investigation by the ICO and you say you will co-operate in any investigation.

**Mike Schroepfer:** They have this information.

**Jo Stevens:** We would like to know who is responsible in your company for that.

**Mike Schroepfer:** I understand, and we have provided that information to it. I am happy to provide this information to you. These proceedings are public and I am trying to be sensitive to naming individuals in a public proceeding.

Q2185 **Jo Stevens:** What is sensitive about it? There are details for who is responsible for different parts of Facebook publicly available. I do not understand the sensitivity.

**Mike Schroepfer:** Again, with respect, I am happy to provide this information. If your goal is to get the information, I am happy to provide it to you. I am not sure why it needs to be broadcast on public TV.

Q2186 **Jo Stevens:** When did Facebook hire Joseph Chancellor?

**Mike Schroepfer:** I believe in 2015.

Q2187 **Jo Stevens:** When in 2015, do you know?

**Mike Schroepfer:** My recollection is November of 2015.

Q2188 **Jo Stevens:** Just before *The Guardian* told you about the data breach. Were you aware that he was a cofounder of GSR?

**Mike Schroepfer:** I don't believe we were.

Q2189 **Jo Stevens:** When did you find out that he was a cofounder of GSR?

**Mike Schroepfer:** I think we first learned about that fairly recently. It was well after the December 2015 event. I would have to look at records but it might have been as recent as last year.

Q2190 **Jo Stevens:** When *The Guardian* were working on the stories I have talked about in 2015 and in March 2018 about Cambridge Analytica, were you aware that Joseph Chancellor was an employee of Facebook and a cofounder of GSR?

**Mike Schroepfer:** We did not understand his possible involvement in this until quite recently, so not in 2015.

Q2191 **Jo Stevens:** Have you investigated the work that Joseph Chancellor was doing with GSR?

**Mike Schroepfer:** We are doing so now.



## HOUSE OF COMMONS

Q2192 **Jo Stevens:** You are doing it now. Have you made him sign a non-disclosure agreement?

**Mike Schroepfer:** Not related to this issue, no.

Q2193 **Jo Stevens:** You have made him sign one related to other issues?

**Mike Schroepfer:** Every employee in the company has a non-disclosure agreement as a standard part of our employment clause.

Q2194 **Jo Stevens:** Is that part of the employee contract or is that a separate agreement? If Facebook employs somebody, do they automatically make them sign a confidentiality clause?

**Mike Schroepfer:** Yes, because every Facebook employee is exposed to a lot of confidential information on a daily basis and we want to make sure that they understand that. One of the things that we try to do as a company is to be very open with what is happening and publish information quite widely, so it is important that every employee knows that we share things with them are not yet public information and we want to make sure they understand to keep that confidential.

Q2195 **Chair:** You made Dr Kogan sign an NDA and he is a director of GSR, but you did not make Joseph Chancellor sign an NDA, and he is a director of GSR.

**Mike Schroepfer:** I want to be clear. In the proceedings that happened post-December 2015, Mr Kogan was the author of the application. In our platform tools it was his name on the application. He said himself that he wrote the application. In the agreements that we had signed with the parties involved, it was Mr Kogan. Mr Chancellor was not mentioned in those agreements. It was not an NDA, it was a confidentiality clause as a part of the contract for that agreement, which I will provide to you after these proceedings.

Q2196 **Jo Stevens:** I think Mr Chancellor co-signed GSR's 4 June 2014 agreement with SCL Elections, obviously an affiliate of Cambridge Analytica. Have you ever seen that document?

**Mike Schroepfer:** No, I have not.

Q2197 **Paul Farrelly:** I am not going to dwell on this, but if you only found out recently about Mr Chancellor's involvement with Dr Kogan, you have either not asked him for his CV or he has missed it off his CV.

**Mike Schroepfer:** I do not know exactly why we did not know but I am telling you the facts that I know.

Q2198 **Chair:** When you said recently, I think you also said last year, is that correct?

**Mike Schroepfer:** I believe last year is the first time we understood his involvement.

Q2199 **Chair:** When *The Observer* reported on the data breach earlier this year,



## HOUSE OF COMMONS

you were aware that Joseph Chancellor had worked with Aleksandr Kogan at GSR?

**Mike Schroepfer:** Yes. To understand the timeline here, the issue is that in the most recent article the allegations were that the data still existed. Our key concern is does Cambridge Analytica still have this data, which is in violation—that is when we started the investigation of all of these things with Mr Kogan, Mr Chancellor and others.

Q2200 **Paul Farrelly:** I only have a couple of questions in this section but we are going to come back to elections and manipulation later on. When we had Dr Kogan in front of us, it was quite clear that he was willing and able to play fast and loose with Facebook, because whatever Facebook's terms and conditions said in writing he thought you never enforce them. He told us that therefore, in his use of semantics, he did not consider you had a policy. It is a dubious position to hold but in this inquiry that we are doing the question is: how much does Facebook care?

**Mike Schroepfer:** We care a great deal. I disagree with the assessment that we did not have a policy. I want you to understand that the goal of the platform was for consumers to be able to use applications and take the data they have on Facebook. One of the constant pieces of feedback we get from people is data portability. They want to take the data they share with Facebook and bring it to another application, to build a great social experience. Whether that is a game or a calendar or a music app, we want to make that as easy as possible.

As we have talked about in many parts of this hearing earlier with issues of elections and ads and false news, those same tools, because they are easy and great for the consumer, can go wrong. This is why we have gone through several iterations of the platform, where we have effectively locked down parts of the platform, which increases friction and makes it less easy for the consumer to use these things but does safeguard that data more, and been a lot more proactive in the review and enforcement of these things.

This was not a lack of care. I will let you make your own assessment, because you get to be the judge, but I will tell you that our primary product is designed to help people share safely with a limited audience. If you want to say it to the world, you can publish it on a blog or on Twitter. If you want to share it with your friends only, that is the primary things Facebook does. If we violate that trust and that data goes somewhere else, we are violating the core principles of our product and that is a big problem. This is why I wanted to come to you personally today to talk about this, because this is a serious issue.

Q2201 **Paul Farrelly:** His justification for the neat little trick that he discovered where he could harvest not just thousands but millions of people's data and then sell it on for political purposes, was that he had his terms and conditions up there for 18 months, making it clear he could sell it to anyone he wanted for whatever purpose, and you never took him to task.



## HOUSE OF COMMONS

Yet you have said you try to make sure that all your developers and people who use your platform like that have terms and conditions but by an automated method. What does the automated method do, just check whether the words “terms and conditions” are there, irrespective of the content?

**Mike Schroepfer:** I think the issue you raise is again an important one. Whatever he wrote in that document, he could write terms and conditions that was a carbon-copy clone of ours and then go and do what he did, which is sell the data. The terms and conditions are one part of it but the much broader issue is how do we protect data and make sure it is there. Since the terms and conditions are a very small part of this, I think the broader issue is technically locking down the platform, proactively reviewing the application. If you are asking me do I wish we had done more of this back then—

Q2202 **Paul Farrelly:** That is rather deflecting the question. At least he was upfront about it and you never took him to task. When you did discover this app—and perhaps others, about which you will give some more details later—you stopped new people doing it but you did not stop the existing people doing it for a year. They got a year’s grace, so if you cared, you did not care 100%.

**Mike Schroepfer:** What you are referring to is in 2014 we announced the changes. Any new app had to abide by these changes, or any revisions to the app. Then there was a grace period until 2015 to have people migrate to this new API. The reason we did this is these changes were significant enough that if we had flipped them on immediately, we would break a large portion of the internet, many apps on the internet, instantaneously. Like any platform developer for a mobile operating system or a system you run on your desktop, you have to give developers time to update their applications to make sure that they do not break when the user changes to the service or uses the new API. This is a fairly standard technique to allow the applications to move so we do not break a bunch of consumer experiences across the web at the time.

Q2203 **Paul Farrelly:** You were giving a period of grace for activities to continue that you considered a disgrace.

**Mike Schroepfer:** The key thing here again, as I said, is there is a strong trade-off between ease of use and friction of the consumer, the ability for me to take all my data, including this information, to this application, and safety, which is how easy is it for someone to abuse this. You can set that pendulum in multiple places. What we were doing over time is moving much more towards safety. This was not a disgrace. The vast majority of the developers on the platform are building great experiences. These are name-brand companies you have heard of, like Spotify and Airbnb and Pinterest. If you talk to them they would say that Facebook was fundamental to helping them grow their business in the early days.



## HOUSE OF COMMONS

That was the goal of the platform and we saw a lot of great things happening. We wanted to, over time, further restrict these sorts of bad activities. There is a limit to how fast we can move to getting these things done without causing undue consumer harm. Literally, if we change some of these things, you would go and visit a site or an app, like your music player, and it would be broken because we had cut off access to the API. Doing that for hundreds of millions of consumers did not seem like the right thing to do at the time.

**Paul Farrelly:** When we come to elections we will have a few more questions about how much Facebook really cares.

Q2204 **Ian C. Lucas:** Can you confirm, following the breach in December 2015 that you found out about from *The Guardian*, that Cambridge Analytica certified to you that they had deleted the information they had from GSR?

**Mike Schroepfer:** That is my understanding, that we did get a certification from Cambridge Analytica.

Q2205 **Ian C. Lucas:** Did you receive that in writing?

**Mike Schroepfer:** I believe so.

Q2206 **Ian C. Lucas:** Could you please send us a copy of that?

**Mike Schroepfer:** I will check with the legal team. I am assuming we can but I will double-check with them and provide it for you immediately after if we can.

Q2207 **Ian C. Lucas:** You received a certification from Mr Kogan and you received a certification from Cambridge Analytica. Were there any other organisations you received a certification from at that stage?

**Mike Schroepfer:** There were multiple parties involved in these. I will provide you all the documents immediately after these proceedings that we can give you.

Q2208 **Ian C. Lucas:** When you say multiple, are you talking about 50, are you talking about three?

**Mike Schroepfer:** No, no, it was primarily Mr Kogan, Mr Wylie and Cambridge Analytica. There may have been one other. I need to provide you with the documents to get the full details.

**Ian C. Lucas:** I will return to this.

Q2209 **Julian Knight:** I apologise for my lateness. I had to answer questions on behalf of the Public Accounts Commission. Mr Schroepfer, your company spent the first part of our inquiry effectively threatening journalists with being sued, with legal action. As a former journalist myself, I can tell you the impact of that on journalists is pretty serious. People lose their homes over those things, especially when multi-billion-pound organisations come knocking. Your head of news partnership, Ms Campbell Brown, said that it



## HOUSE OF COMMONS

was a mistake to go after these journalists for telling the truth, for telling you where you were going wrong. Will you go further? Will you apologise today for this bullying behaviour by your company?

**Mike Schroepfer:** Again I want to be clear, my understanding is that we wanted to make sure the facts were straight. We believe deeply in the need of journalists to be free to investigate all of these matters. It is the same principle we have freedom of expression with our core product.

Q2210 **Julian Knight:** Sorry to cut across you, Mr Schroepfer, but why is your first instinct to send legal letters? If you are so wanting the truth and wanting journalists to express themselves, why is the first thing you did to send legal letters?

**Mike Schroepfer:** My understanding is this is common practice in the UK in terms of correcting letters. I may be wrong.

Q2211 **Julian Knight:** You are wrong. You are wrong in that respect.

**Mike Schroepfer:** The important thing is to get the facts on the matter right.

Q2212 **Julian Knight:** I am really surprised in a country that has the first amendment, you have freedom of speech and, I have to say, a very robust press, that the excuse is that it is a cultural thing and that this is normal thing to do in Great Britain. It really is not in that respect. I am going to ask you again, will you apologise for this bullying behaviour?

**Mike Schroepfer:** I am sorry that journalists feel that we are trying to prevent them from getting the truth out. That is not the intent, so I am sorry.

Q2213 **Julian Knight:** Thank you. Your boss, in a rather folksy way, said in front of the Senate Committee that there had been something bad going on at Cambridge University, I think his phrase was. Again your company is going legal, potentially. That is the implication. Isn't this simply a diversion?

**Mike Schroepfer:** I am not sure what your question is.

Q2214 **Julian Knight:** Mark Zuckerberg said that he thought there was something going bad at Cambridge University. Cambridge University is obviously, whether it is some people who have worked there, involved in some way in design of these apps. Is this not your company again looking at a diversion? You are pretending to be the victim in this respect, when it is your own looseness that has caused this information to get out there.

**Mike Schroepfer:** I want to be clear on a few things. First, Cambridge University is an excellent, fine institution. We have probably dozens, maybe hundreds, of graduates of that university working at our company. It is one of the finest institutions in the UK. I want to make that clear. Secondly, the real issue here is Cambridge Analytica and the sale of data



to them and what they did with that data. That is the primary focus of my time and energy: to understand what is happening there.

There are two components to this. There are people who did things against our terms and service and did things that we do not like. That is partially on them. We have said repeatedly that the mistakes we made were not being aggressive enough in enforcing all of these things and having both technical and operational controls over these, which we started to make changes in 2014 and have made many more, including ones that I detailed last month. I acknowledge both we needed to do more and that others had done some things here. That is the way I would look at it.

**Q2215 Julian Knight:** Your lawyers were at Cambridge Analytica, knowing full well of the involvement of the Information Commissioner. You were there when the Information Commissioner was trying to get a warrant, which hopefully we will see a speeded-up process of. What would you say to those who view this almost as an attempt to pervert the course of justice?

**Mike Schroepfer:** I want to be very clear, I still do not know what data they do or do not have.

**Julian Knight:** Your lawyers were there all day.

**Mike Schroepfer:** Yes, it takes time to analyse these systems. Our primary goal is to understand what data is or is not there and make sure that people are protected. We wanted to do that as quickly as possible. If we had dragged our feet and waited, you would rightfully accuse us of not taking this seriously. As soon as the Information Commissioner asked us to stand down so that they could take precedence, we said, "Of course your investigation takes precedence" and we moved into a mode where we are trying to provide—

**Q2216 Julian Knight:** It was just coincidental that you were there on that day, that you decided to come on that day, rather than the fact is that you knew the Information Commissioner was coming knocking and you decided to get in there in order that you could ascertain what was going on, so you could protect your own corporate position, when what you should be doing is protecting the integrity of the inquiry?

**Mike Schroepfer:** What we were trying to do is get there and get to the answers as quickly as we can.

**Q2217 Julian Knight:** Regardless of the actual inquiry going on?

**Mike Schroepfer:** Once we understood that the Information Commissioner wanted to take precedence, we immediately deferred to them with no argument. Personally I have met with the staff. We are providing extensive technical data analytics and others, to them to assist in the investigation. Their goals, your goals, our goals are all the same: to make sure we understand the facts here and what exactly happened



## HOUSE OF COMMONS

so we are not guessing at that. We wanted to get to the facts as quickly as we could.

**Q2218 Julian Knight:** Yes, damage limitation. The reason why I have asked you these particular questions is it outlines for me a pattern of behaviour, an MO, if you like, for your company: bullying journalists, threatening academic institutions and impeding, potentially impeding, investigations by lawful authorities. I put it to you today that Facebook is a morality-free zone, destructive to a fundamental right of privacy. You are not an innocent party wronged by the likes of Cambridge Analytica, but you are the problem. Your company is the problem. What do you say to that?

**Mike Schroepfer:** I respectfully disagree with that assessment.

**Q2219 Julian Knight:** You see yourself as somehow morally innocent in this respect, despite this catalogue of behaviour.

**Mike Schroepfer:** I think what you want from an organisation is transparency and responsibility. You want us to say when we are responsible for things, which we have in multiple cases. We have talked about the mistakes we have made.

**Julian Knight:** Only when you have been dragged kicking and screaming into that situation by inquiries such as this.

**Mike Schroepfer:** You want transparency on things like ads and whatnot. This is not where I spend my day job. The core of the job is to try to build a service that helps billion of people around the world connect with each other every single day. That is the core of what we are trying to do. Whether it is a nation state actor or a spammer or a developer abusing the platform, we need to do a better job policing all of those abusers of the platform, but I think great things are happening every single day on our products and that is what we try to focus on.

**Q2220 Julian Knight:** One final question. You have mentioned there about monitoring regulation. In America your spokespeople constant references to regulation. This, of course, was self-regulation, which has been shown, frankly, to have been utterly worthless. This is witnessed by the information free-for-all that we have had. Do you think the time has come for robust regulation and empowerment of consumers over their information? Do you think you effectively need regulation right now in order to ensure that there is a level playing field, everyone knows what they are doing and, crucially, consumers get real ownership over their information, what could often be quite personal information?

**Mike Schroepfer:** I agree with you on a few key things here. First of all, whether there is regulation or not, making sure the consumers have visibility, control and can get access and take their information with them, I agree 100%. We have had a feature to do this since 2011, we have made it even more robust in recent weeks and years.



## HOUSE OF COMMONS

Ironically, part of the issue of the platform is we made it easy to people to take their data to third-party developers to build great social experiences, and then abuse has ensued. The challenges with these things are we definitely want to provide control and data access and data portability. We need to balance those things with security and abuse and the bad things that happened when people can get a download of their entire data to a bad actor, so I agree strongly with that.

In terms of regulation, there are multiple laws and regulatory bodies that we are under the guise of right now. Obviously the GDPR is coming into effect just next month. We have been regulated in Europe by the Irish GPC, who has done extensive audits of our systems over multiple years. In the US we are regulated by the FTC and the Privacy Commissioner and in Canada and others.

The question is honestly how do we ensure that the regulations and the practices achieve the goals that you want, which is that consumers have safety, they have transparency, they understand how this stuff works and they have control. The details of implementing that is where all the really hard work is.

**Q2221 Julie Elliott:** I want to move on much more to what has happened in this inquiry regarding elections. Mark Zuckerberg, your boss, maintains that Facebook had no influence on elections. Can you remind us how many adverts were paid for by the Internet Research Agency in US elections?

**Mike Schroepfer:** The IRA are spending—I am sorry, I did not come with the figures for the US elections with the IRA, because I thought you would be—

**Q2222 Julie Elliott:** Can you provide us with that information?

**Mike Schroepfer:** Of course. I came prepared to talk about the UK referendum.

**Q2223 Julie Elliott:** A follow-on to that is can you remind us how many adverts were paid for by the IRA in the UK referendum?

**Mike Schroepfer:** Yes, it was about \$1 of spend.

**Q2224 Julie Elliott:** Because when we look at it, that does not seem to stack up to what we have been hearing. Are you confident that that figure is correct?

**Mike Schroepfer:** We have looked extensively at the information we can find. In the 2016 US election, the counts involved in the IRA issues there, the Russian IRA—as we announced last month, we found proactively another 270 pages that were not only the IRA but a news agency in Russia that clearly had close ties to the IRA, which was found by us. In all of these investigations we have not found any clear participation in the UK referendum. Again, these are adversarial actors that are trying to evade our systems and platforms. Is it possible we missed something? Yes. I do think we have looked pretty hard.



## HOUSE OF COMMONS

Q2225 **Julie Elliott:** Can I draw your attention to the written statement you have given us, where you have said, "Our records show that AIQ spent approximately US\$2 million on ads from pages that appear to be associated with the 2016 referendum"?

**Mike Schroepfer:** I am sorry, I thought we were talking about the Russian IRA. The figures I was giving were for the Russian IRA. If you want to talk about AggregateIQ, I will be happy to talk about that.

Q2226 **Julie Elliott:** Tell me about AggregateIQ.

**Mike Schroepfer:** Sure. As you pointed out, we did do extensive analysis, looking at my statement here, on Cambridge Analytica and AggregateIQ. When we looked at Cambridge Analytica we found no spend on the Brexit referendum. As you mentioned—

Q2227 **Julie Elliott:** Do think that it sought to influence Facebook in terms of the referendum?

**Mike Schroepfer:** I am sorry?

**Julie Elliott:** Influence Facebook users.

**Mike Schroepfer:** Who are you referring to?

**Julie Elliott:** Cambridge Analytica.

**Mike Schroepfer:** I do not know. I can just look at its activity. Given that it spent zero dollars on advertising, it is unlikely it had any effect at all.

Q2228 **Julie Elliott:** What you have said in your written statement is that it was not directly managed. What do you mean by "directly managed"?

**Mike Schroepfer:** It means that Cambridge Analytica itself, and SCL, the parent company, did not run ads on the platform related to the Brexit campaign. There may be others who have contracted their services, which we would not have visibility to. The one that we did discover when we were doing this investigation was the company you mentioned, AggregateIQ, which is a separate company, based in Canada. We looked at that company and found that it had spent US\$2 million on the Brexit referendum in the UK in 2016.

Q2229 **Julie Elliott:** Was that money declared within our election law rules?

**Mike Schroepfer:** I believe it was but I have not looked into that specific detail.

Q2230 **Julie Elliott:** If we move to the referendum itself, if Cambridge Analytica or SCL Group did not, you do not think, do adverts, do you accept that some of the organisations they were doing work for placed adverts?

**Mike Schroepfer:** I don't know.

Q2231 **Julie Elliott:** Do you have any checks and balances within your



organisation to check that type of information?

**Mike Schroepfer:** What you are asking is if an advertiser comes to us and advertises as a customer of ours, who are all the other companies they work with. I do not think that is anything any company in its general course of business.

Q2232 **Julie Elliott:** It is not business, this is elections, which in this country is covered by very different laws than general consumer things.

**Mike Schroepfer:** I understand. In this case what we are talking about is the person directly who is running the advertisement and paying for it. That is the thing that we have clear records on. If they had a consultant—not payment but if they worked with a consultant or other things, it is hard to know that. What we do have is the records of the ads they run and who paid for those ads.

Q2233 **Julie Elliott:** Going back to when you said a \$1 spend, what did you mean by that? Was that per user or per buy?

**Mike Schroepfer:** I believe that was total spend.

Q2234 **Julie Elliott:** Total spend? Did data derived from Cambridge Analytica's models get uploaded on to Facebook using the customer audience feature?

**Mike Schroepfer:** Because it spent zero dollars on the Brexit campaign, it clearly did not use that data because it did not use the product. I want to go into more detail on AggregateIQ, since that is a related company and did do spend. That is where our investigation led us to. I tried to detail in my statement some of the analysis we did on its spend. The question we were trying to get to is is it possible, because there are alleged links between Cambridge Analytica and AggregateIQ, that somehow this data made its way from—

Q2235 **Julie Elliott:** These are not alleged links, they are all part of the same organisation.

**Mike Schroepfer:** Okay. We wanted to follow the data to see if data that went to Cambridge Analytica was used by AggregateIQ for these elections. We looked at a number of different factors to understand this. The first and most important is the campaigns that it runs, AggregateIQ, for the Brexit referendum—

Q2236 **Julie Elliott:** How much did AggregateIQ spend?

**Mike Schroepfer:** US\$2 million. The campaigns it run were based on e-mail lists. It had acquired e-mail lists of people from some source. Mr Kogan's app—

Q2237 **Julie Elliott:** Do you have any idea where that was?

**Mike Schroepfer:** I was going to get to how it cannot be Mr Kogan's app because he did not get e-mails addresses from either the installer of the



## HOUSE OF COMMONS

application or from their friends, so AggregateIQ must have acquired that data from some other source.

The second question we asked is wherever this data came from, did they mix and match it with some other data that might have come from Facebook, to build these audiences. What we then did is say the people that it is trying to advertise to, what is the overlap between that set of people and the people who are affected by the "This is your Digital Life" app. That overlap was approximately 3% to 4%. We then said if you take other apps of similar install size, you get similar overlap rates, as a control, to say that based on our data scientists, this is a random overlap. It is clearly not using that data as the input into the sets of people it is targeting for the Brexit referendum. That is the analysis we have done and I detailed it in the statement.

**Q2238 Julie Elliott:** Did any of your employees alert anyone that this company had stolen Facebook user data in 2015 and was now providing data to target Facebook ads with reference to elections? Did any of your employees alert you to that?

**Mike Schroepfer:** Again, we did not inform people at the time.

**Q2239 Julie Elliott:** Would you confirm that this 3% of 87 million is 2.6 million people?

**Mike Schroepfer:** I do not believe it is 3% of the 87 million, because, first of all, it is only 1 million people in the UK were in total—

**Q2240 Julie Elliott:** How many people do you think the 3% is that you are talking about?

**Chair:** It will be about 20,000 or 30,000.

**Mike Schroepfer:** 30,000 or 40,000 people if it was 3% of that set, but this is a 3% overlap between the two because the audiences it was using may have been bigger or smaller than 1 million. It is, at maximum, 30,000 or 40,000, but may be less, based on the audiences that it had.

**Q2241 Julie Elliott:** The £2 million you have referred to that was spent, was that spent in the US, Canada or the UK?

**Mike Schroepfer:** I do not know offhand, and I believe it was US\$2 million. I do not know there that was spent. If that particular detail is important, I am happy to make sure we follow up.

**Q2242 Julie Elliott:** Could you provide us with that information in writing?

**Mike Schroepfer:** Of course.

**Q2243 Julie Elliott:** How many UK Facebook users and Instagram users were contacted in the UK referendum by foreign, non-UK entities?

**Mike Schroepfer:** I do not know the answer to that question.

**Q2244 Julie Elliott:** Can you find out the answer to that question? Is that



## HOUSE OF COMMONS

information that you would hold?

**Mike Schroepfer:** What is the specific question again?

Q2245 **Julie Elliott:** How many UK Facebook users and Instagram users were contacted in the UK referendum by foreign, non-UK entities?

**Mike Schroepfer:** We would have to understand and do the analysis of, of all the ads run in that campaign, where is the location and the source of all of the different advertisers.

Q2246 **Julie Elliott:** Do you have that information?

**Mike Schroepfer:** I do not have it off the top of my head. I can see if we can get you some form of it.

Q2247 **Julie Elliott:** Our elections are very heavily regulated, and income or monies from other countries cannot be spent in our elections in any way, shape or form, so I would have thought that you would have that information because your company would be aware of what our electoral law is.

**Mike Schroepfer:** I do not have that information on me. I would be happy to follow up.

Q2248 **Julie Elliott:** Can you find that information and provide it to us?

**Mike Schroepfer:** Of course.

Q2249 **Julie Elliott:** Thank you. Following on from that, can you, when you find that information, also find out for us has Facebook contacted those users to tell them that this has happened?

**Mike Schroepfer:** To tell them that they saw advertising from—

Q2250 **Julie Elliott:** From non-UK sources during the referendum.

**Mike Schroepfer:** I do not know that we have notified folks. Again, we can follow up on this specific issue.

Q2251 **Julie Elliott:** Can you find out and let us know that?

**Mike Schroepfer:** Sure.

Q2252 **Julie Elliott:** Lovely. I want to go back to something that David Carroll, who has given evidence to us in this inquiry, said on Twitter on 12 April 2018, that, "Opting out of ad targeting"—you have talked at some length earlier today about ad targeting—"takes 14 taps and strokes on a smartphone". Would you agree with that? This is to users changing their ads, privacy settings, the types of things we were talking about earlier on.

**Mike Schroepfer:** I do not know the exact number of taps. I want to be clear on one thing. The two goals that people want is they want it easy and they want detailed control. When you have detailed control, it means you have make lots of choices where you can make individualised



## HOUSE OF COMMONS

adjustments to things. That is generally what we are offering in this case, which is pretty detailed control over this thing. I would also point out that part of the ads controls we have put into the main part of the GDPR screens we are putting in front of every single new user now.

**Q2253 Julie Elliott:** If we accept that what David Carroll has said is true, would you say that that is quite a difficult thing to do, to allow your Facebook users to opt out of ad targeting?

**Mike Schroepfer:** We go through and we revise these UIs on a very regular basis and we go through extensive user testing to try to make these as easy and understandable as possible.

**Q2254 Julie Elliott:** If that is the case, would you accept that that needs to change and be made easier?

**Mike Schroepfer:** I would tell you that we have gone through extensive user testing on these things and try to make them as easy and fine-grained as possible. If you want fine-grained control where you want to get rid of these interests but not these interests, there is no technical way for me to do that for you in one click. I have to expose the controls—

**Q2255 Julie Elliott:** There are 14 actions.

**Mike Schroepfer:** I do not know what the 14 refers to. I have certainly used the controls myself and I found them quite easy to use.

**Q2256 Julie Elliott:** Could you look into that and provide the Committee with the information of how many clicks, swipes, whatever you have to use, and also, if it is 14—I trust David Carroll is correct on this—explain to us how you could make that less and what actions you are going to take to make that less? Fourteen actions is an awful lot of actions for someone to alter their settings on this.

**Mike Schroepfer:** These are very individualised settings. It has not been my experience that it is 14 clicks, but I think your deeper question is an important one, which is are these things easy to use and do people understand them. That is a very important question and a fair question you should be asking me. What I am telling you is our teams on a regular basis are doing extensive detailed user studies with people where we test out these user interfaces, test out multiple versions of them and—

**Q2257 Julie Elliott:** Will you come back and explain that to us?

**Mike Schroepfer:** I would be happy to try to provide some more information on the process by which we do this, but we are trying to build them so that they are easy to understand and powerful.

**Q2258 Simon Hart:** I want to stay on the subject of political advertising and try to clarify what Mark Zuckerberg has said. He is quoted as saying that after the US election he thought it was a pretty crazy idea to think that Facebook had influenced the outcome of the election. What do you think he meant by that? Was he essentially saying that people who spent



## HOUSE OF COMMONS

several hundred million dollars on advertising on Facebook are wasting their time? What did he mean?

**Mike Schroepfer:** I think he has said since then that he regrets saying that. It might have been narrowly scoped to the issue of the ads published by the Internet Research Agency, which were a very small minority of the total overall political ad spending for the campaign. If you are talking narrowly about that, I think the impact of that has yet to be seen. He has said publicly that he regrets having said that at the time.

Q2259 **Simon Hart:** Earlier on I thought you were giving the impression that political ads were a relatively small part of your business. That could be true. There is the suggestion that there is about US\$600 million worth of campaign ads going around the social media market, of which you have a significant share. Do you know what that share is and what is it as a proportion of your annual income?

**Mike Schroepfer:** I am sorry, the share of political advertising?

Q2260 **Simon Hart:** Yes, what share of the market? Let's say Bloomberg was right and US\$600 million is right for this calendar year. What share of that are you currently expected to receive and what proportion of that, as a percentage of—

**Mike Schroepfer:** It is likely to break down according to the overall share of the advertising market. We are 6% of the global advertising market. We are about 20% of the digital advertising market, so I would assume that—

Q2261 **Simon Hart:** What percentage are you of the campaigning market?

**Mike Schroepfer:** I do not know that figure off the top of my head. I would assume it is within some range of our general market share in these fields.

Q2262 **Simon Hart:** It seems to me quite odd, if you do not mind me saying, to not have a pretty precise feel for that kind of figure. I presume your finance director at Facebook, whatever they are called, takes a very detailed look at these things. We are here to talk about political advertising, among other things, yet it is quite frustration that you do not seem to have a clue of what proportion of this your business accounts for. Of all the questions I thought that might be one you might be able to tell us about rather than get back to us about.

**Mike Schroepfer:** My humble apologies, sir. I want to get you the information you need. Let me tell you a few things that I know now and see if this helps. If it does not, we will make sure you get the data you need.

As I said, we are about 6% of the global advertising market. I think that is probably a good proxy. Political advertising is spent on a variety of mediums. You would assume we are around that range of overall political advertising. The reason I do not have that figure for you is it is not



## HOUSE OF COMMONS

something we track. We have no goals on the political advertising market. I have never seen a target on getting that much of the political advertising part of the market. We are trying to grow the overall advertising business.

The only numbers that I do know, because we looked at them when we were addressing these issues of political ads, is the relative percentage of our overall ad revenue that we gain from political ads, which you can understand goes up and down depending on whether there is a major election or not. Even at its peak during major elections it is a low, single-digit percentage, even at its peak time. It is a relatively small part of our overall ads revenue for the business.

Our overall business, understanding what different parts of the ad business are we a percentage of, those are the things that I am tracking and we are dealing with on a regular basis and that is why I understand those figures. I know our overall market but we do not track this as a segment in the market. We are trying to grow share in any form.

**Q2263 Simon Hart:** You are not trying to increase your market share, because you do not know what it is.

**Mike Schroepfer:** I have not been in a meeting where we have talked about our share of this market.

**Q2264 Paul Farrelly:** I want to ask you a few questions about dark advertising in a moment. In your statement you have committed for the UK, in time for the local elections next year, that you will treat political advertising differently, to the extent that you can identify the source as political advertising, and put ads in a searchable archive, as happens with print. If you can do that here next year, are you going to that in other countries as well?

**Mike Schroepfer:** Yes, we are prioritising the rollout of that capability. It takes us some time to build the technical systems and to address the questions your colleague raised about how to identify these different sorts of ads. That is obviously regional and local. What issues are important in different elections is different. Our schedule of rolling this out is trying to get it out in advance of major elections worldwide.

**Q2265 Paul Farrelly:** You will be doing it, for instance, in the world's biggest democracy where you have the biggest user base, India?

**Mike Schroepfer:** I do not know off the top of my head the exact rollout schedule. I know it is prioritised, getting it out in front of the major elections. The goal is to get this as far as we can in democratic countries around the world.

**Q2266 Paul Farrelly:** If you are going to do that for next year—and with regard to Cambridge Analytica and AggregateIQ you can identify how much they spent—can you make available a searchable archive of what materials they produce for the money that they spend? We will ask both of those



## HOUSE OF COMMONS

companies as well. Can you do that?

**Mike Schroepfer:** I am sorry, forward going?

**Paul Farrelly:** No, historically.

**Mike Schroepfer:** For Cambridge Analytica and AggregateIQ?

**Paul Farrelly:** Yes, for the UK referendum and the US election. Can you do that, technically?

**Mike Schroepfer:** It is difficult to do this retrospectively. We often do not have all of the data. We have done, at your request, a detailed, one-off analysis for Cambridge Analytica and AggregateIQ. We have done similar analysis for the IRA in the US. In this case, because we do not have prebuilt systems that are ready to store this data in a format that is easily queried for all of these things, we have to go and do a whole bunch of work in each particular issue to find it out. It is hard for us to do this backwards looking, unless there is a specific interest.

Q2267 **Paul Farrelly:** You have historic information on what 1.5 billion people do worldwide, on all your systems, which is continually updated. Are you saying it is not possible for you to provide an archive of what two users, Cambridge Analytica and AggregateIQ, spent their money on?

**Mike Schroepfer:** I am sorry, you are looking specifically for Cambridge Analytica and AggregateIQ?

Q2268 **Paul Farrelly:** Yes. I am only talking about those here, because it would be of great interest to those of us who by definition are not the target audience for these adverts, to see examples of what they were and how subtly or unsubtly they may have been changed and the facts might have been changed, and therefore the extent to which there was manipulation to different target audiences.

**Mike Schroepfer:** Yes, these are good questions and specifically in AggregateIQ and Cambridge Analytica related to the UK referendum, I believe we are producing more extensive information for both the Electoral Commission and the Information Commissioner. We are trying to give them all the data we have on the ads and what they spent and what they are like, because your question is a good one.

Q2269 **Paul Farrelly:** Could we have that as well?

**Mike Schroepfer:** Again, we are giving that to the Electoral Commission and the Information Commissioner. I do not understand the rules with ongoing investigations. I will defer to you to tell us what we are allowed to share and not share but I will get you all the information we are allowed to give you.

**Paul Farrelly:** I am sure your lawyers will tell you that you are.

**Mike Schroepfer:** Yes. I am the wrong person to make that determination.



## HOUSE OF COMMONS

Q2270 **Paul Farrelly:** It was reported that dark advertising was used in the US elections to try to dissuade African Americans from voting. Can you tell us a little bit about what happened and the extent to which that did or did not happen and any ways that Facebook was used?

**Mike Schroepfer:** I am not sure what you mean by the term “dark advertising”.

Q2271 **Paul Farrelly:** Let me google it, which I have, through Safari. “Dark advertising is a type of online advertising visible only to the advert’s publisher and the intended target group”. I am sure you know that.

**Mike Schroepfer:** This is where I would agree with you that transparency across all advertising is important. Even in other mediums like television you may not see the ad. It is easier to see because it is on a television channel, but this is why we are rolling out the ads transparency across all advertising not just political advertising. You are going to get this in the UK in June.

Q2272 **Paul Farrelly:** In June. Mark Zuckerberg has vowed to give up dark advertising, has he not, but you are telling me you do not know what the definition is?

**Mike Schroepfer:** What I am telling you is that transparency of what advertisers are running to whom I would agree with you is an important thing. That is why we are rolling out this tool in the UK in June, which means that for any advertiser you can look at all of the ads it is running, regardless of who it is running against. For particularly important things like political ads, we are going further with detailed spend information and historical logs and that sort of thing because that is of particular importance. I agree with you that transparency on what is happening here is very critical.

Q2273 **Paul Farrelly:** When Facebook attaches employees or people associated with it to political campaigns—embedding, I think it is called—what do those people do?

**Mike Schroepfer:** I am sorry, can you repeat?

**Paul Farrelly:** We understand Facebook attaches people to political campaigns—it is called embedding—what do those people do?

**Mike Schroepfer:** I am not familiar with that particular term but I do know that we have sales and support folks who work with most of our major advertisers and help them use our ad systems to best effect. That would include political campaigns and we do it on all sides of any election.

Q2274 **Paul Farrelly:** If a political campaign were using dark advertising, your people helping support their use of Facebook would be advising them on how to use dark advertising?

**Mike Schroepfer:** I think there are two things here. The positive use of advertising on Facebook is instead of blasting a message across the



## HOUSE OF COMMONS

entire United States, if I am running in a small district, you are trying to reach a specific audience.

Q2275 **Simon Hart:** I understand that but if somebody wanted to reach a specific audience with a specific message but did not want another audience to use that message because it would be counterproductive, your people who are supporting these campaigns by these users spending money would be advising them on how to do that, would they?

**Mike Schroepfer:** Yes, and we do help advise the campaigns and all major advertisers on how to use our tools. I want to be clear there is a very clear set of policies on what ads are allowed and not allowed. Hateful, divisive ads are not allowed on the platform. There are a set of community standards on what content is generally allowed. There are a set of ad standards that are, because there is money involved, more restrictive. We take a much harder line on things you are not allowed to advertise on.

The other thing is that people must be authentic when they advertise, which is one of the problems with the Russian IRA in that election. In all cases whenever employees would be working with a customer and an advertiser, they would certainly be advising them to follow all of the guidelines we have in terms of what is an okay ad on the platform. We do not want divisive ads on the platform. This is not good for us in the long run or good for people in our business. We do want people to run effective ads, because it is better for them. It helps the 2 million small businesses in the UK and others.

Q2276 **Paul Farrelly:** We are not talking about that, we are talking about politics and manipulation.

**Mike Schroepfer:** I understand, yes.

Q2277 **Paul Farrelly:** This is why providing us with the archives of what AggregateIQ and Cambridge Analytica in the referendum and the US election spent their money producing and using Facebook for would allow us to judge for ourselves whether what you are saying was true in practice.

**Mike Schroepfer:** Yes, I agree.

Q2278 **Paul Farrelly:** I am going to wrap up now. When you have people working with campaigns like this, embedding and advising people on how to use your platform for their campaigns, it breaks down the myth that you are neutral. You may work for everyone scrupulously, but you are players. You are not a neutral platform, you are players.

**Mike Schroepfer:** The clear thing is we do not have an opinion on the outcome of these elections. That is not what we are trying to do. We are trying to offer services to any customer of ours who would like to know how to use our products better. That is everything from a small business on up to a political party. We have never turned away a political party



## HOUSE OF COMMONS

because we did not want to help them win an election. There is none of that partisanship in how we deal with this. This is simply trying to help each and every election advertiser use the products.

**Q2279 Paul Farrelly:** Dr Kogan made it quite clear to us that in his work with the SCL Elections he did not care who the candidate was. Facebook is Dr Kogan writ large.

**Mike Schroepfer:** I believe in strong, open political discourse. What we are trying to do is make sure that people can get their messages across. I do not think it is for us to decide who the right candidate is, I think it is for the people to do that. In the sense that we will equally support all legitimate candidates for a democratic election, yes, of course we will support all of them.

**Q2280 Paul Farrelly:** In terms of involvement in dark advertising, as it is called, and these sorts of practices, which seem a world away from what Facebook was set up to do when you joined it, for instance, has there been any discussion at senior level, is there any discussion going on now, that, "We might be accused on manipulation, this is bad for our reputation, we should not be involved in it"?

**Mike Schroepfer:** There are multiple issues to unpack here, and please interrupt me if you feel like I am not answering your question, because I want to talk about it—

**Paul Farrelly:** Unpack away.

**Mike Schroepfer:** We want to provide tools that allow people to reach an audience. This is for me as a person to talk to my friends, this is for a business to find customers, this is for a candidate to talk to their constituents. That first principle is one of free and open expression and providing people an audience.

The challenge that we are layering on top of all of this is the rules of the road of what is allowed, either for an individual to say or for an advertiser to say in an advertisement. Do we think it is okay for a legitimate candidate for a democratic election to advertise on Facebook? Absolutely. Do we think it is okay for them to run divisive, hateful ads? Absolutely not. That is against our platform but we think that free political speech is something that is an important part of democracies and thus is something that we should have on our platform.

**Q2281 Paul Farrelly:** With some of the practices that you have allowed, and the reporting of attempts, at least, of political manipulation, people will ask themselves is there anything Facebook would not do to make money, simply because it technologically can. I am not going to ask you that question because it is an easy one for you to rebut. When I was preparing for this session, what popped into my mind was a story in *Rolling Stone* in 2009, just after you joined the company, by a journalist called Matt Taibbi. He wrote, "The first thing that you need to know about Goldman Sachs is that it's everywhere. The world's most powerful



investment bank is a great vampire squid wrapped around the face of humanity, relentlessly jamming its blood funnel into anything that smells like money". Is it of concern to you that in terms of this inquiry and what has been going on that that story pops into my head and that the thought is planted that for "Goldman Sachs" read "Facebook"?

**Mike Schroepfer:** I think the issues we are talking about today are real, serious issues. Earlier in the conversation you were talking about preventing fraudulent advertising, just for commercial purposes but it is still a problem. You are talking about people interfering in an election, either a foreign entity or using divisive advertising even from a legitimate candidate. These are all hard problems.

The biggest trade-off in all of them is not about money. I cannot remember the last time when we had one of these things and we said, "We will save some money by not fixing this problem". The issue is it is technically and operationally challenging to solve all of these things. When you say things like you do not have divisive advertising, defining exactly what that means and finding exactly the line between legitimate free political speech and what is something that is divisive is a challenging to get right at scale, and something we want to make sure we are very clearly not censoring because I think that is our first priority. I do not want to paper over the fact that these are real issues, protecting people's data, protecting the integrity and sanctity of elections. We feel a deep responsibility to solve these problems and make sure our platform is safe.

I understand the scepticism—I don't fault you for it—and if you are asking a question of intent, I can only tell you what is in my heart, which is I do really care about these things, we do really want to get them right. They are hard problems. We are humans who will make mistakes, but we are dedicated to try to solve all of these things. I think we will see how this goes over the arc of time. There is not a lot I can say here that will probably convince you of any of this but I hope that the actual actions that we are taking over a long arc of time will eventually convince you of it, because we have done it well.

Q2282 **Paul Farrelly:** This is my final comment. Perhaps part of the answer is to recruit more humans, to put more people on the case, as you have in Germany, which outlawed hate speech.

**Mike Schroepfer:** I think it is. I tell you, when I am not here, the primary thing is I am recruiting. We are working as hard as we can to get people on the ground all across the world in technical teams to solve these problems, so I agree with you.

Q2283 **Chair:** Just one question I want to ask on dark ads. If an organisation or an individual, say during the referendum campaign here or during any election, set up a page to place dark ads targeting voters during the campaign and then took that page down, took it offline as soon as the campaign was over, how would you be able to identify that activity had



ever taken place?

**Mike Schroepfer:** I would have to confirm, but there is a possibility that we have in a separate system a log of the ads that were run. We would have the page itself, if the page was still active. If they had run prior campaigns and deleted the page we may retain some information about those ads. I do not know the specifics, for example, how detailed that information is and how long the retention is for that particular set of data.

Q2284 **Chair:** I would be grateful if you could confirm that, because I think it is quite important, because obviously what is a big part of our electoral law—and I imagine it is the same in America—is declaration of spend. If someone is hiding the spend by placing dark ads that only the recipient sees and then those are all taken offline after the campaign, if no one has the ability to audit that, that is a major threat to democracy and would be a licence for a major breach of election law.

**Mike Schroepfer:** We can come back on the details on that.

Q2285 **Christian Matheson:** Mr Schroepfer, just a couple of questions on accounts on Facebook, if I may, technical questions. Every now and again—and from memory, twice since Christmas—I have had friend requests on my Facebook account from attractive young women. We have no friends in common. One of them, they did not have any friends, they had no connection to me at all. One explanation might be that they admire my work in Westminster and Chester. Another might be that despite the fact that I am an overweight, middle-aged bloke, they like what they see. Let's do what Mr Knight says and discount them and assume that they are fake accounts. If I allowed my vanity to get the better of my judgment and accepted that friend request, what advantage would accrue to the individual who controlled that fake account?

**Mike Schroepfer:** This is a good question and an important issue. Fake accounts, you have very acutely described one of the vectors that people use for fake accounts, which is they create a fake account on Facebook, they attempt to friend other people on Facebook. The ultimate goal for most of these people is some sort of financial gain. This could be as simple as them friending you and trying to friend some others and then saying, "Hey, I am a friend of Mr Matheson. Here is a great product I tried, check it out" and sending a link that was to some spam or fraudulent product, or even more insidious, they could be friending you and a bunch of your friends and then sending a message to one of them and saying things like, "Help, I am stuck in Parliament in London. I need £500 to get out. Please wire the money to this account" to try to scam one of your friends.

The biggest volume of these we see is straight-up financial scams, where people are trying to find people, build trust and then use that trust to scam them for money. Again, finding and removing these sort of inauthentic and fake scamming accounts is one of the most important things we can do. We find the vast majority of them at sign-up time,



## HOUSE OF COMMONS

many million a day, but some do get through because there are literally buildings full of people in different regions who spend all day trying to build plausible, real personalities. They will do very tricky things—I will not go into detail in this public session—to try to mimic and cloak, like they are a real user, to build this trust and then trap.

If they miss our automated systems, there is a way—I hope you did this to these accounts—you can simply report the account as a likely fake account. That immediately flags for a human review, who do a more extensive analysis than our AI systems can to understand, and if so, remove that account.

Q2286 **Christian Matheson:** There is no technical advantages that would accrue, for example, if I friend one of these accounts, they have access to my data or anything like that?

**Mike Schroepfer:** The basics of Facebook is for most people, they are sharing their posts on their status, on their wall, photos with their friends. As a friend, they could view your profile, like any of the other friends you have on Facebook could view the information on there.

Q2287 **Christian Matheson:** How many fake Facebook accounts are there? Based on what you have just said, it is a dynamic number.

**Mike Schroepfer:** It is a dynamic number.

**Christian Matheson:** Give us a rough ballpark figure.

**Mike Schroepfer:** I know that we report this on a regular basis in our filings. I think is in the order of a few per cent.

Q2288 **Christian Matheson:** You had a clear-out about a year ago, didn't you? You had a purge of fake accounts that you then reported after a few weeks on 14 April 2017.

**Mike Schroepfer:** I do not remember that specific purge, but there are teams whose whole jobs it is to go after this on a daily basis.

Q2289 **Christian Matheson:** There was not one particular time when you went after a particular purge of fake accounts?

**Mike Schroepfer:** There may be. I don't recall the specific you are talking about. The reason is because this is daily. It is not like we have a team that is doing something else and then we put them on fake accounts, there is a team who is completely dedicated to dealing with this and a number of other issues that are finding these literally every single day on the order of hundreds of thousands to millions.

Q2290 **Christian Matheson:** On CBS News, 14 April last year, you made an announcement that you had purged thousands of fake accounts that targeted publishers, although that was a delayed announcement. Is this not something that would necessarily cross your desk as chief technology officer?



## HOUSE OF COMMONS

**Mike Schroepfer:** Again, that is a fairly small number regarding the amount we are dealing with every single day.

Q2291 **Christian Matheson:** Would there have been any link or any connection within that purge in the first quarter of 2017 to election-related activities after the United States presidential election?

**Mike Schroepfer:** I do not know.

Q2292 **Christian Matheson:** Who might know?

**Mike Schroepfer:** We would have to look into it. Again, we are removing accounts all the time, like the recent IRA accounts, 270 of those. We would have to go through and look account by account and see what they did to understand that. Again, because we stop them at creation time and then remove them on a regular basis, it is hard for me to say specifically.

Q2293 **Christian Matheson:** Once you had done this purge, the announcement was delayed for a while, you did not release the information straight away. Why might that delay have taken place before you announced it?

**Mike Schroepfer:** I do not know. We are purging fake accounts all the time and dealing with fraudulent ads and we do not tend to report each specific instance. I know we report aggregate statistics on a regular basis, but it is not something we are reporting here or there, so I don't know.

Q2294 **Christian Matheson:** The fake accounts that you have purged, let's say since the start of 2017, did you have any trace of an involvement from Russia?

**Mike Schroepfer:** I do not know the percentage from Russia. I would guess it is a relatively small percentage, because most of these accounts are financially motivated, actors who are all over the world.

Q2295 **Christian Matheson:** Could you find out what percentage would have had an involvement from Russia?

**Mike Schroepfer:** I would have to see whether we have detailed logs. Again, I am happy to provide this Committee with all the information I have, but I do not know how detailed our logs are for this particular issue.

Q2296 **Christian Matheson:** What you are saying here is that there is a day-to-day purging of fake accounts and that Facebook did not go on a specific campaign around the first quarter of 2017, give or take a couple of months, where you had a specific campaign to get rid of identified fake accounts as one specific operation?

**Mike Schroepfer:** Again, I was not involved in this specific announcement. This does not stick out in my memory as a particularly notable thing and I would probably remember if it was. I am mostly speculating, because what I do know is that volume of work we do on a



## HOUSE OF COMMONS

regular basis, we purge accounts on a regular basis, so I do not know the specific circumstances you are talking about, if it—

Q2297 **Christian Matheson:** In the top level, your level at Facebook, who would have been responsible for this?

**Mike Schroepfer:** There is a team dedicated to integrity issues and security issues. It would be helpful to understand what is the root of the information you are looking for, so I can make sure I am giving you a better answer.

Q2298 **Christian Matheson:** Yes, sure. Who runs that team, that integrity team?

**Mike Schroepfer:** Help me understand what you are looking for and then I can find it, because it depends on the specifics of what it is. I would be happy to figure out how to answer the questions you are looking for.

Q2299 **Christian Matheson:** I am trying to find out whether, as opposed to the individualised scammers, Facebook believes that there was a systemic problem of using fake accounts to manipulate democratic procedures, either here or in the United States or elsewhere.

**Mike Schroepfer:** The information I do know is the extensive investigations we have done trying to understand the actions of Russia in relation to both campaigns. That we have looked extensively at. Again, it is hard to find absolutely everything, but I think what we found is probably it.

In terms of others, I would have to go back and understand what analysis we have done on that. I am not aware of any other large-scale concerns on this, but I can see how to better answer your question.

Q2300 **Christian Matheson:** Thank you. Can I just check, who within the management structure would have responsibility for that?

**Mike Schroepfer:** It depends on the specifics we are talking about. It might be one of my peers.

Q2301 **Christian Matheson:** Give us a suggestion, a job title, not necessarily a name.

**Mike Schroepfer:** We have a person who is the head of integrity, whose jobs it is to solve all of the issues with spammers, fake accounts, all the rest of it. Community integrity is the term.

Q2302 **Christian Matheson:** Does that person report to you or report—

**Mike Schroepfer:** They do not report to me.

**Chair:** —to the chief operating officer or the—

**Mike Schroepfer:** They report through Mark.



## HOUSE OF COMMONS

Q2303 **Chair:** Just for everyone's benefit, according to Mark Zuckerberg's earnings call last night and the information that was released with that, there is about 80 million fake accounts on Facebook.

**Mike Schroepfer:** Thank you.

Q2304 **Giles Watling:** Mr Schroepfer, thank you so much for appearing before us today. First of all, I would like to say I am delighted to hear that you have a head of integrity. That is a really good move, in my view.

In many of the hearings we have had—and we have had people from Instagram and Twitter before us—I get the overwhelming impression we have a bunch of guys here who are very bright, very sharp and really on top of their game IT-wise, not like the rest of the world, but they have been brought kind of blinking into the sunlight of a new reality. They have created platforms for the sake of democracy et cetera, as you have stated today, but then they are finding that they are being used by bad actors and suddenly find themselves behind the curve and are now playing catch-up. Would you say that is a fair thing to say?

**Mike Schroepfer:** I think it is fair to say that when I joined the company in 2008, and I went to school to study computer science, I did not have any idea that a decade later I would be here talking to you about Russia interfering in foreign elections using the products that I had built. That was certainly not my expectation.

Q2305 **Giles Watling:** So my overall impression is not that far wide of the mark?

**Mike Schroepfer:** I think the challenge is many of these problems are new. These platforms are new, the way people are connecting is new, the way people are trying to attack them is new. Once we understand the sort of form of a problem we get very good at deploying technology and other things to get rid of that problem. When there are new things that happen—

Q2306 **Giles Watling:** Would you agree though that you are behind the curve and you are playing catch-up? I get the kind of impression that you are not willing to go there, you are having to be pulled there. Would that be fair? Is that how you feel it is at the moment?

**Mike Schroepfer:** We have said very clearly that we were slow to react on many of these issues.

Q2307 **Giles Watling:** Deliberately slow to react?

**Mike Schroepfer:** No. We were slow because we did not fully understand the threat at the time. That is something I regret. The best I can do now, I cannot fix that back then, but what I can do is dedicate my time and energy to make sure two things happen. One is the specific form of these attacks, where people are trying to do things like interfere in an election, we build every operational and technological defence we can, we build product features like making ads transparent et cetera.



## HOUSE OF COMMONS

Secondly, we do a much deeper, more rigorous, forward-looking, “Okay, not just this problem, what are all the other problems that could be appearing on the horizon that we are proactively building these sorts of defences for?”

**Q2308 Giles Watling:** You are not just looking in the rear-view mirror, you are looking at what—

**Mike Schroepfer:** Absolutely, because I think that is the challenge. If you knew about it in the future, you would have built a defence.

**Q2309 Giles Watling:** You have a platform that has no editorial control, it does not abide by the great tenets of journalism, so therefore you have run into this area now whereby you are looking at possible regulation. How do you think that regulation should take form?

**Mike Schroepfer:** I think your colleague and I talked about this before. The goals have to be clear in terms of user control, user safety, transparency, not just for the user, for everybody, so you can understand these systems, because many of the concerns you have raised I think are very valid, which is, “Hey, if there is stuff happening that the public can’t observe, then there is real possible danger there” so that—

**Q2310 Giles Watling:** But your platform, you say, is open to political speeches and, quite rightly, open to all sorts of political speeches, but it could be argued Hitler’s speeches were free political speeches. How do you make that dividing line between what you can put on your platform and what you cannot put on your platform?

**Mike Schroepfer:** This is a deeply important and challenging issue. On Tuesday this week, I think it was, we published our internal guidelines that our reviewers use when a piece of content is disputed. If you flag something and say, “I do not think this belongs on Facebook” there is a set of guidelines we have, the actual guidelines that people who are trying to make this decision use. We have published in detail—it is 20, 30 pages—on a variety of topics, everything from obviously hate speech and threats of violence and dehumanising a group of humans, not allowed, that sort of stuff not allowed; adult nudity is not allowed on the platform either. These sorts of things are clear guidelines.

One of the things we have said, a challenge here, as you raise, is understanding exactly where the lines on these things are is very difficult. I think the right approach to this is to be a lot more engaging with people in the world on where that line should be.

**Q2311 Giles Watling:** Do you think there should be some form of editorial control?

**Mike Schroepfer:** I think people who are using the products should have a bigger say. First of all, it is understanding what those rules are in detail and then we are going to engage with people in the community to get feedback on if we have these wrong, if we have set the bar wrong. I



## HOUSE OF COMMONS

would say, for example, I have certainly had feedback on both sides about nudity on Facebook. I have had people tell me they think we are too prudish and too restrictive and others who think that it is offensive, what we allow.

**Giles Watling:** That concerns me slightly less than—

**Mike Schroepfer:** I understand, but I am just using it as an easy example for how different communities would have different standards for these things. What we are trying to do is evolve to a mode where the people using the products—because again, it is a product for free expression. I want people to say what they want without fear of censure, without fear of repercussions, but there have to be some basic rules for safety and for decorum.

Q2312 **Giles Watling:** Can I move on slightly to the fundamental model? One of your former managers, Sandy Parakilas, who you probably know of, he once said that Facebook is fundamentally an addictive product. When building the platform, was that a deliberate build or was that something that came along as a by-product?

**Mike Schroepfer:** We want to build products that people like and want to use.

Q2313 **Giles Watling:** But people like and want to use cigarettes.

**Mike Schroepfer:** I think that if you look at the usage of products like Facebook every single day and what people use it for, to connect and communicate, I met my colleague this week, Nicola Mendelsohn, who was just diagnosed with a rare and incurable form of cancer and she turned to a Facebook group, 3,500 people around the world, for help, for support. Doctors are in this group, patients. People join the group and say, "I was just diagnosed. What do I do?" so I think that—

Q2314 **Giles Watling:** I am not denying that there are really positive things that come out of this, but what I am trying to get at is if you develop a deliberately addictive product that therefore you can sell it to your advertisers, because you know that people will go back to it. We have all seen the spiral of addiction that goes with these kinds of things, with the use of Twitter and so forth.

**Mike Schroepfer:** I think there are a tremendous number of day-to-day good uses of Facebook. The thing we want to do is make sure that it is good for people. We have talked extensively about product changes we have been doing, research that we have been doing to understand wellbeing and we published much of this research. We have world-leading experts in the company and we work with third parties. We announced a series of changes earlier this year, whose whole purpose was to make sure that we were reducing time on the site in order to prioritise content from friends and family, content that we call meaningful, meaningful social time, because that at is the heart of what we are trying to do, to



## HOUSE OF COMMONS

get people tools—to Nicola, to me—to share. My two little kids, whose family lives all the way—

Q2315 **Giles Watling:** But people can't put it down, can they? I put it to you that people just can't put it down. That is part of the system, that you place a post, then 15 minutes later you need to look and see if someone has reacted and if they have not reacted, you need to do something else. If they have reacted, you get gratification. That is addiction.

**Mike Schroepfer:** Our goal is to build products that are good. The thing that I can talk about, that is changes we make that reduce time, to reduce usage, but vie people towards this, because what our research has said—and once I explain this, it will be intuitively obvious—there are two ways to use these products. If I simply passively engage and just kind of do as you say, just sit there and scroll and waste time away and I spend a lot of time doing that, that is probably not positive. However, if I am on the product talking to friends and communicating, posting a picture of my kid, getting a comment from their uncle, getting a comment from my mom, writing back, sharing my daughter's play today with them, since I can't be there for it, that is a really positive experience. That is something that I can't wait to see these photos.

**Giles Watling:** I take your point.

**Mike Schroepfer:** That usage of the product is good. This sort of just scrolling behaviour we have tried to educate people is not good and not what we want to optimise the product for.

Q2316 **Giles Watling:** Can I ask you another couple of questions? When the Facebook platform was initially created, what was the intent? Why did it allow developers access to the user data?

**Mike Schroepfer:** The intent on this was to allow people to have great social experiences where they wanted to have them, so not just on Facebook, but to be able to say, "Hey, when I am listening to music, I want to find music for my friends. When I have a calendar, I want to make sure all my birthdays are in that calendar", lots and lots of examples of these. When I play a game, it would be more fun if I played a game with a friend than by myself. The whole purpose of this was to allow developers to build—because we could not build all these experiences—these experiences and allow people to take their data to these experiences.

Q2317 **Giles Watling:** But you were aware that developers might be interested in using the data for purposes beyond simply adding social functionality to the application?

**Mike Schroepfer:** I think all of these things can have good uses and can be abused. We had controls in place. It was clear anytime someone installed one of these applications. We put a lot of work into making sure that before you could use it, it was clear what information the application was using so that consumers could make a clear choice and say, "Wait, I



## HOUSE OF COMMONS

do not want this app to get this information". That is where we focused a lot of our time and energy. We said, "We think people are smart. We think they want good experiences, they want to take their data. Our job is to make sure that they understand what is happening".

**Q2318 Giles Watling:** I get it that you are trying to improve it, but why did you build a platform that made data abuse so easy in the first place?

**Mike Schroepfer:** Again, you have to remember that we were trying to build this and our focus was on clear understanding from the consumer on, "When I use this application, what data am I sharing with it?" This is not different to if you install an app on your Android phone today. That app, at the time in 2013-14, had access to pretty much everything on your phone. It probably did not even prompt you with requests for what was there. I think as a lot of these platforms evolved, even 10 years ago on my computer, I could install from anywhere. Now it has to be a certified developer that goes through a platform.

I think you are seeing an evolution as these things have all scaled, that we are realising that there are all of these bad uses and that we need to swing the pendulum more towards restriction, which has some downsides, but the upside there is safety. That is the evolution that we made in 2014 and 2015, an additional set of changes I announced myself just a few weeks ago to swing that bar from consumer visibility and choice, they are clear what is happening, but they can do it, to much more proactive review and enforcement of all of these things.

**Q2319 Giles Watling:** I get that, but do you think that the harvesting of data and selling it on, using data, is ethical? Can I just ask that?

**Mike Schroepfer:** I do not think selling of data is ethical.

**Q2320 Giles Watling:** You touched on legal earlier, but you—

**Mike Schroepfer:** I do not want this for myself, I do not want it for other consumers. Again, one of the reasons I wanted to talk to you myself is I think these issues are serious issues. We have made mistakes. I think other companies have done bad things, but the root of the issue, the idea that consumers do not have control over their data is a big problem and something I care a lot about.

**Giles Watling:** Thank you, Mr Schroepfer. The fact that you have a head of integrity I think is a wonderful thing.

**Q2321 Chair:** Thank you. I said we would pause at 1.00 pm and it is a minute past. We will have another four minutes and say we will come back at 1.20 pm.

**Mike Schroepfer:** I would be happy to continue if that is better for your schedule. I know your time is—

**Chair:** I think most of the members would welcome a break.



## HOUSE OF COMMONS

*Sitting suspended.*

*On resuming—*

Q2322 **Chair:** Thank you for allowing a brief adjournment, Mr Schroepfer. I know you have an appointment with the Secretary of State at 3.30 pm. I am hoping that we will have concluded by then. We will have to see how we go, but I am mindful of that. We will see what we can do.

To start, I would like to pick up on a few loose ends from the first part of the session. First, with regard to Aleksandr Kogan, we have had word back from his lawyers to say that they have had no contact with Facebook since the session at which he gave evidence before the Committee on Tuesday. I mention that because it would be helpful to us if they could have that contact, then it could be clarified to them what their position is.

**Mike Schroepfer:** Sure. I want to make it clear to this Committee that we want him to be able to be open. We are waiving any confidentiality, if that is not clear from a legal standpoint. I will make sure that our team follow up again immediately after this.

Mr Chairman, there are two things that I would like to clarify, but I am happy to wait for yours.

**Chair:** You first, if you would like to.

**Mike Schroepfer:** There were a few questions that folks asked earlier which I wanted to make sure that I had data on now, just to clarify for the record. One of your colleagues asked a couple of detailed questions about the contract with Mr Kogan. Again, we will provide that to you, but I wanted to give you some of the specifics on that, which you were asking for. You asked for the date of the contract, which was June 2016. A core commitment of that contract was to confirm the deletion of data from himself and anyone who had received the data.

You asked who the others were who were part of the certifications, and I was a little unclear on that. I want to make that clear for the record: it was Mr Kogan himself; Alexander Nix, representing SCL; Christopher Wylie, representing Eunoia Tech; and Dr Inzlicht, from the Toronto Lab for Social Neuroscience. Those were the four parties that were part of the contract. You will see this in detail, but to make best use of our time together I wanted to make sure that you had that data.

I also wanted to clarify one other thing, Mr Chairman—this is my last clarification. We talked a lot about political affiliation and advertising towards that. I wanted to clarify that declaring your political affiliation is, I know, a sensitive category in the EU on Facebook, so you have not been able to target ads against my declared political affiliation previously or now. We also know that this is a sensitive field as part of the GDPR, so we have to receive opt-in consent if you want to share that with others on your profile. We talked about a lot of different things, but since that is



a very specific part of the law, I wanted to make sure that we were clear on it.

**Q2323 Chair:** That has certainly dealt with one of the questions that I was going to ask. Part of the concern on political affiliation is not necessarily declared voting intention but whether your behaviour can make it easier to identify your likely political interests.

On the issue of Dr Kogan and Joseph Chancellor, Dr Kogan has said in interviews that Joseph Chancellor was scoffed at when he was interviewed by Facebook, about his previous experience and his work with GSR. It is almost, it would seem, unusual if he was not asked about what he had been doing when he applied for a job at Facebook, and what his more recent relevant experience was, so it would be useful if the company was able to confirm when it was aware of that.

What do you think it says that Facebook has used a very specific choice of words to describe Dr Kogan and his activities? It said, effectively, that it was a victim of fraud perpetrated by Dr Kogan. What does it say that he has been singled out for this attention, whereas Joseph Chancellor, who worked with him on that project, is one of your employees?

**Mike Schroepfer:** You raise a number of important issues, so I will try to get through all of them. I believe that at the time he was hired, Mr Chancellor was an employee at Cambridge—that was his primary job. I do not know, since I wasn't involved in the hiring, whether he had discussed his involvement at GSR. It is possible, but I have no personal awareness of that. What I do know is that after 15 December 2015, it came to light that there were issues with This Is Your Digital Life and Cambridge Analytica, and in the contract that you will see—discussing all the parties involved and what data they had—that Mr Chancellor was not involved or named in any of that. When it came to light again last month that there may have still been ongoing issues at Cambridge Analytica—that it still may have the data—we started an investigation of both Mr Kogan's role and Mr Chancellor's role. That is what we are doing now.

**Q2324 Chair:** What is Mr Chancellor's role at Facebook at the moment?

**Mike Schroepfer:** He has had a number of roles. He has worked on the VR teams and some other things—work unrelated to the platform.

**Q2325 Chair:** Okay, thank you. When Mark Zuckerberg appeared in front of Congress, he was asked about other app developers that may have developed something similar to what Dr Kogan developed. He said that was something that Facebook was auditing. Are you able to give us any progress report? Do you believe there are other developers like Dr Kogan, who created apps that took Facebook users' data and their friends' data and may have passed it on to third parties?

**Mike Schroepfer:** As Mark shared, and as I shared in one of my public updates, we have kicked off a process to look at all the apps that were live on the platform before that set of changes that we announced in 2014 to restrict access. It is a large number of developers who were on



## HOUSE OF COMMONS

the platform at the time. We are a few weeks into that process. I do not have a progress report for you here today on that. We have committed, as we did recently with Cambridge Analytica, that if we find issues, we will report them to the affected users. As we find issues, we will publicly update folks.

Q2326 **Chair:** Will you be notifying the relevant information authorities, too?

**Mike Schroepfer:** It would be fairly public if we are talking to users, so I assume that we talk to all the authorities on a regular basis. I assume that we would inform all the relevant parties.

**Chair:** We would expect the Information Commissioner to be informed.

**Mike Schroepfer:** We are working closely with her and her office and we will give her any information that she needs.

Q2327 **Chair:** When Sandy Parakilas gave evidence to the Committee a few weeks ago, he said that when he was working at Facebook and looking at relationships between Facebook and developers, and their access to Facebook user data, there were widely held concerns at that time about the vulnerability of data, and that once developers had got it, there was very little the company could do to track what they were doing with it. Is that something that he ever raised with you?

**Mike Schroepfer:** No.

Q2328 **Chair:** Are you aware of that being discussed by members of the executive team at that time?

**Mike Schroepfer:** I know that every time we are making product decisions there is, as I discussed earlier, this strict trade-off between ease of use and low friction, and safety. One makes use easier, but it also makes abuse easier. We are constantly trying to find the line. That is why, prior to understanding any of this, we made the changes to the platform in 2014 and thereafter. It is more of an ongoing series of discussions on the detailed features of it.

At the time, as I discussed with your colleague earlier, there was a lot of focus on giving clear controls to people, to help them understand that the idea was that people have clear choice in what they are going to do. Our job is to make sure that it is very clear what data will be accessed by this app. We spent a lot of time on the dialogues and the process and enforcing that with developers, to make sure that people understood what was happening. A lot of the idea was that with good developers and informed consumers it would work, but as we have seen, that was not enough.

Q2329 **Chair:** Are you aware of any other developers that gathered data in the way Dr Kogan did and then sold it on to third parties?

**Mike Schroepfer:** We are in the middle of this investigation, so I do not have an update for you.



## HOUSE OF COMMONS

Q2330 **Chair:** I understand there is an investigation going on, but a progress update might say, "Yes, we are aware of a small number, but there are thousands and thousands we have to check." At this moment in time, are you not aware of any other developers that did what Dr Kogan did?

**Mike Schroepfer:** If you will indulge me for a second, the challenge with these things is that the transfer of these things is not on our platform. There are conversations about our hard drive and things like that and prior testimony. So tracing down the fact that this developer had some sort of engagement with some other third party is not as easy as running through our logs and understanding exactly what happened. That is why it takes time to understand what has happened here with all the developers.

Q2331 **Chair:** Would I be right in saying that, to your knowledge, Dr Kogan and Cambridge Analytica are the only organisations that have received letters from Facebook demanding that they destroy data, because of the company's concerns that they had misused it?

**Mike Schroepfer:** I don't know, because we have done enforcement actions against other platform apps to take them off the platform, for a variety of concerns. I do not know the specific answer to whether we have.

Q2332 **Chair:** But what about that particular concern—the passing on of data?

**Mike Schroepfer:** The answer in this hearing is that I do not know.

Q2333 **Chair:** Your concerns in many ways underline the general concern about the problem, which is that once developers have the data, it is very difficult for you to know what they are doing with it. Actually, neither Dr Kogan nor Cambridge Analytica would probably ever have received a letter from Facebook if it had not been for a report in *The Guardian* alleging what they had done.

**Mike Schroepfer:** I agree with you that a very core problem of consumer data and data in general is that once it gets into someone's hands—if I forward you an email, you have a copy of that email and I cannot easily delete it; you must delete it. That is a problem with any electronic communication or data. This is why I think we have moved and the future is in proactive enforcement. Dealing with these things after the fact is not great, so we need to figure out how to prevent them in the future and make sure that consumers have clear control over their data, that developers are reviewed before they are on the platform, and that the platform is much more restrictive in the data it provides. I agree that it is challenging to deal with it once it happens, which is why we have been focusing our energy since 2014 on a much more proactive review of all this.

Q2334 **Chair:** You have made reference to 2014 several times, as Mark Zuckerberg did in his written statements and his testimony. If there was so much concern in the company that in 2014 a major change was made



## HOUSE OF COMMONS

to privacy settings to prevent friends data being accessed, where was the caseload that said, "We've got to make this change, because people are taking data and we don't know what they're doing with it, and it's not right that people's data is put at risk in that way"? If Facebook's motivation for making this change was responding to genuine concerns about user privacy, what were the examples that were referenced at that time to make that decision?

**Mike Schroepfer:** I don't know specific examples, but I do know, again, that this is evolving. In the early days, it was very much about how we make it exceptionally clear that people installing applications understand what data they access. This was at a time when an equivalent process on a mobile phone did not even tell you what data this app could get access to; you just installed it and it could get access to your location, contacts and a bunch of other things. Our focus was very intently on providing consumers with information up front so they could make a choice. We went through many, many iterations of that—many different ways where developers had to specifically request additional data. Over time, as we went through several iterations of that, we just decided that it was better to restrict this data up front and to review all these applications.

Q2335 **Chair:** Does Facebook's chief privacy officer report to you or to someone else in the company?

**Mike Schroepfer:** They do not report to me.

Q2336 **Chair:** Who do they report to?

**Mike Schroepfer:** I believe they report to our head counsel, Colin.

Q2337 **Chair:** Are you given briefings by them about concerns or privacy breaches?

**Mike Schroepfer:** I would be involved if there were any security concerns on the site. My primary responsibility is the core technical capabilities of the system, so if we have security concerns with that or technical measures we need to work on, those are the things that I tend to be involved with.

Q2338 **Chair:** You will know that Mark Zuckerberg was asked about a company called Palantir, which some people have called an American version of Cambridge Analytica. Have concerns ever been raised about that company's activities and whether that company has gained improper access to Facebook user data?

**Mike Schroepfer:** We are looking at lots of different things now. Many people have raised that concern and, since that is in the public discourse, it is obviously something else we are looking into.

Q2339 **Chair:** But that is part of the review work that Facebook is doing?

**Mike Schroepfer:** Correct.

Q2340 **Chair:** Okay. Finally, I just want to ask whether you can elaborate a little



## HOUSE OF COMMONS

on the statement in your written statement about collaboration between SCL and AIQ during the referendum. I know one of my colleagues wants to come on to this in a bit more detail later, but I don't know whether there is any more you can say at this moment to elaborate on what is in your written statement.

**Mike Schroepfer:** Yes. What would you like to know?

Q2341 **Chair:** To start off, could you explain a little bit more about what the nature of that collaboration was and how significant it was?

**Mike Schroepfer:** This is between Cambridge Analytica and AggregateIQ?

**Chair:** Yes.

**Mike Schroepfer:** The collaboration we saw was some billing and administrative contacts between the two of them. You would see similar people show up in each of the accounts, and things like that. We have provided a lot of detail on this to both the Electoral Commission and your Information Commissioner. I don't know, again, since she has a pending investigation into the specifics of this, how much detail her office wants to go in a public forum. I would be happy to provide all the information we have provided to her to you and the entire Committee privately, but since there is a pending investigation I want to be sensitive about disclosing that in a public forum.

Q2342 **Chair:** As you know, the Committee has taken evidence from people in a public forum who are themselves part of the Information Commissioner's investigation, including people like Brittany Kaiser, who has given evidence to us, so I see no particular reason why you cannot share that with a parliamentary Committee.

**Mike Schroepfer:** Again, I am happy to share it with the Committee, but I would prefer to share it in private, just out of an abundance of caution since they are leading the investigation on this.

**Chair:** Fine. We will come on to that.

Q2343 **Jo Stevens:** Just a point arising out of the clarification. Thank you very much for confirming the details about the NDA. There was one point that you left out, though. I asked a question about whether any payment had been made to Dr Kogan, or from Dr Kogan to Facebook, as a consequence of signing that NDA.

**Mike Schroepfer:** Thank you for asking. As part of this contract, no payment was involved.

Q2344 **Jo Stevens:** Was any other payment made?

**Mike Schroepfer:** I'm sorry, I don't know what that means.

Q2345 **Jo Stevens:** You said there wasn't a payment as part of this contract. Was any other payment made?



## HOUSE OF COMMONS

**Mike Schroepfer:** I believe there was no payment involved in this at all.

**Jo Stevens:** Thank you.

Q2346 **Brendan O'Hara:** You have said quite a few times today that you are doing lots of things now, but isn't it the case that this is a crisis that has been coming down the line at Facebook for a number of years, and you have chosen to do very little, or tinkered around the edges of it, rather than facing up to the crisis that was inevitably going to come?

**Mike Schroepfer:** Which issue are you talking about?

Q2347 **Brendan O'Hara:** In terms of Cambridge Analytica, the Aleksandr Kogan issue and the data harvesting—this was an issue that was always going to come to a head, don't you think?

**Mike Schroepfer:** Again, as I said earlier, the idea that I would be here today was not in my consciousness even back then, when we were building the platform. We were trying to build great tools for developers and consumers to use these things. With the fullness of wisdom and of time, we know now that there is more we wish we had done earlier, but all I can tell you is what I know I was thinking at the time, and what the teams were, which was trying to build these experiences. If we thought it was going to end in this spot, I think we would have done those things earlier.

Q2348 **Brendan O'Hara:** You told my colleague, Ms Stevens, that Facebook did not read all the terms and conditions of the apps, but you had automated checks at that time. When did that end?

**Mike Schroepfer:** I think there are a few things here. There is the specific language of the terms and conditions of developers; we had automated checks to make sure those terms and conditions existed. That is similar to, again, app stores you will see on many platforms. Most mobile platforms do not actually read the terms and conditions, they just require that they are there, even to this day. The terms and conditions is an important part, but even if we had read the terms and conditions of an app and it seemed like it was fine, there is a much deeper set of questions about what data that app is asking for, for what purpose and whether it is an overreach of data. To the Chairman's astute questions earlier, the challenge is making sure that there is no overreach on the data, because then if something goes wrong it is harder to deal with. Our focus was on the review—

Q2349 **Brendan O'Hara:** So where were those safeguards that you talked about?

**Mike Schroepfer:** I'm sorry, sir?

**Brendan O'Hara:** Where were the safeguards?

**Mike Schroepfer:** In 2011, prior to the change in 2014, there was a reactive reporting process that we had put in place, so that if someone



## HOUSE OF COMMONS

had concerns about a developer or a developer app, we had a team at the company that was working with the developers and would enforce, either due to external reports or other concerns we would raise. The shift that happened was one from consumer visibility and choice, which was reactive, to proactive review in 2014, where we had to look at the apps and understand the developers upfront before they could use the platform.

**Q2350 Brendan O'Hara:** Do you accept that it shows there has been a failure of the system that we are where we are today, given that you recognised in 2011 that this was happening and that there was a need for it to be looked at, and yet this crisis has been allowed to develop over the course of seven years? Your sitting in front of this Committee today would suggest that there has been a complete failure of safeguards and systems within the company.

**Mike Schroepfer:** I agree that, knowing what we know now, we wish we had done more then, at the time. Being there at the time, the idea that we would end up here was not where we thought it would go.

**Q2351 Brendan O'Hara:** When was the Facebook app review team established?

**Mike Schroepfer:** Again, we had reviews that we would do on a proactive basis whenever there was concern raised or a report about an app. I don't know the exact genesis of that, because the platform started before I joined the company. I think it may have occurred in the very earliest days of the platform, but I don't know the exact year. Then, again, we went to the proactive review model in 2014.

**Q2352 Brendan O'Hara:** What prompted the change in 2014?

**Mike Schroepfer:** Again, in responding to the Chair's questions, we had gone through multiple evolutions of the platform on a variety of different features. It started on the web, then just on Facebook itself, then it moved to allowing you to use Facebook features on your own website. It moved to mobile phones. We had multiple iterations of the controls that people had to see what data was there. We went through multiple evolutions, and then there was the 2014 change to lock down the platform more. It was a big event, but it is one of many iterations. There have been subsequent iterations. I announced even further changes to the platform a month or two ago in the abundance of caution.

**Q2353 Brendan O'Hara:** In your written submission you say that, although you announced changes in 2014, you know that they didn't go far enough. That kind of goes back to the heart of what I was saying right at the start. You were not unaware of this looming crisis. A company such as Facebook, with its aggregated intellect, could not have been unaware of this looming crisis. You tinkered around the edges in 2011 and again in 2014. Did nobody at a high level of Facebook say a crisis was looming unless you fundamentally changed what you do? Did everyone buy into the changes in 2014 and believe that that was the answer?



## HOUSE OF COMMONS

**Mike Schroepfer:** Again, I can tell you what I know and thought at the time. Hindsight is always 20:20. There is a real tension, which is true of the changes we made in the last month. As we made them, we broke a bunch of applications on the web and on mobile phones. That happened in 2014. This was useful functionality that consumers enjoyed, and we had this really strong tension between how much you can build these social applications versus how safe you are. I think there is a trade-off there.

I will tell you very honestly that, if I knew at the time that I would be testifying in front of this Committee about election interference as a result of the platform, I would have made some changes. This is not where we thought this would end up. I am not trying to shirk our responsibilities at all. We have been very clear that we wish we had done more. The best we can do with that is to understand how to focus now on not making that mistake again.

Q2354 **Brendan O'Hara:** Going back to your written submission, where you said that you knew the 2014 changes did not go far enough, when did you realise that they had not gone far enough?

**Mike Schroepfer:** As I said, as a result of the concerns over Cambridge Analytica. Again, the issue here is the use of user data, and the reason that you are all rightly concerned is that user data impact on its own is a big problem, but the idea that it would be involved—in any form—in an election is a much bigger deal. It basically caused us to stop work at the company and say, "Okay, what are all the possible issues that we may have?" We had to do the risk planning on all possible things that we had not then seen but that might have happened.

We are in a different world now from then. We have seen things, and you are asking me fair questions. These things have been happening, and we are on notice of them. What are all the changes we could make so that, if something were to happen in the future, I could answer to your questions that I have done absolutely everything I knew how to do to prevent it? That is the sort of mood we are operating in now. We have made additional changes to the platform and products through reviews. We will make more changes as time goes on.

Q2355 **Brendan O'Hara:** Yes, but when did you realise that the changes you had made in 2014 were insufficient?

**Mike Schroepfer:** Again, I think it was this review in the last month, when we announced this additional set of changes. They weren't actually in response to a specific issue but to the broader issue of abuse of the platform. Again, we switched the company's stance to be as conservative and locked down as we think we can, so that I don't have to come back and visit you in a year or two on a different issue that we wished we had known about. That is the best thing I can spend my time on right now.

Q2356 **Brendan O'Hara:** What I am struggling to get is that—you are saying



## HOUSE OF COMMONS

you discovered a month ago that what you did in 2014 was insufficient, but we have already had a witness, Sandy Parakilas, who himself said in 2012 he went to Facebook senior management and warned of their lax data security procedures. There is a pattern here. There is 2011; there is this warning in 2012; there is your own admission in 2014; and now there is this crisis that we are in the middle of. Isn't it the case that the only difference now, and why you are acting now, is simply that the rest of us know? Had it not exploded in the public forum in the way that it has, nothing would have really changed, would it?

**Mike Schroepfer:** I disagree, because the changes in 2014, again, weren't because of a big public uproar like this. There has been a constant evolution of the platform. I think the threats are dynamic. In 2014, we were not worried about the Russian IRA interfering in elections. That was a new threat that we didn't understand at the time, and so it is hard to have built a system that was fully responsive to things we didn't know about.

The best we can do now, sir, is spend all of our time and energy asking those hypothetical questions about what are all the possible vectors of abuse and what are the reasonable trade-offs against safety and security. I think there isn't an easy, complete solve for all of these things. I think all of us live in a world that makes trade-offs on a daily basis that trade convenience versus safety in a variety of ways. I think, again, we are trying to get that balance right on the spectrum continually as we go.

Q2357 **Brendan O'Hara:** What you are asking us to believe is that nobody in the entire Facebook organisation between 2014 and last month saw this coming. Nobody saw this crisis that we are now in the middle of coming. Are you asking me to believe that?

**Mike Schroepfer:** I can tell you what I know and you take your own judgment from that. I can tell you that, again, the changes that were made in 2014 were quite disruptive to the developer community. They were painful for a lot of companies, who were very frustrated by the changes we were making, but they were one of many we were trying to do along the way. Similarly, when we announced these recent changes we again broke many apps in trying to do it. Those changes were because we were sitting there again saying, given how much concern—understandable concern, fair concern—there is over these issues, I do not want to be in this situation again, so what are all the ways we can do it? It is simply a change in security posture. You may or may not choose to be at a different level of security and threat awareness in the multiple environments, depending on what you know about what the risks are, versus convenience.

Q2358 **Brendan O'Hara:** You say again in your written submission that you are conducting a full review of any app with suspicious activity, which is commendable, but isn't it the case—and how would you respond to the accusation—that the reason you are doing it now and you didn't do it prior to this publicity is simply because it was far too profitable for



Facebook not to act?

**Mike Schroepfer:** I think it is important to note that we don't charge for the platform, so we don't make money by the more people who use it. I think the reality, as I have said, is that we are sort of more in a no-stone-unturned world right now, where we can't change the prior events, and I am very disheartened by that, but what we can do is spend our time trying to do everything we can to understand in more detail what actually happened not just in this case but in any related cases—because I think that is important, that people get a full accounting of what happened—and then do all of the work we can to dramatically reduce the probability that this happens in the future.

Q2359 **Brendan O'Hara:** On the app review team, how does it compare in its structure, its scope and size to what it was in 2014?

**Mike Schroepfer:** I don't actually know that it changes over time based on the number of developers and what's happening, so I don't know that off the top of my head.

Q2360 **Brendan O'Hara:** Do you confidence that the app review team is large enough and sufficiently well-resourced now, compared to what it was?

**Mike Schroepfer:** I will say that we have challenges getting all the resources we need to deal with all the different threats we have on the platform. It is just an unfortunate reality that we are growing everything. Mark has talked about adding 10,000 people just this year to help the security and content review. My core job is to hire the best machine learning and AI professionals around the world, to help us build systems that can do this more efficiently. In every walk of these issues—if you choose any we are talking about today—I am trying to hire more people to help solve those problems. If you picked any one and said, "Do you want to hire more?", the answer is yes.

Q2361 **Brendan O'Hara:** Mr Zuckerberg said that he has committed Facebook to auditing any and all suspicious apps. In your role, how will you ensure that that audit will be complete and how will you be able to audit the companies and apps that have since shut down, or can you?

**Mike Schroepfer:** We are in the middle of the audit now. Because we are dealing with historical events, we may not always have perfect information on all these things, but I think that the reason we are doing this gets to the heart of a lot of the important issues you are raising—that is, let's not wait for something to come to light from someone else. Let's understand what is going on here, make sure that we can properly inform consumers and make sure that we can have a dialogue about how these systems should work in the future. We may well find another app that has done something unexpected and that may inform how we build technical restrictions to that. Maybe they use a piece of data that we thought was innocuous, but it turns out not to be. These are the sorts of things that we need to understand to be able to build defences, restrictions and operational control to prevent these things in the future.



## HOUSE OF COMMONS

Q2362 **Brendan O'Hara:** Have you set a deadline for the completion of this audit?

**Mike Schroepfer:** We are going as fast as we can.

Q2363 **Brendan O'Hara:** There is no deadline. I know that Mr Zuckerberg said, "We expect it to take many months". Is that maybe years?

**Mike Schroepfer:** We have mobilised teams inside the company. We have hired many external resources. It is hard to set a deadline except as fast as we can.

Q2364 **Brendan O'Hara:** A couple of final questions. When you are doing your audit of the apps, how do you audit a company for which the trail has been lost or for which the contact details have changed? How would you do that?

**Mike Schroepfer:** This is going to be a challenge, again, because we are dealing with historic events, so we will not have perfect information or detail on any of these things. It may very well be that this company is defunct, but we can look at how they used the platform. Maybe there were two people who used the app and they asked for relatively innocuous data, but the chance that that is a big issue is a lot lower than an app that was widely in circulation. We can at least look at that sort of information and try to chase down the trail. If we have concerns about it, even if the company is defunct, it is possible that we can find former employees of the company and find out more information about it. This starts with trying to identify where the issues might be and then run the trail down as much as we can. As you highlight, there are going to be limits to what we can find, but I think our goal is to understand this as best we can.

Q2365 **Brendan O'Hara:** Have you considered inviting the Information Commissioner's Office to get involved in current or future audits?

**Mike Schroepfer:** We are giving them regular briefings on all the work we are doing and sharing a tremendous amount of information with them. I would guess that we are sharing information on this too, but I know that I personally shared a bunch of details about a variety of things we are doing. Similarly with the Electoral Commission, we want them to get to the heart of this too.

Q2366 **Brendan O'Hara:** I have two final questions. Can Facebook collect data of non-Facebook users, and if it can, how?

**Mike Schroepfer:** We discussed this a bit briefly, so I will recap. Forgive me, please interrupt if I am covering things that you think I have already covered. There are tools that websites can install on them. They can install code from third parties. These are common tools that are available. I highlighted that your own website uses tools from six different companies. When I visit the parliamentary website to read the news about my testimony, you have six different companies that have installed code on that website. The browser I am using to visit your site



sends a piece of information called a cookie, which sends data to each one of those different companies. We are one of those in this case, because you have chosen to include Facebook code on the site. In which case, we would get a log on our servers of that cookie information, which is information about the browser or device you are using to connect to that. Importantly, if you are not a Facebook user, it means we don't have things like name and personal, identifiable information. All we really know is that this browser instance had hit this site at this time. This is kind of basic log information—that is the basic information, the logging.

**Q2367 Brendan O'Hara:** What use to you is that information, and what do you do with it?

**Mike Schroepfer:** There is a use for it. The reasons why third parties install this are multiple. For example, the "Like" button is popular, or the "Share" button, so people who are reading an article can re-share that on Facebook. We have multiple uses for it.

One of the actual important uses of this is understanding—we talked a lot earlier about inauthentic accounts, fake accounts and people trying to evade our systems—if we have seen this browser before, if it has visited our site, whether it has a relatively normal pattern of behaviour. If it then shows up and decides to register a Facebook account, it is probably less likely that it is a spammer or scammer than this brand-new thing that we have never seen before showing up and trying to register an account. It is one of many signals we would use to try additional means to prevent that person, for example, registering an account at that time.

**Q2368 Brendan O'Hara:** So if I am not a Facebook user but you pick up my data, that is what you will use it for.

**Mike Schroepfer:** We use it for several things. We use it primarily for security—that is one. One of the things that these tools provide for websites is counting and statistics, analytics, on how many different devices visited. It is common for online journalists to say how many people read this article versus this article. In this case, we don't really know people, because it is associated with a browser cookie, but we could say that X number of different browsers had visited this site, and that sort of information is useful for most web publishers, which is why they tend to include these services, and many others.

**Q2369 Brendan O'Hara:** Finally, as you know, the European Union's general data protection regulation takes effect next month. That will give individuals much greater control over their own personal data, and I suspect that Facebook will be fully and entirely compliant with that. Post-GDPR, has Facebook any plans to transfer all or any personal data of EU citizens out of the EU to North America?

**Mike Schroepfer:** As part of operating our services, we run data centres all over the world. Those data centres are in the United States, Sweden, Denmark and Ireland, and data will be transferred between those different data centres.



**Q2370 Brendan O'Hara:** But under the protections that GDPR affords European Union citizens post-GDPR, which is next month, can you guarantee that you will be entirely compliant with that level of privacy afforded by the GDPR for every single EU citizen who is a Facebook user, and that they will not be transferred to a server in America, where the GDPR won't apply?

**Mike Schroepfer:** Yes. I want to be very clear. We are excited to be in compliance with the GDPR for every single EU citizen, no matter where the computer capacity is. I actually think that the GDPR has been a good moment for all of us—as we have seen with these issues raised today—to get more visibility into the issues of control of data, or on choices consumers can and cannot make on these different things. As part of this we show a screen to every single user in the EU, which requires you to go through and select a bunch of options to opt in to a variety of different things, to agree to the terms of service to make sure that you understand it. A lot of that process highlights controls that already existed somewhere else in the app, as we discussed. Your colleague raised earlier the challenges of finding and understanding all the controls, so putting all the key things in one place is a good chance for people to understand.

**Q2371 Brendan O'Hara:** To be absolutely clear, as an EU citizen and a Facebook user, I will have the full protection of the GDPR, and Facebook for me as an EU citizen will be entirely GDPR-compliant.

**Mike Schroepfer:** As I understand it, we are doing full compliance with the GDPR for EU citizens. In fact, many of the basics of GDPR are also being rolled out to the rest of the world. So the series of screens that we have developed for the GDPR we are in the process of localising for other regions, to roll them out to other regions. We think that the idea of giving people a whole lot more information on what is going on and having them make choices is good.

**Q2372 Brendan O'Hara:** Could you explain to me why Facebook have just transferred 1.5 billion accounts from Ireland to the US?

**Mike Schroepfer:** My understanding of one of the provisions of the GDPR is that it specifies a lead regulator. In this case, it would be Ireland, the Irish DPC, which was required to be the lead regulator for all the users served out of that region. We have had very clear feedback from people in other regions—South America and Asia—that they would prefer to work with a local regulator to understand issues for that region. By moving those users in those other regions from Ireland to the US, the US law does not have a notion of the lead regulator, so the US does not become the lead regulator. It opens up the opportunity for us to have local markets, have regions, be the lead and final regulator for the users in that area.

**Brendan O'Hara:** I am sorry. I did not understand that.

**Mike Schroepfer:** It is very simple. If I am a—



## HOUSE OF COMMONS

Q2373 **Brendan O'Hara:** But why have those accounts been transferred from Ireland to the US immediately ahead of the GDPR?

**Mike Schroepfer:** Once again, my understanding is that the goal is that if I am a citizen of Argentina, I live in South America, and I want a local regulator for my country or my region to have the final say on issues related to how Facebook works with me and my data, and I want them to have regulations, that would be in conflict with the GDPR, if those citizens were covered by the GDPR, which specifies that there is a lead regulator in Ireland. We wanted the flexibility to make sure, as we have been requested very vehemently by many regions, that they would be able to have the final regulatory say for people in their region.

Q2374 **Jo Stevens:** It is purely coincidental that it is three or four weeks ahead of the GDPR.

**Mike Schroepfer:** Again, as I said, it is so that we can work with regulators in those regions and not have it mandated via law that they must be regulated by another country.

Q2375 **Ian C. Lucas:** Who owns Facebook content? Is it the person who puts it there, or is it Facebook?

**Mike Schroepfer:** It is the person who puts it there. They have rights to download it and delete it as they see fit.

Q2376 **Ian C. Lucas:** You mentioned the example of cookies on the House of Commons website. If I am not a Facebook user, and I go to the House of Commons website, and the cookie puts me in touch with Facebook, even though I have not ticked any Facebook terms and conditions, who owns that information?

**Mike Schroepfer:** That is because I am visiting the parliamentary website. Assuming you are compliant with the laws in the EU regarding consent for use of cookies, which require—you will have seen the banner up there. You as the website are consenting me as the user the fact that you use cookies. Again, you use cookies from your own domain plus six other domains—actually much more than six other domains, but it boils down to six companies—so the user does not go and get consent from each one of those six companies, they get consent from you that you are using cookies, and that is what controls the interaction between the user and your site.

Q2377 **Ian C. Lucas:** Who owns the information that Facebook hold that I have visited the House of Commons website?

**Mike Schroepfer:** Again, if you are not a Facebook user, this is not personally identifiable information.

Q2378 **Ian C. Lucas:** I didn't ask that. It is information, though, is it not?

**Mike Schroepfer:** It is information about a machine—about a browser—

Q2379 **Ian C. Lucas:** It is information about an individual. It is an unidentified



## HOUSE OF COMMONS

individual, but it is information about an individual. Who owns that information?

**Mike Schroepfer:** Respectfully, I disagree. It is very common for people to share phones and share browsers. Multiple people use the same device to visit a site. If two different people use the same device to visit that site, I do not know the difference between them, I just know that this browser visited it at that time.

Q2380 **Ian C. Lucas:** Forgive me, Mr Schroepfer. It is a piece of information that Facebook holds about a contact that was made, even though the person who made the contact may not be a Facebook user. That is correct, is it not?

**Mike Schroepfer:** It is a piece of information. Technically, there is a thing called a cookie on the browser, which identifies the browser. For example, if you—

Q2381 **Ian C. Lucas:** I understand that, but I come back to the question, who owns it?

**Mike Schroepfer:** I think in that case, we are controlling the logs. I do not know the rules over who—

Q2382 **Ian C. Lucas:** So Facebook own it?

**Mike Schroepfer:** I do not know the legalities of who owns that piece of information, but again, it is not personally identifiable to you. It is common practice on a lot of websites. Every website you visit gets a log of visitation.

Q2383 **Ian C. Lucas:** Facebook own that information, even though I, as the source of the information, may not have a relationship with Facebook.

**Mike Schroepfer:** There are two things here that I want to clarify. I don't know that it is you. You can clear your cookies. Someone else can use the browser. The only thing I know is this browser visited this site at this time. It is not associated with any personally identifiable information, so even if I wanted to ask you to delete that data, I would not know how to know it was yours. We would have to know about you in order to do it, at which point we would have associated it with you. That is the challenge. This is, again, how every website on the web and every analytics product that is providing this information about who visits the website works.

Q2384 **Ian C. Lucas:** Is that information of value?

**Mike Schroepfer:** I discussed before a couple of uses of it. One of them is security, so we can tell the difference between, "This browser has been here a couple of times before," and, "It's brand new—we've never seen it—so we may have our shields up a bit more." And, again, it is a service to the website. If they choose to include our code, we can do things like say, "We've seen three different browsers, or three different phones, visit this article and six visit this article."



## HOUSE OF COMMONS

Q2385 **Ian C. Lucas:** Can I just ask you to give me a yes or no answer to this question? Is that information of value to Facebook?

**Mike Schroepfer:** Again, these are complicated issues, so I want to make sure I'm being very clear. We use it as a free service to websites because protection is—

Q2386 **Ian C. Lucas:** I asked you a very straightforward question.

**Mike Schroepfer:** For security purposes, absolutely. If you made us turn this off, it would be devastating for our ability to detect fake accounts.

Q2387 **Ian C. Lucas:** Thank you. Can I ask you about an answer that you gave me to a question earlier? Did Facebook pass user information to Aleksandr Kogan or Cambridge Analytica?

**Mike Schroepfer:** I'm sorry, I don't actually—

Q2388 **Ian C. Lucas:** Earlier on, I asked you about the fact that Cambridge Analytica certified that they had deleted data. Do you remember that—in 2015?

**Mike Schroepfer:** Yes.

Q2389 **Ian C. Lucas:** So did Facebook ever transfer user data to Cambridge Analytica?

**Mike Schroepfer:** To my knowledge, no. What has happened here is that Mr Kogan, or GSR, had an app, it got access to information by using the platform, and then he transferred the data to Cambridge Analytica.

Q2390 **Ian C. Lucas:** Did Facebook transfer information to Mr Kogan?

**Mike Schroepfer:** Mr Kogan was an app developer. He installed an app on the platform, and that app got access—

Q2391 **Ian C. Lucas:** I would really like a straightforward answer to the question. Did Facebook transfer information to Aleksandr Kogan?

**Mike Schroepfer:** Again, I feel like you are asking a very specific question, so I want to make sure that I am getting to the heart of what you are trying to find. As a result of Mr Kogan running an app on the platform, that app, when users used it, had Facebook user information in it, which Mr Kogan would have on his servers. So that information was transferred from one party to another as part of using that application on the platform.

Q2392 **Ian C. Lucas:** So he extracted information from Facebook? Is that a way of describing it?

**Mike Schroepfer:** I think it is a way apps work on any platform. They get access to information in order to serve the user.

Q2393 **Ian C. Lucas:** But you were unhappy about that, and that was why you asked him to delete it.



## HOUSE OF COMMONS

**Mike Schroepfer:** No. I want to be clear. What we designed the platform for was to use information to build great products. If you want to build a social game that other people want to play with, you need the right information for that. The thing we objected to, which was clearly against our terms of service, was using information for one purpose—"I want to get people to install this app"—and then taking that data and reselling it or giving it to another party for a different purpose. That is something consumers obviously object to. It is clearly against our policies. That is the rub of why we are here today: making sure this data is not used in ways that it is not intended for.

Q2394 **Ian C. Lucas:** Mr Schroepfer, I am going to give you some evidence that we heard at an earlier hearing from Facebook. I just want you to see it.

**Mike Schroepfer:** Thank you.

Q2395 **Ian C. Lucas:** Did you know that we heard evidence from Facebook in Washington DC in February?

**Mike Schroepfer:** Yes.

Q2396 **Ian C. Lucas:** Have you read that evidence?

**Mike Schroepfer:** I am looking at it now. I have not.

Q2397 **Ian C. Lucas:** You have not read the evidence that your company gave this Committee in Washington DC? You had not read it before today?

**Mike Schroepfer:** I'm sorry, I'm reading evidence from something else that's not Washington DC.

Q2398 **Ian C. Lucas:** Sorry. I am going to take you through the evidence very closely.

**Mike Schroepfer:** Great.

Q2399 **Ian C. Lucas:** Have you read the evidence previously? **Mike Schroepfer:** Which evidence are you referring to, sir?

Q2400 **Ian C. Lucas:** The evidence that Facebook gave to this Committee in Washington DC.

**Mike Schroepfer:** I'm sorry; you mean the US Committee—

Q2401 **Ian C. Lucas:** We had a meeting with Monika Bickert and Simon Milner. They gave evidence to this Committee in a session in Washington DC.

**Mike Schroepfer:** Okay.

Q2402 **Ian C. Lucas:** Did you know that?

**Mike Schroepfer:** I'm sorry; I've been confused. Because it was Washington DC, I thought you might have been talking about the congressional testimony.

Q2403 **Ian C. Lucas:** No, I'm talking about evidence to this Committee in



## HOUSE OF COMMONS

Washington DC. Did you know that that evidence had been given?

**Mike Schroepfer:** Yes.

Q2404 **Ian C. Lucas:** Have you read that evidence previously—before today?

**Mike Schroepfer:** I have read some of it.

Q2405 **Ian C. Lucas:** Do you know Simon Milner?

**Mike Schroepfer:** Yes.

Q2406 **Ian C. Lucas:** What is his position?

**Mike Schroepfer:** He has recently changed positions, but I know that he has been involved in policy issues here in the EU.

Q2407 **Ian C. Lucas:** We asked Mr Milner about Cambridge Analytica. My colleague Mr Matheson asked him a question, and I'm going to read it. It's question 447. Mr Matheson asks: "Have you ever passed any user information over to Cambridge Analytica or any of its associated companies?" Simon Milner's reply was: "No." Mr Matheson went on: "But they do hold a large chunk of Facebook's user data, don't they?" Simon Milner: "No. They may have lots of data, but it will not be Facebook user data. It may be data about people who are on Facebook that they have gathered themselves, but it is not data that we have provided." Mr Matheson went on: "How will they have gathered that data from users on Facebook?" And Mr Milner said: "There can be all kinds of things that these organisations do. I think what data they have would be a good question to ask them, rather than us. We have no insight on that." Would you like to comment on that exchange?

**Mike Schroepfer:** What would you like to know, sir?

Q2408 **Ian C. Lucas:** Do you agree with what Mr Milner said?

**Mike Schroepfer:** Well, we learned, subsequent to this—the challenge here again is that we did not give data to Cambridge Analytica. Mr Kogan ran an app on a platform. That app got data. He, again, as we talked about—in December 2015 we learned he may have transferred that to Cambridge Analytica. And the reason we have reopened all this is that, as you all have learned and we have learned last month, there are allegations that that data still existed at Cambridge Analytica. I still—

Q2409 **Ian C. Lucas:** Can I just stop you there? In November 2015, Facebook knew and were concerned about Cambridge Analytica, and you had an agreement of sorts, which you have referred to today, with both Cambridge Analytica and Mr Kogan for them to delete data. All that information was known to Facebook in February of this year, wasn't it?

**Mike Schroepfer:** The fact that that happened in December '15? Sure.

Q2410 **Ian C. Lucas:** So why was none of that information given to this Committee?



## HOUSE OF COMMONS

**Mike Schroepfer:** I'm not sure exactly as I read Simon's statement again. At the time, it was accurate, because we didn't think Cambridge Analytica had data and we had not given them data. The problem that has come up since then is the idea that they still retain data. Again, to this day, I still have not had eyes on a single piece of data there, so I don't know for sure, but we are assuming everything is true and they do have the data, and that is the problem we have today.

Q2411 **Ian C. Lucas:** Mr Schroepfer, you were very well aware or Facebook was very well aware in December 2015 that there had been this—I'm going to call it a data breach, which precipitated action on your part, so why did you not tell this Committee about that when we heard evidence from you in February?

**Mike Schroepfer:** Again, as I am reading these questions, they are a question of whether we gave them data or they have data. The answer to both those questions—on the first one, we, to this date, haven't given them data. And at the time, we, again, had legal certifications that they did not have that data anymore, so—

Q2412 **Ian C. Lucas:** Mr Schroepfer, to date, you have answered questions in a straightforward manner, but I have to say this. My colleague Mr Matheson said: "How will they have gathered that data from users on Facebook?" And the response is: "There can be all kinds of things that these organisations do." You had very specific knowledge as a business, as a company—Facebook—in February of what had happened in this case. Why didn't you tell this Committee about it?

**Mike Schroepfer:** I don't know why he did not elaborate on that particular point. I don't even know if he at the time knew all the details of this. A lot of this stuff has come to light in sharp relief for us in the last month. I am trying to give you the best information I have on why someone said something.

Q2413 **Ian C. Lucas:** Can you tell us whether Mr Milner answers to you in Facebook?

**Mike Schroepfer:** I don't believe so.

Q2414 **Ian C. Lucas:** Who does he answer to?

**Mike Schroepfer:** I believe he reports up through our chief operating officer.

Q2415 **Ian C. Lucas:** Do you think he told us the truth?

**Mike Schroepfer:** I know Mr Milner to be an honest person, so I am guessing he was telling you the best of his knowledge at the time.

Q2416 **Ian C. Lucas:** Do you think that Mr Milner should have told us about the agreement between Cambridge Analytica and Facebook when he gave evidence to us, when we raised Cambridge Analytica with him?



## HOUSE OF COMMONS

**Mike Schroepfer:** I think we are trying to do the best we can to give you all the information.

**Ian C. Lucas:** I don't think you are, Mr Schroepfer. I don't make this allegation lightly: I think Facebook concealed the truth from us in February.

**Mike Schroepfer:** Again, I am trying to give you all the information I have now. I do not know whether he was even—

Q2417 **Ian C. Lucas:** In February, Facebook had all the information that you have given us today about the agreement with Cambridge Analytica, did it not?

**Mike Schroepfer:** We have tremendously more information about this entire situation now.

**Ian C. Lucas:** You had the information about the agreement with Cambridge Analytica that you made in December 2015.

**Mike Schroepfer:** Again, I don't know whether he was specifically informed of that. I am guessing that he did not actually know, but I don't know for sure.

**Ian C. Lucas:** You are guessing he didn't know.

**Mike Schroepfer:** I don't know; I haven't spoken to him about it.

Q2418 **Ian C. Lucas:** Who knows?

**Mike Schroepfer:** Who knows what, sir?

Q2419 **Ian C. Lucas:** Who knows about what the position was with Cambridge Analytica in February this year? Who was in charge?

**Mike Schroepfer:** I do not know all the names of the people who knew that specific information at that time.

Q2420 **Ian C. Lucas:** We are a parliamentary committee. We went to Washington for evidence and we raised the issue of Cambridge Analytica. Facebook, as an organisation, concealed evidence from us on that day. Is that not the truth?

**Mike Schroepfer:** I completely understand the root of what you are getting at. You have a right to get all the data you need at every point in time. Again, I don't know what happened here. I am doing my best to give you all the data you need today.

Q2421 **Ian C. Lucas:** You are doing your best, but the buck does not stop with you, does it? Where does the buck stop?

**Mike Schroepfer:** It stops with Mark.

Q2422 **Ian C. Lucas:** It stops with Mark. Will Mark answer these questions?



**Mike Schroepfer:** I don't know.

Q2423 **Ian C. Lucas:** Does he know? When did he first know about Cambridge Analytica?

**Mike Schroepfer:** I don't know the answer to those questions.

Q2424 **Ian C. Lucas:** Have you discussed Cambridge Analytica with Mark Zuckerberg?

**Mike Schroepfer:** Over the last few months, these topics are pretty much all we discuss.

Q2425 **Ian C. Lucas:** Did you talk to Mark Zuckerberg about the agreement between Cambridge Analytica and Facebook that was reached at the end of 2015?

**Mike Schroepfer:** No, I am not sure I was aware of it at the time.

Q2426 **Ian C. Lucas:** When did you first find out about it?

**Mike Schroepfer:** Within the last month.

Q2427 **Ian C. Lucas:** Why won't Mr Zuckerberg come to us and answer the questions?

**Mike Schroepfer:** I understand that he has been getting requests from all over the world to come and talk about this. He is trying to dedicate his time in the office to solving these problems and to get to the heart of it. He asked me to come—I am one of the senior members of the leadership team. I am trying to do my best to answer the questions. We thought, particularly since you wanted to go into fake news and to understand the details of this, that I could cover the technical details—the overlap between the different audiences and how it may have affected the ads. My goal was to give you much more detailed information than you previously had, not comment on prior—

**Ian C. Lucas:** We want the truth.

**Mike Schroepfer:** I understand that.

**Ian C. Lucas:** We did not get the truth in February.

**Mike Schroepfer:** Again, I think he told you the best information he had at the time.

Q2428 **Ian C. Lucas:** That's not good enough. We are a parliamentary committee. We are elected individuals. There are millions of constituents who are concerned about this issue. I remember Mr Zuckerberg giving an interview back in 2009 to the BBC—he was prepared to talk to them. Do you not think it would be the right thing to do for him to come and explain to us why someone representing Facebook did not tell us the full truth in February?



## HOUSE OF COMMONS

**Mike Schroepfer:** Our goal is to get you all the data you need in extensive detail: written statement last night, the additional information I provided to multiple commissions here in the UK and the time I am spending today. I will do my best in the future to make sure that as things change you get the information. I completely understand and agree with your assertion about needing to get to the truth and the heart of these matters. I have no quarrel with that.

**Ian C. Lucas:** So when we speak to Facebook employees, we want to be told the full truth.

**Mike Schroepfer:** I understand that.

Q2429 **Ian C. Lucas:** We were not told the full truth in February, were we?

**Mike Schroepfer:** Again, I do not know what he knew or didn't know.

**Ian C. Lucas:** We were not told about this agreement.

**Mike Schroepfer:** Again, I am not sure that he knew about it. I don't know the specifics of it. I do know what I know now and will do my best to tell you everything I know about these topics. That is the best I can do.

**Ian C. Lucas:** You have a Head of Integrity at Facebook.

**Mike Schroepfer:** Community integrity. I misspoke, sir. The idea is to understand the community standards, security and different issues of content on the platform.

Q2430 **Ian C. Lucas:** Mr Schroepfer, I remain to be convinced that your company has integrity, after what they said to us in February. Does your company have integrity?

**Mike Schroepfer:** I believe we do. As I said earlier, I personally try to put my heart into building products that are good for people. I believe deeply in our mission and our products, and the good that they can do in the world. It hurts when we make mistakes. It hurts when people abuse our platform. We are human and make mistakes. I wouldn't want to work at a company that I didn't believe had integrity. I have worked with Mark and Sheryl for 10 years now. It is the longest stint in my professional career. I understand your concerns. I understand the scepticism. It is right to have that appropriate level of scepticism. It is your job. The best I can do at this point is provide you with detailed information on all of these things, and commit that I will work with you and others to the best of my ability, most importantly to prevent any of these things from happening in the first place, and secondly, as we understand the issues here, to share them openly with you, the Electoral Commission and the ICO.

Q2431 **Ian C. Lucas:** When did you first discover the existence of the agreement? You said within the last month.



## HOUSE OF COMMONS

**Mike Schroepfer:** That is when I became aware of it.

Q2432 **Ian C. Lucas:** Would you ask Mr Zuckerberg to come to give evidence to us, to explain why his company did not give full disclosure to a parliamentary Committee in February?

**Mike Schroepfer:** I will certainly discuss everything that happened here today with Mr Zuckerberg when I return.

**Chair:** You may know that Mark Zuckerberg has agreed to give evidence to the European Parliament. It has been announced during the course of our session today.

**Mike Schroepfer:** I'm sorry, sir?

Q2433 **Chair:** Did you know that Mark Zuckerberg has agreed to fly to Brussels to give evidence to the European Parliament?

**Mike Schroepfer:** I did not know that. That is news to me as of right now.

Q2434 **Chair:** Okay, well that was reported since we have been in session. So he has obviously found time to get out of the office and go to Brussels. We will certainly be renewing our request for him to give evidence, given that he is planning to make a trip to Europe. Clearly, we respect the fact that you have given your time to be here today and answer our questions so far, but there are clearly some questions that you do not have the information on or may refer to a bit of the business you are not directly engaged with. Therefore, we still do need the opportunity to put some of these questions to him.

Following what Mr Lucas said, what has been a frustration for us in this inquiry is a pattern of behaviour from the company, an unwillingness to engage, and a desire to hold on to information and not disclose it. When we started this inquiry, Facebook didn't want to respond to any of our requests for information and wanted to deal only with the Electoral Commission and the Information Commissioner's Office. When we asked Facebook if it would investigate, on the same terms that it had done in America, to look for evidence of Russian involvement from the Internet Research Agency during the Brexit referendum, Facebook refused to do that and then subsequently changed its mind. We had the evidence session in Washington. We asked not just Simon Milner but Monika Bickert about vulnerability of user data and about the relationship with Cambridge Analytica. We asked Monika Bickert expressly whether she knew of an instant where a data breach may have occurred and she wasn't able to answer that question. Subsequently, we are aware that the company knew—whether those two individuals were aware, they were selected by Facebook to represent the company—an awful lot more about all of these issues than it was prepared to discuss at the time. We wouldn't be having this discussion now if this information hadn't been brought into the light by investigative journalists and Facebook even tried to stop that happening as well. While none of these acts may be—some



## HOUSE OF COMMONS

of them have been caught out—directly telling a mistruth, it is a pattern of behaviour, of seeking to pretend that this isn't happening and that these inquiries are unwelcome.

It has been a cause of great frustration to us. We are grateful that you are here today, but I hope you understand that Mr Lucas's line of questioning reflects a frustration that is shared by the whole Committee on our inability to get straight answers to what were fairly straight questions at the time. I don't think anyone looking at those transcripts in February, knowing what they know now, would feel that the Committee was given straight answers. Chris, did you want to come back in?

**Q2435 Christian Matheson:** Yes, on a few things, Chair. To follow on from what the Chairman and Mr Lucas have said, if you realised that what Mr Milner said wasn't entirely accurate, you might have been able to write to us and say, "We think we might not have given you the full picture here." Did it ever occur to you to contact the Committee and perhaps correct the evidence that he had given?

**Mike Schroepfer:** Again, I was not personally involved in this, so I don't know the details of that. I know that when the request came that you wanted a senior leader from the company, or Mark, to visit, I volunteered to visit because I thought it was an important enough issue that I wanted to make sure you guys got detailed facts, especially as it relates to a bunch of technical information about these things, which I think is critical to understanding both what happened and the possible impact it may have. Again, Chairman, I understand your concern deeply. I hope our actions from this week, in providing information not just to the commissioner but to yourself, my written statement and the documents we are submitting later on the contract and other things people have raised questions on in my time here, is a beginning of the feeling that you believe you are getting the information you want.

**Q2436 Christian Matheson:** Let me ask a technical question that might be more up your street: has Facebook ever been successfully hacked?

**Mike Schroepfer:** We are attacked all the time. There are fake accounts happening all the time, and I know we have had employees' laptops compromised by malware. We have had multiple attacks on the systems. It is a regular problem, as it is for most companies.

**Q2437 Christian Matheson:** Has that ever involved the theft, in this case, or the compromise of personal data?

**Mike Schroepfer:** I am not aware of any exfiltration of data in that way.

**Q2438 Christian Matheson:** Okay. A thought occurred to me when the Chairman was speaking to you earlier about the Martin Lewis bogus advertisements. Obviously, he is a very well-known personal finance expert in this country. Those were adverts paid for by the bogus advertisers, weren't they?

**Mike Schroepfer:** Yes, these are fraudulent ads paid for by third parties.



## HOUSE OF COMMONS

Q2439 **Christian Matheson:** Do you return the money to them?

**Mike Schroepfer:** Do we return the money to them when we shut down a fraudulent ad? I am not sure, actually.

Q2440 **Christian Matheson:** So you might keep the money that the advertisers paid?

**Mike Schroepfer:** I am actually not sure, offhand, what happens to that when we shut down a known fraudulent ad.

Q2441 **Christian Matheson:** Right. Could you find out for us, please, and let us know?

**Mike Schroepfer:** Sure.

Q2442 **Christian Matheson:** Because obviously, if money is being made off the reputation of Mr Lewis—if the fraudulent ads are being closed down but you are keeping the money—that would be rather a queer situation.

**Mike Schroepfer:** I understand, and to be clear, these ads are bad for users, so that is the reason why we care a lot about them. One of the biggest complaints we get is if someone sees an ad and is scammed, or sees content on Facebook and is scammed. That is the easiest way to do a heck of a lot of brand damage to our company, because they are going to be mad at us because they saw it on Facebook. I understand what you are getting at, but trust me, we are motivated to get these ads off the platform, because at the end of the day it is going to be an unhappy consumer, which is bad for us. Again, it is challenging because these folks are trying to evade our detection systems in multiple ways, so to get all of it down immediately is technically challenging, but I will say we are motivated to do it because it is a bad experience for our end user.

Q2443 **Christian Matheson:** Sure, and I get that it is bad for you, but there is a possibility, isn't there, that you will be given the ad revenue from these companies when they place the ads? There is a possibility that you will still get the revenue for these advertisements.

**Mike Schroepfer:** Again, I don't know specifically what happens in that case.

Q2444 **Christian Matheson:** If you could find out and let us know, I would be really grateful.

**Mike Schroepfer:** Absolutely.

Q2445 **Christian Matheson:** Chairman, if I may, I want to return to the issue of AggregateIQ, Vote Leave and the UK Brexit referendum. I understand that you said that \$2 million-worth of spend was made on that issue, though you could not tell Mrs Elliott whether that was Canadian or US dollars, or whether the amount was paid in sterling and you just converted it.

**Mike Schroepfer:** I know the amount, but I don't know whether that



was the currency or how it was paid for at this time.

**Christian Matheson:** When we were in Washington, Mr Lucas teased out from your colleagues the idea that Facebook would have a lot of information on these adverts. Those of us who are investigating this don't have any information, so we don't know what we don't know. I would like to ask whether the following types of information on that advertising campaign by Vote Leave is available.

First, would it be clear whether it was Vote Leave itself that paid for or placed the adverts through AIQ, or would you be able to identify whether it was one of the affiliated organisations, such as BeLeave or Veterans for Britain?

**Mike Schroepfer:** I think we have provided—it is probably more useful to do in written form, because I think you are going to ask a bunch of questions like this—

**Christian Matheson:** I am.

**Mike Schroepfer:** What we know is that AIQ spent it on a variety of different campaigns related to the referendum. You mentioned two pages. I think they had ad spend on both of those pages, on behalf of both of those pages.

Q2446 **Christian Matheson:** I am also interested in the billing—whether AIQ was billed or whether the bill was diverted to, or paid for by, a third party. If it is possible to have that information, that would be useful.

**Mike Schroepfer:** My understanding is that AggregateIQ was the advertiser of record, so they were the ones paying the bills for the advertising. Again, these are the details that I would want to get to you in writing to make sure we have all the specifics.

Q2447 **Christian Matheson:** For the avoidance of doubt, I am going to chuck a couple of extra questions in there so you know exactly what I am asking for you to reply to.

What is the total value of the spend? That would be spend by Vote Leave and also the affiliated organisations, such as BeLeave and Veterans for Britain, and indeed the Democratic Unionist party. I would like to know what the adverts were. Could we have copies of the adverts, even perhaps just in paper form as opposed to watching them? I would like to know whether it is possible to know to whom they were sent and how that would have been decided. Who would have decided that? Who would have decided who the recipients were and, in particular, how many of them? To whom were they sent and how would that recipient list be agreed? Is that the kind of thing you might be able to provide for us?

**Mike Schroepfer:** I know we have provided more extensive information to the Electoral Commission and the ICO. I think our teams would be happy to provide you with the information we have. I am guessing we can show you the ads. I don't know how detailed our logs are, because



they are not permanent, on who saw them. Your colleague asked this before, and understanding the ads is part of the issue, so we would be happy to get you the information you need.

**Q2448 Christian Matheson:** I am grateful. Forgive me, as you are being helpful in responding, but when we asked for this information in Washington, we were told we were going to get it and we never did.

**Mike Schroepfer:** My humble apologies, Sir. I will make sure.

**Christian Matheson:** I am really grateful.

**Mike Schroepfer:** There may be limitations with historical data, but with the data we have, we will make sure we follow it up.

**Q2449 Christian Matheson:** There were other campaigns running in parallel to the Vote Leave campaign and its affiliated or associated campaigns, for example Leave.EU, which was the unofficial campaign for the leave side in the Brexit referendum. I am interested in whether the same group of people who received the Vote Leave, BeLeave and DUP adverts received similar advertising from other Brexit organisations. The reasons is that allegations have been made to this Committee about data sharing in some areas and I want to see if there is any evidence of data sharing elsewhere, or whether a common dataset was used. I don't know, but I would be interested to see. Would you be able to find out whether the dataset of people who received the Vote Leave adverts also received adverts from other parts of Brexit?

**Mike Schroepfer:** Again, I will need to look and see. I will commit to trying to get you all the information you need. There may be limitations in the historical logs that we have for these, so depending on how detailed your requests are, and how small they are, we may not have everything.

**Q2450 Christian Matheson:** Do your best. I will be really grateful. Also, who paid for any additional adverts? What were they? I would be really grateful for the work that you are doing on that, because obviously it is central to one of the main areas we are looking at.

Could I ask a final technical question? Mr Farrelly in particular, who is not in his place, spoke earlier about the perils of dark ads—the ads that only the sender and the recipient and obviously Facebook can see. Is it technically possible that you could attach a little rider to every video that is uploaded on to Facebook to say who the original uploader was?

**Mike Schroepfer:** I believe that is generally true. If a page uploads a video, you know that that video is attributed to that page. I am not sure that is always true in advertisements. I think the root of what you are getting at is something we agree on, which is the need to have much clearer transparency on all of these things. As we said in June, we will get all of that if we are all running ads on a product or, again, for political ads in advance of the 2019 elections. So that specific feature, I am not sure—but we are going to go for much broader ads transparency very shortly.



## HOUSE OF COMMONS

Q2451 **Christian Matheson:** But it is possible. If I uploaded a video on to Facebook, you could automatically attach something to say, "This video was first uploaded by Chris Matheson."

**Mike Schroepfer:** We know the account that first uploaded the video, whether it is a personal—

Q2452 **Christian Matheson:** No, you know that, but the person receiving the video doesn't.

**Mike Schroepfer:** It would be possible to know that, yes.

Q2453 **Christian Matheson:** Would it be desirable?

**Mike Schroepfer:** I don't know. We would have to understand—that is the key. One of the things that we try to do is make sure that we get the right information in front of people, because when we give people information overload they ignore it. So I think the question is: what is the critical information I need to understand what this ad is about? This is why, for example, in the political ads we are trying to do a better job of saying who the advertiser involved in this was.

As to transparency, there is always an interesting question—what other ads is this advertiser running? As I am looking at an ad, to see other ads running gives a much better sense of what they are trying to do as a consumer. So I think your general idea of providing more information about the source is a very good idea. There are still the specifics, given the limited pixels on a screen—what is the critical information that does the best job to tell people what they need to know. I don't know what the specific, right piece of information is, but I agree with your general idea of getting authenticity in there.

Q2454 **Christian Matheson:** It just strikes me—if it is not one of these fake accounts that we spoke about earlier—if someone's name is going to be attached as the originator of an advert or a news story, it is more likely to be legal, honest, decent and truthful if it can be attributed to that individual.

**Mike Schroepfer:** I want to be clear: right now in the product, when you look at an ad, you can see who is running that ad. There is a click there to see who is running that ad right now, and it is associated with a page—you have to have a Facebook page to run an ad, so it is associated with that. I vehemently agree that authenticity and having actions associated with an entity or person is a critical part of all this.

**Christian Matheson:** Thank you.

Q2455 **Jo Stevens:** I have a very quick question to follow up on Mr Lucas's questions earlier. You understand that we feel very strongly that we were misled by Mr Milner in his evidence to us in February, in Washington. Facebook promoted Mr Milner in March, to vice-president. How many vice-presidents does Facebook have?



## HOUSE OF COMMONS

**Mike Schroepfer:** I don't know the number off the top of my head. It is in the order of 100, or a few hundred.

Q2456 **Jo Stevens:** Would you normally expect someone to go from director of policy in the UK to a vice-presidential role within the company?

**Mike Schroepfer:** That is not an unusual move.

**Chair:** You may not have seen it, but Mr Milner has certainly made his mark in Singapore, it would appear—certainly in front of our equivalent Committee there, who had a similarly testing engagement with him.

Q2457 **Christian Matheson:** I think he got a promotion because he had taken one for the team a couple of times.

**Mike Schroepfer:** I doubt that was it, Sir.

Q2458 **Chair:** I would like to pick up on a few questions, following on from earlier discussion of the GDPR and data downloads. Obviously there has been a lot of discussion about this, and about people's right to request to get their data back. If someone makes a request like that to Facebook, under the new GDPR rules, what will they get back from Facebook?

**Mike Schroepfer:** This product is already live now, so you don't have to wait until 25 May to look at it. There is a site called "View your information" or "Download your information" and you can look at extensive information on Facebook. You can either view it right there, if you want to sort it by time, or if you just say, "I want everything"—you can say, "Give me all the data." That takes us a little bit of time to process, but we give you a zip file that has all of that data.

Q2459 **Chair:** Does that data include not just your metadata—which we were talking about earlier on—from Facebook itself, based on your interactions and things you have done on Facebook? Would it also include data that Facebook has gathered about you by observing other sites that you have visited and other things you have done away from Facebook?

**Mike Schroepfer:** The DYI data is actually focused on a key desire that people have had. The basics of that functionality have existed since 2011, but GDPR makes front and centre the right to data portability—for someone to take their data somewhere else if they want to. That is at the heart of the focus of that product.

For information such as what you are talking about, it is also on the same screen, but it is about your ad information, which basically includes the interests we have derived based on that data. We can see that. Again, I gave you the examples earlier that I like coffee and I have cats, so I might be interested in topics related to those. That information, which is derived from a variety of sources, is visible right there in those tools.

Q2460 **Chair:** I can get that as well?



## HOUSE OF COMMONS

**Mike Schroepfer:** You can get that. I know that it is in the ads tools. I think it is part of the DYI tool. Those tools are constantly evolving. I am pretty sure it is in the big zip file.

Q2461 **Chair:** So your expectation is that I would get back not just the data that Facebook has about me based on what I do on Facebook, but also any other data that Facebook has picked up about me based on other things I have done online?

**Mike Schroepfer:** Yes, and the key thing there is that we are trying to show it as we use it. Ultimately, these things are processed in a variety of ways and we then build a set of interests. Those interests are the things that advertisers can use in order to advertise against. You may not have specifically written, "I am interested in cats"—you may have liked a page or visited a website and so on. That data, which we derive, is included in that.

Q2462 **Chair:** Okay. If I am not a Facebook customer, but Facebook has nevertheless built up data about me, as we were talking about earlier on, can I go to Facebook and ask for that data?

**Mike Schroepfer:** Again, because I don't know you and I don't have that data associated with you, I wouldn't know how to get that data. The information we have would be about devices and browsers. It is raw information. It is not, I believe, kept indefinitely. There is no way to get it because it is not associated with you.

Q2463 **Chair:** But if it is associated to a device?

**Mike Schroepfer:** Again, multiple people use devices, so it is not clear that all of that data— If you shared your device with someone, we may be giving their information to you. It is never associated. Again, all we have is device information. We don't know that it is you, so it is hard for us to honour a request for that data without possibly giving device data from someone else, because we can't authenticate it because it was never stored and related to your information.

Q2464 **Chair:** But if I wasn't a Facebook customer and I said to you, "This is my device. I want any data that you have linked to this device that you have gathered about me. It is my device—I own it and pay for it—and I want that data," your decision would be that you wouldn't give it to me because you couldn't be 100% certain that all that data was mine?

**Mike Schroepfer:** We don't currently give that data out, no.

Q2465 **Chair:** Is that being discussed with the data authorities? Would the ICO regard that as a reasonable position, or would they think that you should give that data back?

**Mike Schroepfer:** I haven't been involved in specific discussions on that, but I am sure our teams have.

Q2466 **Chair:** Certainly, since Mark Zuckerberg's testimony in Congress, there



## HOUSE OF COMMONS

has been some interest in the data that Facebook gathers on non-Facebook users. I therefore think there would be interest here, too, under the GDPR rules, in whether someone would have the right to get that data back. At the moment, it seems that, so far as Facebook is concerned, they wouldn't.

**Mike Schroepfer:** Again, you could say that it is your device, but since that data wasn't originally associated with you, I have no way to verify that it is actually your device. You could have grabbed my phone and said that that is the browser that you want the browsing history for from Facebook. There are challenging issues here, because the stored data is not associated with a person; it is associated with different devices and browsers.

Q2467 **Chair:** I am sure there would be a way of demonstrating that it was my device. I would be interested to know if that could be done, maybe with the co-operation of my mobile service provider, and if I could make a successful application on that basis. I am not saying that I will do that myself, but I feel pretty confident that there will be some test cases in that regard when the new rules come in.

**Mike Schroepfer:** Okay.

Q2468 **Chair:** Going back to some of the issues that we discussed earlier, if as a result of my time on Facebook I have shared some of my data with Facebook developers, through engaging with their tools, how can I get that data back if I choose to leave Facebook?

**Mike Schroepfer:** There are two parts to this. In addition to notifying people affected by Cambridge Analytica, we gave the same controls to everyone else on the platform—even if they were not affected—that show, front and centre, not only which applications they are currently using, but which they have used in the past. We also decided to sever connections from applications that they haven't used after 90 days. Maybe you tried out a game a while ago and haven't been using it. We just want to cut off access automatically, so that the developer cannot get new information on you, because the fact that you haven't used it is probably a good signal. Of course, if you go back to it, the data is still there; if you took a hiatus from Candy Crush and want to come back to it, we don't want half your data to be gone. But then if you wanted to leave it, there is an option in those settings to delete all of those. That removes the access of the developer to access information from you at Facebook. When that happens, we send an electronic signal to the developer, requesting that they delete the information associated with this user. That is generally what happens.

Q2469 **Chair:** Do you audit that, to make sure that the developers do that?

**Mike Schroepfer:** As part of our advanced process, we are working through all the developers and making sure that they are complying with all of our procedures, which includes data deletion from people on the platform.



## HOUSE OF COMMONS

**Q2470 Chair:** But other than sending them legal letters saying, “You’ve got to do this”—it would seem to me, from everything that has been said today, that you don’t have a system of randomised checking, or going to see developers to say, “Well, we’ve sent you several requests. We want to come and check that you have fulfilled what we asked you to do.”

**Mike Schroepfer:** We do talk to developers on a regular basis on a variety of these different issues, and if there are concerns or complaints, we will follow them up and deal with them.

The starting point for all of this is making sure that people understand what this is and trust it. Is this a random game they haven’t heard of, or a big brand such as Spotify? And making consumer choices about whether they are comfortable, because ultimately they are connecting their Facebook data with a third party from the very beginning, so there is an element of trust between the consumer and that brand, in terms of whether they trust that brand to be a good steward of their data.

We need to do everything we can to inform the consumer to police bad activity off the product, to follow up when we find these things and ideally to review these apps, as we have been talking about, before they go on, so that there are generally good actors on the platform.

**Q2471 Chair:** But I think that some people might also distinguish between different types of third parties they engage with. I might choose to leave Facebook but remain a Spotify customer. If I chose to leave Facebook, it might be unlikely that I am going to carry on playing FarmVille, or a game that has been designed specifically with Facebook users in mind. I understand that you can turn off the data pipe, so that with games or tools that I am not using any more the developer no longer gets my data, but the historical data they probably still have, and other than writing to them there doesn’t seem to be a mechanism by which Facebook can check that the data that has been requested to be destroyed has been destroyed.

**Mike Schroepfer:** Again, as part of the terms they are required to honour these requests. We send an electronic notice to them on a particular user when they remove it from the platform, to delete the data. Through all of this we are taking a much more expansive view of how we audit working with the developer, so I am assuming that this is part of what we will be looking at.

**Q2472 Chair:** But in 2011 there was a United States Federal Trade Commission ruling against Facebook, because of breaches of data privacy rules. As a consequence, was there not a requirement to have an audit every two years, looking at the relationship between Facebook and third-party developers in the use of data?

**Mike Schroepfer:** I believe so.

**Q2473 Chair:** So have those audits been undertaken?



**Mike Schroepfer:** I believe they have, yes.

Q2474 **Chair:** In that case, why didn't those audits pick up on, say, Aleksandr Kogan's work with Global Science Research?

**Mike Schroepfer:** Again, we didn't know at the time; no one caught the issue at the time.

Q2475 **Chair:** We didn't talk about this earlier on, but I think that ruling is significant, because that should have been a warning to the company about the seriousness of some of these issues, and while you said that people weren't across what Aleksandr Kogan was doing, there should have been a heightened level of awareness and concern about whether things like that were going on.

**Mike Schroepfer:** Again, we were looking at these issues all the time and not just with the FTC; the Irish data protection commissioner had gone through several technical audits. Reviews of the platform had made specific requests on a number of different dimensions, including making sure that we surfaced tools that we had built to allow me as a user to prevent any of my friends from taking my data to a third-party platform app; making sure those tools were front and centre. They were part of the new user flow and part of the product, to make sure those tools were there.

So, at the time we were operating in a mode where we were trying to make the controls clear to users, and trying to make it clear what data and app would access. Again, by the very fact of using this app, whether I transfer the data from Facebook or they give me a form and I type it in, I'm giving my data to this application.

So there is an element of trust between me and this brand that whichever method you use—because if they don't use Facebook, they'll just ask me for the relevant data they want; it just takes longer. You still have that trust with that brand. We're trying to make sure we're doing everything we can, again to get the bad people off and give people control, trust and understanding. Over time, as we evolved, the platform got bigger, Facebook had more users on it, and it became clear that we needed to have much more stringent access to a lot of these things.

Q2476 **Chair:** How much data does Facebook share with Governments, or get from Governments, about citizens?

**Mike Schroepfer:** I don't know that we do. We do research collaborations on aggregate data, but I do not know if we are doing that with Governments or not.

Q2477 **Chair:** But if I made a data request to Facebook, in the zip file you spoke about earlier on, would any Government information relating to me be included in that as well?

**Mike Schroepfer:** What Government information are you looking for, sir?



## HOUSE OF COMMONS

**Q2478 Chair:** The Government might have an interest in sharing data to work with companies to analyse social problems and social trends. Equally, I imagine if I had been party to a police investigation into a serious crime, you may have had a data request from the Home Office about that as well.

**Mike Schroepfer:** Obviously, we reply to lawful requests from law enforcement agencies in the UK and the US, and we publish a transparency report regularly on the volume of those requests for data.

**Q2479 Chair:** When I get my zip file, as you referred to earlier on, does Facebook keep a copy of that, or is that the only copy of that dataset, and therefore it no longer exists within Facebook?

**Mike Schroepfer:** That is basically a bundling up of information that we already have. We would retain that information, unless you choose to delete your account. Sometimes you may want to say, "I want my data, and I want to close my Facebook account." If you delete your account, we will delete all your data. I think our guarantee is by 90 days, and the only reason for that is that there is a large number of back-up systems and other systems. We have invested a lot of work in making sure that we diligently scrub your data from all the different systems. That takes a bit of time. We usually get it done faster than 90 days, but that is the commitment we make. Your data will be gone from our servers at that point.

**Q2480 Chair:** Just a couple of questions going back to political advertising. You spoke about the new tools that Facebook is developing whereby I will be able to see which advertisers place which ads and the campaigns that they have run, and their back history to some extent, as well as those adverts. Would it also include targeting data? Would I understand not just who the advertiser was and what other adverts they had run, but why they chose to advertise to me?

**Mike Schroepfer:** Yes, I believe that is what we are doing for political ads transparency specifically. For all ads we are going to show you all the ads being run by the advertiser. For consumer brand products there may be some competitive information that is sensitive for them, but for political ads we believe that getting more transparency is more important.

I believe among the things you'll see will be how much was spent on the ad, what audience they were trying to reach, and some basic information on how much it was viewed. An obvious question is whether an advert was seen one time or a million times. That is an important piece of data. Basically, we are trying to get all the information that we thought people would want to know, to ask important questions about who is advertising in an election and how it is impacting things.

**Q2481 Chair:** Facebook is removing the ability to edit link previews, I believe, for people's postings. Has that been in response to concerns about people editing link previews to distort the information contained through the



## HOUSE OF COMMONS

link?

**Mike Schroepfer:** I honestly do not know the answer to that question. If it is important I can try to find out and get back to you. I did not know that we were removing that feature.

Q2482 **Chair:** Over the past few months things have been written about it. I think the interest for us in it in particular is whether it is being done by the company in response to concerns about fake news operators seeking to edit link previews to make it more likely that someone will click through to the link, and maybe give a distorted impression of what the content is on the page as they go to it.

**Mike Schroepfer:** I see. I do not actually know if that is the cause of this. Again, forgive me if this is important information to you. I am now curious myself, so I will go and find out.

**Chair:** That is the reason for the interest anyway: whether that has been done in response to concerns raised within the company.

Q2483 **Jo Stevens:** I want to ask you about some activity overseas, but first, going back to what we were discussing about Aleksandr Kogan and Joseph Chancellor, just so that I am absolutely clear, you told us that Facebook were only aware that Joseph Chancellor worked with GSR last year—2017.

**Mike Schroepfer:** Again, in the recruiting process the recruiter and the people hiring him probably saw a CV and may have known he was part of GSR; so, had someone known that? Had we connected all the dots to when this thing happened with Mr Kogan later on? Had he been mentioned in the documents that we signed with Kogan and party—no. So is it possible that someone knew about this and the right people in the organisation didn't know about it? That is possible.

Q2484 **Jo Stevens:** So the answer to my question: is 2017 correct or not? That is what you told me earlier.

**Mike Schroepfer:** That is when the people involved in this investigation—our legal team—started to understand this association. I think prior to that a recruiter might have known, who was recruiting Mr Chancellor at the time, but I don't know that they sent over that information to legal, because this predates any of the knowledge on the issues with recruiting.

Q2485 **Jo Stevens:** We have evidence that shows that Facebook knew in November 2016 that Joseph Chancellor had formed the company GSR with Aleksandr Kogan, which obviously then went on to provide the information to Cambridge Analytica. I am very unclear as to why Facebook have taken such a very direct and critical line, as the Chair said earlier, with Aleksandr Kogan, but have completely ignored Joseph Chancellor, who I think is still working for you.



## HOUSE OF COMMONS

**Mike Schroepfer:** I understand your concern. We are investigating Mr Chancellor's role in this right now.

Q2486 **Jo Stevens:** But he is still working for you.

**Mike Schroepfer:** There is an employment investigation going on right now.

Q2487 **Jo Stevens:** But he is still employed by you.

**Mike Schroepfer:** Because we are dealing with an employment legal matter at this point I would prefer not to go into more detail, but we are investigating his association with us right now.

Q2488 **Jo Stevens:** Okay, so you are undertaking an investigation. What sort of work is he doing at the moment, then?

**Mike Schroepfer:** Immediately, right now, I don't know what he is doing. As I said before, I believe he works on virtual reality, and some other things like that. The thing I do know is he hasn't worked on the platform.

Q2489 **Jo Stevens:** So this is a man who is a director of a company that has been involved in this data breach—in a situation where you have insisted on an NDA with Dr Kogan—and you have publicly criticised it, calling it a fraud and a scam, I think, but you don't know what Joseph Chancellor, who was a director of the same company, is currently doing in Facebook.

**Mike Schroepfer:** Again, he is under investigation, to understand his role in all of this. Again, some people, like recruiting and others, may have known about his association with GSR. He was recruited prior to all of this happening with Mr Kogan. It didn't reach the employment law and people investigating these other issues, to my knowledge, until 2017. I learned about much of this very recently, so that is the full situation.

Q2490 **Jo Stevens:** I wanted to ask you about Myanmar. I was interested in this Free Basics tool that you have, which you are using in developing countries, as I understand it so that people can access various services on their mobile phones without data charges—and Facebook plays a huge part in that. You are doing that. In Myanmar—I just should let you know, I went to Bangladesh and the border with Myanmar last November, to the refugee camps for the Rohingya who have fled Myanmar—the United Nations have accused Facebook of playing a determining role in stirring up hatred against the Rohingya in Myanmar. I am quoting from what they have said. "It has...substantively contributed to the level of acrimony and dissention and conflict...within the public." Social media has been exploited to spread hate speech and just last month UN officials said that your platform had morphed into a "beast" that helped spread vitriol against Rohingya Muslims. Are Facebook reviewing how they are operating in Myanmar?

**Mike Schroepfer:** Absolutely. The situation in Myanmar is awful. On a personal level, when I am not working, one of the causes I spend my



time on is refugees, because I think the idea that someone is displaced from their home for reasons outside their control, because of what they believe in, or because of war, is just awful. As I said, the platform is one of free expression. In regions like this where there is hate or dehumanisation on a platform, the real challenge on the ground that we need to be doing more on is getting more people with local knowledge of all the different dialects and understanding of the cultural sensitivities. They understand the line in terms of, "In this culture, this is a dehumanising comment that should not be getting on the platform." We need more policy people on the ground to get better meetings with NGOs and others. I know our teams were briefed last week—many of our NGOs on the ground. We are briefing them again next week to talk about all the different things we are doing. I want to be clear: what is happening here is awful and we need to and are trying to do a lot more to get hate speech and all this kind of vile content off the platform.

**Q2491 Jo Stevens:** When did you start doing that work? Obviously the atrocities have been going on for more than a year.

**Mike Schroepfer:** I do not know exactly. We have been working in Myanmar for a long time. We have had people on the ground for a long time. I do not know exactly when we have decided to amp up or increase dramatically the presence of people on the ground. We also have dedicated product teams in the engineering ranks to see whether there are product changes we can make to make those products better. There are some challenges on a technical level. For example, there is a dialect that people use there that we do not have very good language data on. It is not Burmese. We may have to switch some of the product to change how that works. We have quite good tools in English and a couple of other languages that are evolving to help automatically detect such things as hate speech.

**Q2492 Jo Stevens:** How long does it take between a report being made to you and you responding to that reported issue using the tools that you have got?

**Mike Schroepfer:** We say in our community standards that we attempt to respond within 24 to 48 hours. I would guess that that varies from region to region. I think in this region the key is to ensure that we have people who can not only respond quickly, but respond adequately and really understand the local issues. To complete my point on the technical work, I am also trying to understand how we can translate into Burmese the work we have done in English for machine learning. That gets you an immediate reaction. As you try to post something, we would be able to catch it immediately. Once I am out of here—when I am not with you, I am going to spend my time working on those sorts of things.

**Q2493 Jo Stevens:** If you could let us know what the average time is so far for responding to reported issues, that would be very helpful. Do you know how many fake accounts have been identified and removed in Myanmar?



## HOUSE OF COMMONS

**Mike Schroepfer:** In Myanmar specifically, I do not know that specific number offhand.

Q2494 **Jo Stevens:** Would you be able to let us know?

**Mike Schroepfer:** I will see what data we have.

Q2495 **Jo Stevens:** Thank you. How much of your revenue is derived from Myanmar, as a company?

**Mike Schroepfer:** I do not know that number off the top of my head either. I would guess it is small.

Q2496 **Jo Stevens:** If you could let us know that as well, that would be really helpful.

**Mike Schroepfer:** I'll see what we have.

**Jo Stevens:** Thank you.

Q2497 **Chair:** Just one or two final questions, then I think we are done. I want to ask for clarification on one of the questions linked to AIQ. You mentioned the work that Facebook has done looking at the—I think when we were discussing the overlap between Cambridge Analytica's work and AIQ's work, you said that about 30,000 to 40,000 data profiles had come from Aleksandr Kogan's surveys, which had become mixed into the datasets that AIQ had. I think that was—

**Mike Schroepfer:** No, that is not—excuse me, Chairman, but I want to correct what I said there. AIQ ran a series of ad campaigns. They used email lists. They would upload a hash list of emails to us and say, "I would like to show this ad campaign to this group of people." What we looked for was overlap. Again, because Mr Kogan did not get emails, they certainly did not get the emails from him. They at least sourced data from somewhere else. We then looked at the overlaps. Of all those campaigns that people had run, of the people who installed Mr Kogan's app—we looked at the intersection between those two. If it was 0%, I could say with 100% scientific certainty that that was unlikely to be involved. It was a 3% to 4% overlap. I do not know the absolute number; I just know the relative overlap. If you picked another app that was installed as frequently as Mr Kogan's and compared that user base against one of these ad campaigns, you would get a 3% or 4% overlap. That is why I say that we are more certain than not that any overlap there is effectively random chance. It is not that that data was sourced and used here.

Q2498 **Chair:** We have a figure of about 30,000 to 40,000 users that the overlap represents—that would be the number. Based on Facebook's own numbers, we know that there is a total audience of about 1 million people in the UK whose data could have been gathered by Aleksandr Kogan as a consequence of people engaging with his app. That is the total of Facebook users who took the survey and their friends. The audience of that is about 1 million people. That is how we got to the 30,000 to



## HOUSE OF COMMONS

40,000 sample base that could be in that overlap.

Does Facebook know whether that is just, as you say, random chance—what would be statistically expected—and not planned, or was it a defined audience that AIQ had created? Was there a custom audience that they created and uploaded to Facebook that is based on that overlap and that sample? A sample of that size, even though it is a small percentage, would be equivalent to the base set of data profiles that Brittany Kaiser spoke to us about last week—saying that your training set would be a sample set of about 40,000 people.

**Mike Schroepfer:** A 3% to 4% overlap would be highly—again, if you just threw a dart at a dartboard full of apps that were installed and of a significant size, and picked that one, you would get a similar overlap. That to me makes it statistically very unlikely that this is that dataset. I would expect that if they were using or had this dataset, or some fraction of it—I do not know why if they had some of it they would not just have all of it.

There is also some confusing testimony here because Mr Kogan said on Tuesday that he did not give any UK data. It was only US data, if I remember correctly, but this was targeted at UK users. Again, I think we are just trying to connect all the dots to all these things.

Based on the analysis that we have done of the data, it is my assessment that it is highly unlikely that these datasets were using Mr Kogan's. I would expect a much greater overlap if that were the case.

Q2499 **Chair:** Okay. I would be grateful if you could provide this information to the Committee: if there were custom audiences created by AIQ that were uploaded on to Facebook as part of their work during the campaign, whether it is likely that any of those audience members were people who had taken Aleksandr Kogan's survey.

**Mike Schroepfer:** Sure, yes. I think we have more detailed analysis on that, which we have shared with the relevant parties that are doing the investigations.

Q2500 **Chair:** Outside Aleksandr Kogan's survey work, have you seen evidence that SCL or Cambridge Analytica shared data with AIQ to support their work during the campaign—from other sources?

**Mike Schroepfer:** I don't know. What we do know, as I said in the written testimony, as we covered earlier, there are overlapping people between those two companies and some business and billing contacts that imply that there is a relationship there. Again, because Cambridge Analytica did not advertise in the Brexit campaign, it is not clear whether they had shared data of any form, whether from us or others, with AggregateIQ. It is hard to know without getting into both those companies and asking them those questions, which is why we are happy to work with the ICO and others who are actually onsite in those locations to get answers to those questions.



HOUSE OF COMMONS

**Chair:** I think, Mr Schroepfer, that concludes our questioning this afternoon. Thank you very much for joining us and for your time.