Digital, Culture, Media and Sport Committee
House of Commons, London SW1A 0AA
Tel 020 7219 6120 website www.parliament.uk/cms

Rebecca Stimson
Head of Public Policy
Facebook UK
1 Rathbone Place
London W1T 1FB

21 May 2018

Dear Ms Stimson

Oral evidence from Facebook

Thank you for your letter of 14 May.

As I said in my statement last week, many of Facebook's answers do not include sufficient detail or data evidence. This lack of transparency is disappointing.

Please see the specific points on which further information is required in the attached document.

If Facebook truly recognises the 'seriousness' of these issues as it says it does, we would expect that Mark Zuckerberg would want to appear in front of the Committee and answer questions that are of concern not only to the UK Parliament, but Facebook's tens of millions of users in this country. We re-state our willingness to do this by video link, if that would be the only way workable solution.

We request a response by Monday 4 June.

Kind regards,

DAMIAN COLLINS MP

CHAIR, DCMS COMMITTEE

21 May 2018

DCMS Committee's response to the 14 May 2018 Facebook letter (in blue)

1. What is the percentage of sites on the internet on which Facebook tracks users?

Facebook provides a number of different tools that third parties, such as website owners and publishers, can choose to integrate into their services. These technologies have a range of purposes: Facebook social plugins, such as the Like button and Share button, enrich users' experience of Facebook by allowing them to see what their Facebook friends have liked, shared, or commented on across the Web. Facebook also offers the Facebook Pixel, which allows third parties to understand how people are engaging with their content and better reach people who use or might be interested in their products and services.
We receive information when a site or app that use these Facebook technologies is visited. Specifically, our servers log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of lnternet design); and (ii) any additional information the publisher of the app or website chooses to share with Face book about the person's activities on that site (such as the fact that a purchase was made on the site).
(See https://www.facebook.com/policies/cookies). Facebook requires third parties using these technologies to do so in accordance with all applicable laws including, where applicable, obtaining appropriate valid consent from the end user.

As explained by Mr Schroepfer (Q2103), many companies offer these types of services and, like Facebook, they also get information from the apps and sites that use them. He explained, for example, that Parliament's website www.parliament.uk collects and shares browser and cookie information with six different companies- Google, Linkedin, Twitter, Hotjar, Pingdom and Facebook- so when a person visits Parliament's website, it sends information about their visit to each one of those third parties. Twitter, Pinterest and Linkedin all have similar Like and Share buttons to help people share things on their services. Google has a popular analytics service. And Amazon, Google and Twitter all offer login features. These companies - and many others - also offer advertising services. In fact, most websites and apps send the same information to multiple companies each time you visit them.
Between 9 April and 16 April 2018, the Facebook Like button appeared on 8.4M websites, the Share button appeared on 93 UK websites, and there were 2.2M Facebook Pixels installed on websites. We do not know the total number of websites in the world in order to express this as a percentage.

You state that "Facebook requires third parties using these technologies to do so in accordance with all applicable laws including, where applicable, obtaining appropriate valid consent from the end user". Why is the onus on smaller operators, with limited budgets, to comply with data legislation? Why shouldn't the onus be on Facebook to check this?

You state that the Facebook like button appears on 8.4m websites. Yet according to Similar Tech, a web marketing and research firm, Facebook Connect is used by 16,406,599 websites. Even accounting for sites using Facebook Connect without using Facebook's Like button, how do you explain this discrepancy?

2. Did the Internet Research Agency use custom audiences? What targeting tools did the IRA use for their advertising? Did they have a custom audience for state-by-state campaigns/races in the USA? Did they use look-alike audiences from Facebook as part of their advertising spend?

The vast majority of lnternet Research Agency adverts did not use custom audiences to target the ads we identified that were run in the United States between June 2015 and August 2017. In the limited cases when it did run ads using custom audiences in its targeting, the IRA used either a Website Custom Audience or Lookalikes. The former enables advertisers to target people on Facebook that have visited their website, through use of the Facebook pixel. The Lookalike audience tool enables advertisers to reach new people on Facebook who are similar to members of an existing audience. In addition, we found that the IRA did not use Data File Custom Audiences (DFCAs), which is the only type of custom audience that is created based on data provided by the advertiser. Advertisers create DCF by uploading a data file with a list of people for whom they have contact information, such as email addresses and phone numbers. Once the file is uploaded, the data is hashed (to safeguard the privacy of the people involved). Facebook then uses the hashed data to find matches with Facebook users to create the audience.

From which websites was Facebook pixel data used by the Russians in their website custom audiences, used to target their advertising at Facebook users in America?

3. What is Facebook's definition of a political advertisement? What budget does Facebook put behind examining the parameters and use of political adverts?

The precise definition of what constitutes a political advert will vary by location reflecting local laws and regulations. In the UK, the Electoral Commission provides relevant guidance (for example, regarding what constitutes campaigning in a referendum, and what constitutes political campaigning). As part of preparing to roll out our political advert transparency measures in the UK we will be working with the Commission (together with other relevant UK stakeholders and experts) to develop appropriate definitions for the UK.
Our advert transparency measures are aimed at identifying both adverts placed by or on behalf of a politician or candidate, as well as adverts aimed at influencing opinion on political issues. As confirmed to the Committee by Mr Schroepfer, our intention is for Facebook's new transparency measures to be in place in the UK in time for the UK local elections in 2019, if not before.
A key stage of our transparency efforts - the view ads tool - will become available in the UK in June of this year. This will enable people in the UK to see all of the ads every advertiser is running on Facebook at the same time.
In time for the local elections in May 2019, we will require those seeking to run political adverts to complete an authorization process to help ensure ads are coming from authentic accounts and when they run they will be required to display who paid for them. They will be placed in a searchable archive that would include the ads themselves and certain information about them (such as how many times an ad may have been seen, how much money was spent on them, and what kinds of people saw them).
Our teams are dedicating considerable time, effort and resources to addressing advertising transparency, particularly with respect to political adverts. While there is no single budget figure, this is a critical engineering and business priority and teams from across our companies have and will continue to tackle these issues with urgency.

In response to the question of how much budget Facebook spends on examining the parameters and use of political adverts, you replied: "While there is no single budget figure, this is a critical engineering and business priority and teams from across our companies have and will continue to tackle these issues with urgency." This answer is what both

Christopher Wylie and Chris Vickery have called "weasel words", and has told the Committee nothing. Please answer the question.

4. How many developers did your enforcement team at Facebook take action against between 2011-2014?

Facebook replied: "Due to system changes, we do not have records for the time-period before 2014 that establish we terminated for developer violations. However, we regularly taken action against app. For example, in 2017, we took action against about 370,000 apps, ranging from imposing restrictions on certain features to removal of the app from the platform. And beginning in 2014, Facebook proactively reviewed all new apps seeking to access anything beyond basic data fields and has rejected more than half of apps (about 299,000 apps in total) seeking those permissions".

Do you really have no records of developer violations for the time-period before 2014? If you don't have records, would you agree that that is a serious omission?

The large figures quoted (about 299,000 apps in total) would also include spam. We would like a specific answer to the number of actions taken against data violations, in accordance with Section 3 of the Facebook Platform Policies.

5. Does the NDA signed with Dr Kogan prevent legal action being taken? What was the date of the agreement? Was there a payment made to Dr Kogan?

Facebook replied: As stated by Mr Schroepfer (Q 2322), a formal agreement was signed by Dr Kogan on 24 June 2016 in respect of his obligations to delete Facebook user data and obtain certifications from other third-parties to whom he provided some data (SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto). A copy of the agreement is enclosed. This agreement with Dr Kogan contained a standard confidentiality clause. No payment was made by any party in connection with the agreement. As Mr Schroepfer also explained, we want Dr Kogan to be able to be open about these events and have waived this confidentiality obligation.

Why was the NDA signed on 24 June 2016, over 18 months after Facebook was first made aware of the data harvesting carried out by GSR? Why was it signed on the result day of the UK Referendum?

Why did the NDA cover data only? If you were attempting to be thorough, why did the NDA not cover derivatives or models?

Does the NDA prevent legal action being taken?

Who, from Facebook, signed the NDA? We would like to know who signed it, so that we are aware of who, on Facebook's senior management team, knew about the data harvesting. Did you deliberately hide the signature when you sent us a copy of the NDA?

6. Who was the person at Facebook responsible for the decision not to tell users affected in 2015?

The information that surfaced in December 2015 reported that Dr. Kogan may have shared data

that he obtained lawfully from users on Facebook's platform with a third party (Cambridge Analytica) in violation of our developer policies. Dr. Kogan's violation of our policies did not trigger a legal notification obligation by Facebook, both because the data shared with Dr. Kogan's app was authorized by users and because of the nature of the information itselfconsisting of information people shared publicly or with their friends on Facebook (generally not passwords, financial data, or other data requiring notification under laws in place at the time). Accordingly, our focus in December 2015 was to ensure that Dr Kogan and anyone with whom he had shared data promptly deleted all data. We retained an outside law firm to investigate and take action against Dr Kogan. We obtained certifications from Dr Kogan and others he shared data with assuring us that all variants of the data had been deleted. We also promptly removed Dr Kogan's app from the Facebook platform. An audit of Cambridge Analytica and the other parties involved would likely be the most effective way of seeking to determine what data was in fact shared and whether it was deleted at the time.
Because we are taking a broader view of our responsibilities that go beyond our legal obligations, we have since notified all people potentially impacted with a detailed notice at the top of their News Feed. In doing so, we have likely notified many people who did not have their data passed to Cambridge Analytica. Not only did we take an expansive methodology to identify users whose information may have been shared with Dr Kogan's app, but we also notified all potentially affected users outside the United States, despite Dr Kogan's statements - including to the Committee - that he only passed information relating to US users to Cambridge Analytica.

To repeat the question, who was the person at Facebook responsible for the decision not to tell users affected in 2015?

We have received a lot of evidence that would show that Facebook was aware of the data harvesting by GSR prior to December 2015.

7. Who at Facebook heads up the investigation into Cambridge Analytica, including all the strands of the investigation?

Our legal team, led by General Counsel Colin Stretch, is leading the investigation into Cambridge Analytica.

8. Has Joseph Chancellor signed an NDA?

As stated by Mr Schroepfer (Qs 2192-2194), Joseph Chancellor has not signed a non-disclosure agreement with Facebook relating to this issue. All employees of Facebook (as with many businesses) are required to sign a standard confidentiality agreement as part of their employment, and Mr Chancellor is no exception.

Is Joseph Chancellor's confidentially agreement retroactive, covering the period before his employment? If it is, would you release him from that restriction?

9. Agreement to provide documentation that Cambridge Analytica had certified the deletion of the data.

A copy of the certifications from those to whom Dr Kogan said he gave the data are enclosed.

10. What was the number of paid adverts from the IRA during the US election?

After the 2016 US election, we found that fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram adverts between June 2015 and August 201 7. All adverts have been published by the US House of Representatives and are available here: https ://democrats-intelligence.house.gov /face book-ads/ social-mediaadvertisements.htm.

We asked for these adverts months ago. Why did you not provide this information when we asked for it? Why did you give this information to Congress, but not to Parliament?

Was there any US or Russia data overlap?

11. From which country did the $2 million that AIQ spent on ads come?

According to its advertiser registration, AIQ was based in Canada. However, in order to run adverts on behalf of Vote Leave and other UK referendum campaigners, AIQ would have required access to be granted to their Facebook pages by the respective campaigns. In other words, the VoteLeave and other campaigns explicitly granted access to AIQ to be an administrator of their pages.
From our internal investigation so far, to run adverts on Facebook, AIQ incurred approximately $1.6 million USD to run adverts from the Vote Leave Facebook Page; approximately $329,000 USD to run adverts from the BeLeave Facebook Page; approximately $51,500 USD to run adverts from the Veterans for Britain Facebook Page; and approximately $32,700 USD to run adverts from the DUP Vote to Leave Face book Page.

You have not answered the question. To repeat, from which country did the $2 million that AIG spent on ads come?

12. How many UK Facebook users and Instagram users were contacted by non-UK entities during the EU referendum?

Many Facebook and Instagram users are frequently in contact with friends and family in other countries, and may read foreign media, or may follow celebrities or public figures abroad. Many referendum campaigners have at some point used foreign consulting or advertising agencies. Our understanding is that all registered campaigners need to report details of their suppliers during the referendum period to the Electoral Commission. The Electoral Commission then publishes these suppliers' details on the public register available on its website.
Regarding alleged coordinated foreign activity during the EU Referendum, we have previously addressed the Committee's questions on Russian interference (in our letters of 17 January and 28 February 2018). We found a few adverts connected to the IRA which ran during the regulated period of the EU Referendum campaign - 15 April to 23 June 2016 - that were shown to a small number of people in the UK. As requested by the Electoral Commission we shared information about how much was spent by the IRA to reach UK voters during this period. This amounted to around 1 USD. We also provided copies of the Adverts to the Electoral Commission.
The release of the set of IRA adverts by the US House of Representatives, which shows a significant amount of activity by the IRA with only a handful of their adverts listing the UK as a possible audience, confirms the position we shared with the Electoral Commission and the Committee.

To repeat the question, how many UK Facebook users and Instagram users were contacted by non-UK entities during the EU referendum?

According to evidence that Facebook submitted to Congress, and now released publicly, Russian anti-immigrant ads were placed in Oct 2015 targeting the UK (as well as Germany and France). These amounted to 5,514.85 roubles. Yet you told us that there was only $1 of spend during the regulated period of the referendum by the Internet Research Agency. Why the discrepancy?

Could you tell us the total amount of political advertising paid for by Russian agencies targeting Facebook users in the UK since October 2015, to date?

13. How many clicks or swipes does it take to alter your Facebook privacy settings on a smartphone? What steps are you taking to reduce the lengthy process of changing one's privacy settings?

We have recently rolled out changes to our settings. To access Privacy Settings in our updated menu, it only takes three clicks. First, users click on the three bars at the bottom of the app. Then, they click on "Settings & Privacy." Finally, they can click on either "Settings" to access the full suite of core Facebook settings, including privacy, or they can go straight to the "Privacy Shortcuts" menu to access core privacy settings.

During our preparations for GDPR, we heard feedback from regulators, policymakers, and users that-- while it's important we offer many granular privacy settings-they are too distributed across the platform and should be centralised in one place. We took this feedback on board and, following a significant engineering and design effort, we also created an updated Settings menu where users have easy access to all the core Facebook settings in one place. Now, instead of having settings spread across 20 different places on Facebook, users can go to one place. The updated menu is now clearer, more visual and easier to find. From this one place, users can now make their account more secure, control their information, control the ads they see, and manage who sees their posts and profile information.

14. What proportion of political campaigning ads globally are run on your platform? Do you have a rough estimate, based on average political campaign spend data?

We are not aware of any data on total political advertising spend globally - whether online or otherwise - which would be required in order to estimate what proportion of that advertising is placed on Face book, nor do we have a reliable way today to know what adverts previously run on our platform are "political". As Mr Schroepfer stated (Qs 2262-2263), Facebook does not monitor market share of political advertising or have the means to do so.

Why do you not know which adverts previously run on your platform are political? What steps, if any, are you taking to remedy that?

You say you have no figure for global spend on political campaign ads, so cannot estimate your market share. What is the annual spend on Facebook, globally, for political campaign ads, and issues-based influence campaigns?

15. What data on dark ads do you have?

We understand dark ads to refer to adverts that an advertiser targets to a specific audience but that are not otherwise viewable on Facebook (outside the audience for the adverts).
In general, Facebook maintains for paid advertisers data such as name, address, and banking details. We also maintain information about advertiser's accounts on the Facebook platform and

information about their ad campaigns (most advertising content, run dates, spend, etc.). Advertisers do not however obtain information from Facebook which personally identifies recipients of their ads.
We believe that the Committee's concerns will be addressed by the new feature which we've been testing in Canada called "view ads". This is a key step in our commitment to advert transparency, and lets anyone see all the adverts a Page is running on Facebook- even if they are not in the audience for the advert and even if the user does not follow the Page running the adverts. This will apply to all advertiser Pages on Facebook - not just Pages running political adverts. We plan to launch "view ads" globally in late June of this year.
Users are also always able to see who is showing them adverts and how they are being targeted, including by clicking the drop-down menu available in any advert and selecting "Why am I seeing this?". This tells the user who the advertiser is and provides them with an explanation of how he or she has matched the advertiser's targeting criteria. If users do not wish to see further adverts from the advertiser concerned, they can then choose "Hide ad". Users can also "Report Ad" from this drop-down menu, including because the user considers the advert to be misleading or a false news story. Through this drop-down they are also directed to their Ad Preferences and Ad Settings where they can see and amend the interests on which advertisers can target them; see and amend the advertisers that are able to target them as a result of previous interactions; and opt out of receiving adverts based on data from third-party partners.

Rather than giving us a definition of dark ads, and how Facebook is attempting to reduce the impact of dark ads, can you tell us what data on dark ads you have?

You say you maintain the address and banking details of every Facebook advertiser. Why then when you've previously submitted evidence regarding adverts from Russia have you used as your criterion adverts paid in roubles?

The feature "view ads" sounds as though a user could not see all the ads from the page of a bad actor without having either been targeted by that actor, or being aware of the page. Is this the case? Would you explain in detail how "view ads" works?

You say that 'In general, Facebook maintains for paid advertisers data such as name, address, and banking details,' but could there be campaigns where this information has not been retained by Facebook?

16. Is it possible for Facebook to view pages set up during elections (e.g. the EU Referendum campaign) that host dark ads, and then are taken down a day later? Is it possible that no-one would ever be able to audit these dark ads, as no one (not even Facebook) would see them during the time they are online?

We refer you to our answer to question 15 above regarding the information we retain in relation to adverts and advertisers on our platform, including when the underlying Page is deleted.
We are also working to further increase ads transparency specifically around political advertising. Advertisers running advertisements for political adverts on Facebook and Instagram will be required to be authenticated before they can run political adverts. In addition, political adverts will be accompanied by "paid for by" information. We will also release a public, searchable archive of adverts with political content, which will include adverts that are deleted or run for a short time. We are working to roll this out in the UK before the local elections in May 2019.
It is important to note that the systems that will identify electoral and issue adverts subject to our new ads transparency policies are in the process of being developed and will not be perfect. We are invested in continuing to develop and refine these systems as fast as we can to improve accuracy in identifying ads subject to these requirements.

Rather than concentrating on your current work to increase ad transparency, can you answer whether it is possible for Facebook to view pages set up during elections that host dark ads, and then are taken down a day later? Can you audit these dark ads?

Does Facebook have the ability to audit ads that have been removed from the platform, ie when the content has been deleted?

17. Was there any link between the US elections and the 2017 purge of fake accounts?

The 2017 purge of fake accounts that was referenced by the Committee (Qs 2288 - 2297) relates to steps we took to disrupt a specific spam operation (see https://www.facebook.com/notes/facebook-security/disrupting-a-major-spamoperation/10154327278540766). The operation was made up of inauthentic likes and comments that appeared to come from accounts located in Bangladesh, Indonesia, Saudi Arabia, and a number of other countries. We are not aware of a connection to the 2016 US elections.

You mention "a number of other countries". Which other countries?

18. What proportion of the fake accounts you purged had any involvement from Russia?

We are not aware of links between the spam operation referenced in Q 17 and the Russian government.
Outside of the 2017 "purge", in our review of the 2016 US election we found that the Russian Internet Research Agency had set up a network of hundreds of fake accounts to spread divisive content and interfere in the US presidential election. We began investigating their activity globally and taking down their Pages and accounts. In Autumn 2017, we removed 4 70 fake IRA accounts and Pages. In April 2018, we removed more than 270 further accounts and Pages operated by the Internet Research Agency.

19. Do you know how many developers were using and selling data on to third parties such as GSR? Is GSR the only company that has received letters from Facebook, demanding that they delete their Facebook data?

To clarify, GSR is a company established by Dr Kogan - the developer of the thisisyourdigitallife app. We understand that Dr Kogan/GSR transferred data at some point to third-parties that include Christopher Wylie (and his company) and Cambridge Analytica/SCL Elections. We obtained certifications of deletion from each of those third parties.
We are in the process of investigating every app that had access to a large amount of information before we changed our platform in 2014. If we find suspicious activity, we will take steps to investigate or take enforcement actions against the app. If we determine that there has been an improper use of data shared with third parties, we will ban those developers and notify everyone affected.

How can you be investigating every app that had access to large amounts of information pre 2014, when in Q4 you said that you did not have data on apps terminated before 2014, due to system change? Also, to repeat the question, how many apps had access to large amounts of data? Also, how do you define "a large amount of data"—is it by number of accounts accessed, number of API requests, or some other measure?

When did your investigation begin? (Last year, Facebook announced that it had paid $9.5 billion to Facebook developers, so developers are a constituent part of Facebook's structure).

20. What kind of developer activity leading up to 2014 led to Facebook's major policy changes related to sharing friends' data? (Please give specific examples.) Were these changes responding to genuine concerns among Facebook users?

In early 2014, Facebook introduced changes to provide users more choice and control over what information apps received, to reduce the amount of data that could be shared with third-party apps, and to establish a new review and approval process for any new apps that sought to request anything more than basic information about the installing user. We announced these changes because, among other things, we learned that consumers wanted more control over their information. These changes accompanied a new version of the platform API, called Graph API V2, which incorporated several key new elements. The changes included:
• Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorised the same app;
• Limiting the data that apps on the new platform could access about friends of the installing user; and
• Providing users with even more granular controls over the categories of their data an app operating on the new platform could access.
We are in the process of restricting the data available to apps even more severely, so that the only data that an app will be able to request without App Review will be name, profile photo, and email address.

You mention consumer demand, but you do not comment on developer activity. To repeat the question, what kind of developer activity leading up to 2014 led to Facebook's major policy changes related to the sharing of friends' data?

Were developers able to access large amounts of data about users, without having their app reviewed? How many developers had this kind of access? Have users ever been explicitly notified that their data has been harvested, en masse?

21. How many Facebook staff have been added to the app review team since 2014?

Facebook wrote: We work continuously to make our platform safer and more secure, and our effort to do so is a holistic one that often involves hiring additional employees as well as continually evaluating our processes and policies. Facebook has several groups dedicated to detecting, investigating and combating violations of its policies. Those efforts have expanded and evolved over time. For example:

• Our Developer Operations team reviews Facebook apps requesting detailed personal information for policy violations. The Developer Operations Policy Enforcement team looks for policy violations and either brings developers into compliance or removes them from the platform. The Developer Operations Review team conducts an upfront review of apps to confirm proper use of advanced permissions.

• Our Security teams make sure the worst actors and abusers are dissuaded from targeting

our products, communities, and company. The teams also stay abreast of trends in attacks and are composed of investigators, analysts, and security engineers.

• Our Platform Integrity team builds systems and automation to detect and enforce misbehaving platform applications, with a focus on commercial spam. The team detects and fixes Developer Platform security gaps, and redesigns platform products to make them harder for bad actors to abuse.

We have and will continue to add more people and resources to our Developer Operations team, as well as other teams that work on privacy, safety, and security at Facebook. This year we are doubling the number of people who work on safety issues overall from 10,000 to 20,000, and that includes content reviewers, systems engineers and security experts. We are on track to hit this goal.

You quote the thousands of staff who work on security issues, but you have not given us a figure of the amount of staff who work on the platform team. Please can you send us that precise figure, which we originally asked for.

22. What is the legal situation regarding Facebook storing non-Facebook users' data?

When a person who is not a registered user of Face book visits a site or app that uses our services and accepts the use of Facebook cookies (or similar technologies), we receive logs of this visit in the same manner described in response to question 1 above. This is an inherent feature of how the Internet works and occurs automatically by virtue of the fact that the person's device contacts Facebook's servers in order for the Facebook buttons and other features on those sites to work. The information received in this manner allows Facebook to identify a specific browser; however, when the person visiting the website or app is not a Facebook user, we do not receive any information that would allow us to identify the individual using that browser. Facebook's processing of such data for non-users complies with all applicable laws. Our privacy policy (https://www.facebook.com/policy.php) explains in detail what we do with the information we receive, and makes clear that we may collect data from people away from Facebook who are logged out or don't have a Facebook account. Our Cookies Policy (https://www.facebook.com/policies/cookies/) provides more detailed information about how and why we use cookies and the controls that people have. And we comply with applicable EU laws by obtaining consent from European users before dropping cookies that are not strictly necessary by displaying a cookie banner to every browser visiting Facebook for the first time to notify users about our cookie use as follows: *"To help personalise content, tailor and measure ads and provide a safer experience, we use cookies. By clicking on or navigating the site, you agree to allow us to collect information on and off Facebook through cookies. Learn more, including about available controls: Cookie Policy.* "
In order for third parties to use our Facebook technologies in their websites or apps, it is also a contractual requirement that they do so in accordance with applicable laws and that where necessary they obtain valid consent or have another legal basis to share browser or app logs with Facebook from their service.

Do non-Facebook users explicitly grant permission for the use of Facebook cookies on non-Facebook websites, or is this implied, or is Facebook not mentioned directly at all?

To say that "this is an inherent feature of how the Internet works" is disingenuous, as it is a part of how Facebook's web tracking and web features work, but Facebook is not the Internet, nor is the Web the Internet. Please comment on this point.

The process by which a user might learn about Facebook's tracking, their privacy policy, etc., is far from explicit, and is in fact hidden. Please comment on this point.

How is Facebook defining "valid consent"?

23. Did Facebook pass user information to Cambridge Analytica or to Aleksandr Kogan?

No, Facebook did not pass user information gathered by Dr Kogan's app to Cambridge Analytica. As Mr Schroepfer explained to the Committee (Q 2389), Facebook provided tools that let users share their data and their friends' data with Dr Kogan's app, and Dr Kogan in turn appears to have shared some of that data with Cambridge Analytica and other third parties.

Facebook passed the data of users to Kogan without their permission, by allowing individuals to grant data access to their friends' data. Please comment on this point.

24. At the 8 February evidence session, Chris Matheson asked Simon Milner, "Have you ever passed any user information over to Cambridge Analytic a or any of its associated companies?" Simon Milner replied "No". Chris Matheson asked, "But they do hold a large chunk of Facebook's user data, don't they?" Simon Milner said, "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." [Qq 447-448] Do you agree with this answer?

This question was answered in Mr Schroepfer's evidence to the Committee (Q2407-2419, Q2429-2430). Additionally, we should point out that the quotation contained in this question is an incomplete representation of the evidence that Mr Milner gave on 8 February 2018 (see http:// data. parliament. uk/writtenevidence/committeeevidence.svc/evidencedocument/ digital-culture-media-and-sport-committee/fake-news/oral/78195.pdf). That evidence also included the following relevant clarification regarding the statements you have quoted:

Q473 Chair: *[...] I just have a couple of clarification questions I want to ask before we finish. Going back to the discussion on Facebook developers, Mr Milner, you said that it was not true that developers had Facebook user data- but they had data about people on Facebook. I just wondered what the difference was between those two things.*

Simon Milner: *I suppose I was initially assuming that Mr Matheson was saying "Have you provided data? Has Facebook provided data to Cambridge Analytica or some other outside entity?" We do not provide your data to anyone without your permission; but the developer, the system that Ms Bickert was talking about, does allow people to decide, "I am prepared to let them have some of my Face book data in order to get a service from them. "I am sorry if I implied-*

As explained above, we found out in December 2015 that Dr Kogan may have transferred data obtained from Facebook users by his app to Cambridge Analytica. Any data Dr Kogan shared with Cambridge Analytica took place independently, outside of Facebook's platform (and we still have not been able to verify what sharing, if any, occurred because we have been holding off on our forensic audit of third parties at the request of the Information Commissioner's Office). Face book did not permit or agree to that transfer and it happened in breach of Facebook's Platform Policy. On learning this, we acted promptly to terminate Kogan's app from our platform and demanded that Dr Kogan and GSR, as well as the other entities to whom they confirmed they had disclosed data obtained via the app, account for and irretrievably delete all

such data. Facebook obtained written certifications from Dr Kogan, GSR, and other third parties (including SCL and Christopher Wylie) declaring that all such data they had obtained (including derivative data) was accounted for and destroyed. These deletion certifications were all obtained many months prior to Mr Milner's testimony; and Mr Milner's testimony is consistent with their contents and our understanding of the facts at that time.

In March 2018, after Mr Milner's testimony, Facebook received information from the media suggesting that the certifications we received may not have been accurate. We immediately banned SCL and Cambridge Analytica from our advertising platform and have since been investigating. As part of our investigation, we have hired a forensic auditor to understand what information Cambridge Analytica had and whether it has been destroyed. That is the most effective way to know whether Cambridge Analytica still has the data it obtained from Kogan. We paused the audit in response to the UK Information Commissioner's Office request, so that they can pursue their investigations first.

This answer is insufficient, as it ignores the facts that Facebook knew, and acted on, at the end of 2015 and the beginning of 2016:

- **On 9 December 2015, Harry Davies of the Guardian contacted Facebook UK Communications Department on 9 December;**
- **11 December 2015, the Guardian publishes an article on the Ted Cruz campaign, Cambridge Analytica, GSR, and the harvesting of Facebook data;**
- **Dec/Jan 2015/16, Mark Zuckerberg testified to Congress that Facebook then contacted Kogan and Cambridge Analytica.**

At the time, a fundamental feature of Facebook was that a Facebook user could grant access to friends' data, without their permission. GSR took advantage of that feature. Facebook was deliberately passing users' data to third parties, without those users' permission. Please comment on this.

25. At the time of Simon Milner's testimony in February 2018, who at Facebook knew about Cambridge Analytica? Who was in charge?

It was not until March 2018, after Mr Milner's testimony, that Facebook learned of allegations from the media that, contrary to their assurances, Dr Kogan and Cambridge Analytica did not delete data about Facebook users that Dr Kogan obtained through his app. At that point, a number of people at Face book became aware of these allegations, and we commenced a company investigation involving hundreds of different people, ultimately managed by our General Counsel, Colin Stretch.

Again, this answer is insufficient. There were multiple reports in the press, in both the UK and the USA, about the work of Cambridge Analytica and its relationship with Aleksandr Kogan and GSR. Facebook must have been aware of these articles. In testimony from Christopher Wylie, in July 2014, Aleksandr Kogan was delayed in his work because Facebook has denied access to Kogan. Kogan had a conversation with Facebook engineers about this.

26. When did Mark Zuckerberg know about Cambridge Analytica?

Mr. Zuckerberg did not become aware of allegations that Cambridge Analytica may not have deleted data about Facebook users obtained through Dr. Kogan's app until March of 2018, when these issues were raised in the media.

Our objection to your answer to question 25 applies also your answer to question 26. The CEO of Facebook either must have been aware of the multiple reports of data harvesting in the press, or he was willfully blind about the seriousness of the incident.

27. Can you tell us about the financial links between SCL and Cambridge Analytica?

We will provide separately our confidential letter to the Electoral Commission which addresses this issue.

28. How much money has been made from fraudulent ads (for example - but not limited to - the recent case of financial expert Martin Lewis?) When you find out they have been fraudulent, do you return the money to the purchaser of the ads?

Fraudulent ads are not allowed on Facebook. They are in breach of our advertising policies and we will remove them. We have been working with Mr Lewis's team for some time and have removed a large number of ads that feature him and violate our Ads policies. To make all of this happen automatically, as has been suggested, is technically challenging. We are constantly working on improving our machine learning tools to better detect fraudulent or misleading ads and prevent them from appearing on Facebook, and we are making good progress in this area. Where we discover adverts that violate our policies or applicable laws, we do not generally return money and it would seem perverse to return it to someone attempting to deceive our users. Instead, we make investments in areas to improve security on Facebook and beyond. In addition, the investments that we are making to address security issues are so significant that we have informed investors that we expect that the amount that we will spend will impact our profitability.

To repeat the question, how much money has been made from fraudulent ads? Your answer supposes that Facebook should be allowed to operate with their advertising going unchecked, simply because the operation is too large to monitor. As such, you seem to be implying that you should be allowed to run fraudulent ads until you perfect your technology to the point that you can detect and stop fraudulent ads. This is unacceptable.

29. Can we see copies of adverts from AIQ? Who were these adverts shown to? Who paid for them?

As explained in Ql 1 above, AIQ incurred approximately $2 million USD advertising on Facebook for a number of EU referendum campaigners. We are in the process of identifying and compiling the content and additional information for these adverts. We have also notified the campaigns who commissioned these adverts that the Committee has asked to see their content. We understand that you intend also to speak to the campaigns as part of your inquiry and will be able to put questions about their advertising, strategy and funding directly to them.

We asked to see the adverts, and did not ask to be referred to the campaigns. To repeat the question, can we see copies of adverts from AIQ? Who were the adverts shown to? Who pair for them?

30. Why wasn't GSR identified during audits of third party developers?

Dr Kogan signed a certification on behalf of his company, GSR, confirming that it had deleted all Facebook data obtained through his app. So GSR was one of the parties that signed a certification following our December 2015 investigation.

31. How can the feature allowing users to edit previews of articles (in response to concerns over Fake News) he removed?

We agree that allowing users to edit link previews can be abused to contribute to fake news and so we removed this ability in 2017, as part of our continuing efforts to stop the spread of misinformation on our platform. This remains disallowed for most people who share content on Facebook. However, conscious of the needs of publishers on our platform, we have provided a means for publishers to indicate their ownership of links and continue to be able to edit how their own links appear on Facebook. We allowed this because we know that media pages use this feature daily to customise and post links which they own.

32. What work is Joseph Chancellor doing right now for Facebook? What is his job title? Was Facebook aware of Joseph Chancellor's involvement in GSR at the time of his application to the company, or during his employment?

Mr Chancellor is a quantitative researcher on the User Experience Research team at Facebook, whose work focusses on aspects of virtual reality. We are investigating Mr Chancellor's work with Dr Kogan/GSR through counsel. The remainder of this question was answered by Mr Schroepfer (Qs 2186 - 2199, 2489).

33. Mr Schroepfer said that recruitment is taking place to boost work being done in Myanmar. When is this happening and can you provide more details?

We've been too slow in Myanmar to deal with the hate and violence. We are investing in people, technology and programs to help address these very serious challenges.
Specifically, our work has been focused on:
Policies - removal of hate speech and repeat offenders: We have clear rules against hate speech, harassment and fake accounts. This content has no place on Facebook, and we work hard to keep it off our platform. Our Community Standards (https://www.facebook.com/communitystandards) prohibit hate speech that targets people based on their race, ethnic identity or religion. We remove violating content when it's reported. We have also designated several hate figures and hate organisations in Myanmar. These include Wirathu, Thuseitta, Ma Ba Tha, and Parmaukkha. This means they are not allowed a presence on Facebook, and we will remove accounts and content which support, praise or represent these individuals or organisations.
People - more Myanmar dedicated resources: In the past two years, we have added dozens more Burmese language reviewers to handle reports from users across our services. We have also increased the number of people across the company working on Myanmar-related issues and we now have a special product team working to better understand the local challenges and build the right tools to help keep people in the country safe. We are hiring more staff dedicated to Myanmar, including Burmese speakers and experts.
Products - tools and technology to help detect and remove content and accounts that violate our policies: We have improved the way we detect fake accounts on our service - including

ones that are hard to spot. Specifically, our technology is able to more effectively recognise fake accounts by identifying patterns of activity - without assessing the content itself. For example, our systems may detect repeated posting of the same content or an increase in messages sent.
Partnerships - digital literacy education with local partners: We launched a local language version of our Community Standards (https://www.facebook.com/safety/resources/myanmar) to educate new users on how to use Facebook responsibly in 2015 and we have been promoting these actively in Myanmar, reaching over 8 million people through promotional posts on our platform alone. We've also rolled out several education programs and workshops with local partners to update them on our policies and tools so that they can use this information in outreach to communities around the country.
One example of our education initiatives is our work with the team that developed the Panzagar initiative (https://www.facebook.com/supportflowerspeech) to develop the Panzagar counterspeech
Facebook stickers to empower people in Myanmar to share positive messages online. We also recently released locally illustrated false news tips, which were promoted on Facebook and in consumer print publications. We have a dedicated Safety Page for Myanmar (https://www.facebook.com/safety/resources/myanmarand) and have delivered hard copies of our local language Community Standards and safety and security tips to civil society groups in Myanmar who have distributed them around the country for trainings.

You have not answered the question of when this happened/is happening.

34. What is the average time taken to respond to content that has been reported to Facebook in the region?

User content reports are reviewed by our Community Operations team who work around the globe 24 hours a day, seven days a week. The vast majority of the content reported to us is reviewed within 24 hours. It can be even faster for specific types of content such as credible threats or suicide prevention, as we optimise our processes to make sure that our team of experts handles these sensitive reports as quickly as possible.

This response does not answer the question – it states "the vast majority of the content reported to us is reviewed within 24 hours". Instead, we want to know the *average time taken* to respond to content that has been reported to Facebook *in the region*.

35. How many fake accounts have been identified and removed in Myanmar?

We don't break down the removal of fake accounts by country. We will however be publishing our transparency report this week which will include information about the prevalence and removals of fake accounts globally.

If you don't break down the removal of fake accounts by country, this poses another question – why do you not break down the removal of fake accounts by country? Is it not a simple process to break down the removal of fake accounts by country? If you cannot break down fake accounts by country, is this not a serious lack of investment in developing analytics to deal with fake accounts? Given the seriousness of the issues regarding online disinformation and Facebook, the humanitarian crisis of Myanmar, and the impact of elections in Europe and America, country-by-country reports would be enormously helpful to the public, and to prosecutors.

36. How much of your revenue is derived from Myanmar?

Myanmar is a small market for Facebook. We do not publish country advertising revenue figures.

You may not publish country advertising revenue figures, but you will have that information. Again, how much of your revenue is derived from Myanmar?

Why will you not publish country-by-country advertising revenue figures? You regularly publish 'regional' figures, so why not country figures?

37. Are custom audiences used as a tool by AIQ using the GSR data from the US? What was the total value of AIQ Vote Leave spend on Facebook? Can we see examples and copies of adverts that they used? To whom were they sent, and who decided what kind of targeting to use?

This question has been answered in our response to Qs 11 & 29 above.

Question 29 refers to Question 11, and Question 11 has not been answered. We asked for examples and copies of adverts that AIQ used, where they were sent, and who decided what kind of targeting to use. Please answer the question.

38. Is there evidence that CAISCL shared data with AIQ?

From the investigations we have conducted to-date we have found no evidence that AIQ used data obtained from Dr. Kogan's app to advertise on our platform for the purposes of the EU referendum. Specifically, as Mr. Schroepfer explained in his written submission to the Committee:

• Many of the Referendum-related ad campaigns AIQ ran on Facebook employed Data File Custom Audiences (DFCA) to target Facebook users. Advertisers create DCFAs by uploading a data file with a list of people for whom they have contact information, such as email addresses and phone numbers. Once the file is uploaded, the data is hashed. Facebook then uses the hashed data to find matches with Facebook users to create the audience. DFCAs are the only method through which an advertiser can input its own data to attempt to identify specific Facebook users for ad targeting. However, all of the DFCAs AIQ created used email addresses to match to the individuals from the data file AIQ uploaded with Facebook users. The data gathered through Dr. Kogan's app did not include the email addresses of app installers or their friends. This means that AIQ could not have obtained these email addresses from the data Dr. Kogan's app gathered from Facebook. AIQ must have obtained these email addresses targeted in these campaigns from a different source.

• We also conducted an analysis of the DFCAs employed by AIQ in its Referendum-related ads, on the one hand, and UK user data potentially collected by Dr. Kogan's app, on the other hand, and found very little overlap (fewer than 4% of people were common to both data sets, which overlap we believe to be consistent with random chance). As a result, we have no evidence This suggests that data from Dr. Kogan's app was not used to build AIQ's targeting data sets in connection with these Referendum campaigns. Only AIQ has access to complete information about how it generated these data sets.

39. Why was data responsibility moved from Facebook Irl to Facebook Inc in California just one month before GDPR kicks in?

Mr Schroepfer answered this question at the hearing (Q2372-2374). All users in the EU will continue to be provided with the Facebook service by Facebook Ireland, who remains the data controller for EU user data. Facebook Inc. will provide the Facebook service to people outside of Europe, which is not a change for many parts of the world. This ensures that we can continue to be responsive to local regulatory concerns, without an obligation to work through an EU-based Lead Supervisory Authority for people outside of Europe (under provisions in the GDPR, the Irish Data Protection Commissioner would be the lead supervisory authority responsible for all people receiving services from Facebook Ireland, a controller based in the Union). We've received strong feedback from regulators and judicial systems outside of Europe that they want us to be directly responsive to them and not be required to go through Europe on data protection matters.
This also allows us to customize our terms and data policy to reflect regional norms and legal frameworks. For example, the Facebook Ireland terms and data policy describe the legal basis that applies to each form of data processing, but this is not a concept that has any relevance outside of Europe. Likewise, we are providing different versions of our Facebook Inc. terms in different countries. For example, consumers outside of the United States will be able to bring legal action against Facebook in their home country, whereas people inside the United States are required to bring legal action against Facebook in courts in California. These changes are now reflected in separate localized terms.
Facebook has now held lengthy meetings or evidence sessions around the world. In the UK we provided written submissions to this inquiry, we have provided senior officials to give evidence to the Committee's session in Washington, one of the most senior people in the company has given 5 hours of testimony in the UK Parliament and today we have answered the 39 further questions provided by the Committee. We were disappointed after providing a very significant amount of information to the Committee at the last hearing the Committee declared our response insufficient.

This is an insufficient response. GDPR does not require, for example, that data violations in Mexico should be handled through European regulation. GDPR requires that, if Mexican data were to be processed in the EU, it should be processed in accordance with EU law. This would be *in addition* to Mexican regulation.

If a Facebook user in the EU sends a message from a user not in the EU, does Facebook consider that message to be processed in the EU, or not in the EU?

In conclusion, we continue to hold the belief that Mark Zuckerberg should appear before the Committee. The insufficient contents of this letter, coupled with previous oral evidence and written correspondence, do not satisfy us that you have provided all the information that we require.