facebook

Damian Collins
Chair, Digital, Culture, Media and Sport Committee
House of Commons
London
SWlAOAA

8 June 2018

Dear Mr Chairman,

Thank you for your letter dated the 21 May 2018. We have endeavoured to reply to your questions below as promptly and fully as possible.

Below are the answers to your additional questions:

Additional Questions to Response #1

- **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?**

EU law imposes clear obligations in respect of both the processing of personal data and the use of cookies and similar technologies. The law imposes these obligations on both the providers of third-party technologies such as Facebook and Google as well as website and app operators themselves, depending on their individual circumstances. The law therefore places the responsibility on all operators, regardless of their size, to ensure that they are compliant with any and all legal obligations that may apply to them based on their individual circumstances, including in cases where the apps or websites collect or use data for their own purposes (i.e. as a "controller"). This is in addition to, and not instead of, any legal obligations that may fall upon Facebook.

- **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?**

Facebook Connect (now called Facebook Login) and the Facebook Like button are very different products. Our number of 8.4m was based on the number of unique domains over a 7-day period which used the Facebook Like button.

facebook

Additional Questions to Response #2

- **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?**

The following former Internet Research Agency (IRA) Facebook and Instagram Pages were the sources of the IRA's website Custom Audience:

  - United Muslims of America;
  - Black Matters US;
  - Being Patriotic; and
  - Defend the 2nd.

Additional Questions to Response #3

- **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.**

We understand the Committee's desire for additional information, but the many teams across Facebook (for example engineering, product, security, sales, policy, legal) working on this also work on multiple other projects. As we don't track hours spent per project per person we generally don't have per project budget figures, including for adverts with political content.

Additional Questions to Response #4

- **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?**

At the time of our response, we understood that we did not have records that reliably established the number of apps we terminated for developer violations prior to 2014. However, as our investigation has continued to progress, we have this week determined that we have records dating back to 2010 that we are currently analysing. We will update the Committee in due course.

- **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.**

The approximately 299,000 apps referenced in our response were those that sought access to anything beyond basic data fields and were rejected at the App Review stage.

facebook

Additional Questions to Response #5

- **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?**

The agreement was signed as part of the formal agreement between Dr Kogan and Facebook in which he asserted that he had deleted all Facebook user data and derivative data obtained from Facebook Applications. This agreement concluded months of negotiation between Dr Kogan's law firm and the law firm that Facebook engaged to enforce its policies. The similarity in timing to the result day of the UK Referendum is a coincidence.

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

The settlement agreement with Dr Kogan required deletion of derivative data as well as raw data. The settlement agreement defined 'App Data,' which was required to be irretrievably deleted, to include 'Facebook user information obtained from the Facebook Applications and data derived from such Facebook user information, specifically: a) personality scores and average personality scores; b) derived dimensional scores summarising information captured in the "likes"; and c) a co-occurrence matrix of likes.'

- **Does the NDA prevent legal action being taken?**

The settlement agreement does not prevent legal action for any breach of the representations or commitments made in the settlement or for any matters outside the scope of the settlement. Instead, as described in the settlement agreement and Mutual Release, provided to you with our last response, Facebook and GSR/Dr Kogan released each other from claims and liabilities relating to Dr Kogan's app and his subsequent sharing of some data with other parties, in consideration for his agreement to certify the deletion of all data acquired through the app and derivatives thereof. The settlement agreement does not affect the legal rights of any parties other than Facebook, GSR and Dr Kogan.

- **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?**

The settlement agreement was not signed by a member of Facebook's senior management team. It was signed by a member of Facebook's legal department involved in enforcing Facebook's policies against Dr Kogan and GSR. The version we sent you did not have the Facebook employee's signature on it, but it did include the names of the third parties to whom Dr Kogan provided data. The only redactions therein made for the purposes of sending the document to you are marked with a black bar.

facebook

Additional Questions to Response #6

- **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.**

As previously stated, the allegations regarding Dr Kogan were not brought to our attention in until late 2015. We understood them to be a violation of our policies and took action consistent with our developer enforcement program. Because we had terminated the app from our platform, our focus was on securing commitments to delete all remaining data. With the benefit of hindsight, we wish we had gone beyond our legal obligations and notified people whose information may have been affected. We have since done so. Mr Zuckerberg has stated that ultimately he is responsible for what happens with Facebook.

We understand that Mr Wylie claimed that in July 2014, Dr Kogan told Mr Wylie that he had a conversation with Facebook engineers about difficulty accessing data with his app. More recently, Dr Kogan has testified to the Committee that Mr Wylie's story was not true and that he knew no Facebook engineers with whom he could have had a conversation. We have been unable to identify any evidence to support Mr Wylie's claim.

Additional Questions to Response #8

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

No, the agreement is not retroactive, and does not cover the period before his employment.

Additional Questions to Response #10

- **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?**

The adverts we provided to the US Congress pertained to activity in the US and not to the scope of what we understood the Committee's focus to be (potential Russian interference in the UK during the Brexit referendum campaign). The adverts are available at https://democrats-intelligence.house.gov/facebook-ads/social-media-advertisements.htm, and a list of the filenames of adverts that were provided to Congress that were also targeted to users in the UK is attached.

Additional Questions to Response #11

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

  The payments to Facebook originated from a bank in Canada.

Additional Questions to Response #12

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

Given this figure would include everything from messages from friends and family overseas, to updates from sports teams and celebrities, to adverts in global advertising campaigns, to Pages and accounts followed by UK users, it is likely to be most UK Facebook and Instagram Users.

- **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?**

As we have previously reported to the Committee, we have not found any systematic targeting of the UK by the IRA in the referendum period (15 April to 23 June 2016), only the minimal activity we reported to the Committee already. Looking further back over the activity of the IRA accounts from as early as January 2015 (including the period of over a year before the start of the regulated referendum period), the total spend on impressions delivered to the UK is approximately $463. This is inclusive of all of the adverts released by the US Congress last month. The $1 spend we previously reported reflects the amount spent during the regulated referendum period by the IRA which is the time period which the Election Commission asked us to investigate.

Additional Questions to Response #14

- **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?**

Our systems do not have a perfect or reliable way to classify the category that advertisements (which are developed and distributed by third-parties on our platform) fall in, whether it is political or housing or educational or otherwise. We are heavily investing in advanced technologies and machine learning to better assess advertisements that fall into specific categories (like political and issues adverts) so we can identify and enforce policies and tools that may apply, like the transparency tools we've discussed. These systems are not perfect but they are continuously learning and improving. In addition, issue-based advertising is particularly difficult to define at a global scale as there is no universal definition of a political issue advert and this concept varies by culture and geography. We are continuing to refine our definition of this in collaboration with external stakeholders in anticipation of rolling out our transparency tools in the UK.

Additional Questions to Response #15

- **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?**

Most targeted advertising on the Internet is not visible to anyone except the target audience. On Facebook by contrast, adverts are generally visible to a broad audience as they also exist as posts on the advertiser's Page. We do allow advertisers to create and boost a post without publishing it on their Page, but these ads (as well as other ads) will soon be viewable to all Page visitors on a "view ads" surface. Regardless of how the advert was created, we retain certain advertiser data as well as information about their ad campaigns.

- **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**

As described in our letter to the Committee of 28 February 2018, we used multiple indicators, only one of which was Russian currency, to identify accounts possibly operated by someone located in or connected to Russia. Please refer to our response to question 15 below in relation to maintaining addresses.

- **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?**

Our 'View Ads' feature will allow users to view all adverts a Page is running, regardless of whether or not that user falls within the targeted audience for that advert. Information on how 'View Ads' works, including screen shots detailing this feature, is available here: https://newsroom.fb.com/news/2017/10/update-on-our-advertising-transparency-and-authenticity-efforts/.

- **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?**

Yes. For example, an advertiser is not required to provide their address when placing advertising. Further, we may not have full credit card or bank account details where an advertiser has updated or otherwise removed these payment methods from their account. However, advertisers wishing to run adverts with political content in the US will be required to verify their identity and location. We plan to roll this out in the UK in advance of the local elections in 2019.

Additional Questions to Response #16

- **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?**

Yes. As explained in our previous response, we retain certain advertiser data as well as information about an advertiser's accounts on the Facebook platform and information about their ad campaigns (most advertising content, run dates, spend, etc.), including when the underlying Page or Ad is deleted.

Additional Questions to Response #17

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

We are unable to provide a reliable full breakdown because the top countries listed are an approximation. Fake accounts use various techniques to attempt to disguise their location, including redirecting their traffic from remote locations, using proxies, VPNs and botnets. We listed the countries that appeared to be the source of the majority of the engagement, based on our best judgment, but we do not believe that we can provide a more reliable complete breakdown that will actually be helpful in understanding the activities we disrupted.

Additional Questions to Response #19

- **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?**

We stated in our 14 May letter that "[d]ue to system changes, we do not have records for the time-period before 2014 that establish *the number of apps we terminated for developer violations*." (Emphasis added). In any case, as stated in our response to question 4 above, our investigation has continued to progress.

- **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?**

We are in the process of investigating. Tens of thousands of apps have been identified for review. In general, an app will be reviewed if (among other reasons, e.g. escalation through Data Bounty) it launched prior to the changes we made to platform policies in 2014, if it had a significant number of users and if the app sought to access significant data fields. Please note that there is a distinction between having the ability to access large amounts of data and actually accessing that data, the latter of which is part of our ongoing investigation. All of the factors you listed contribute to our definition of having potential access to large amounts of data.

- **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).**

In March 2018, we began the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014.

Additional Questions to Response #20

- **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?**

This question has been answered extensively by Mr Schroepfer and elsewhere. At the time Dr Kogan launched his App, developers were able to request consent to access data through the Graph API V1, without that app being reviewed proactively. We are investigating how many developers may have misused the platform. This changed in 2014 when we announced significant restrictions to the categories of data third-party apps had access to and began

proactively reviewing all apps seeking more than basic information. 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 employ 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 US, despite statements by Dr Kogan and Cambridge Analytica that only US user data was shared, as well as documentation obtained by your committee that further supports this conclusion. The 2014 data licensing contract between GSR and SCL (an affiliate of Cambridge Analytica) suggested that the derived data that Dr Kogan/GSR expected to share with SCL under that contract may have related to users in only eleven US states. We have not been able to independently verify whether the sharing was in fact limited in this way, but will work to do so.

Additional Questions to Response #21

- **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.**

We are unable to provide a precise figure, as our products are built and supported by staff from many different departments across the company, and many different teams work on platform features at a given time.

Additional Questions to Response #22

- **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"?**

We provide clear and transparent information to people about how we collect data on third-party sites in a number of ways — including in a prominent consent tile that all EU users must engage with to continue using Facebook. The information we provide to users about how we collect and process their information is prominent, not hidden.

Visitors to Facebook also are clearly informed about, and provide consent to, Facebook's use of cookies by a prominent cookie banner, together with our Cookies Policy and our Data Policy, which provide further detail about how we use these technologies and how we process the data in question.

Our Cookies Policy (available at https://www.facebook.com/policy/cookies/) makes clear that we use cookies and similar technologies on other websites and apps that use Facebook's services, such as Facebook social plug-ins, whether or not that person is a registered Facebook user or is logged in. The Cookies Policy also provides details about how people can exercise controls over the use of such cookies (for example, by disabling or deleting cookies in their browser settings).

Furthermore, our Data Policy (available at https://www.facebook.com/about/privacy) provides extensive information about what data we collect, how it is used, and the controls people have. This also explains to users the legal basis upon which we process this data, in accordance with applicable data protection law.

All of these policies are clearly and permanently accessible and easily navigable for all visitors to and users of Facebook products, regardless of whether they are a registered Facebook user or are logged in. We have recently updated these policies to make them even more accessible for users (taking into account specific guidance from the Article 29 Working Party) and to optimise for both desktop and mobile environments.

Facebook does not create profiles for people without a Facebook account. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically 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 Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, as stated by Mr Schroepfer, 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 browser information about their visit to each one of those third parties. This Facebook News Room post has more information about how this works:https://newsroom.fb.com/news/2018/04/data-off-facebook/. This information is not used to create profiles on non-Facebook users.

In addition, in order for third parties to use our Facebook technologies in their websites or apps, it is 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.

Additional Questions to Response #23

- **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.**

Dr Kogan's app only had access to data about the installing user that the installing user chose to share with the app, and to data about friends of the installing user that was: (1) made available by those friends to the installing user; and (2) shared with the app in accordance with those friends' own privacy settings regarding such sharing with third-party apps. This was authorised by the installing user in the same manner as regularly practiced by other digital platforms including Apple's iOS and Google's Android operating systems and related app platforms.

Additional Questions to Response #24

- **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.**

We have explained multiple times that Facebook does not pass user data to third-party app developers, and (prior to 2014) users could not grant third-party apps access to their friends' data unless their friends had shared that data with them and unless their friends' privacy settings permitted it. If a user's privacy settings did not allow sharing with third-party apps installed by their friends, that information was not shared. These limitations were consistent with Facebook's Statement of Rights and Responsibilities and Data Policy at the time, which were agreed to by every Facebook user when they registered for the service, and Facebook developed education materials alerting people to these apps settings, including education integrated into the new user sign up flow for every user, at the insistence of the Irish Data Protection Commissioner.

Additional Questions to Response #25

- **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.**

With regard to the statements made by Mr Wylie, please see answer 6 above. On 11 December 2015, The Guardian published an article reporting that Cambridge Analytica had used "psychographic profiles" based on Facebook users' information in support of Ted Cruz's presidential campaign. Facebook contacted Cambridge Analytica on the same day the article was released and was told by Cambridge Analytica that if it had obtained any Facebook data, it had not been deliberate. Cambridge Analytica disputed the factual accuracy of The Guardian report and assured Facebook in writing, on 18 January 2016, that it had deleted the data it received from Dr Kogan/GSR and their server contained no backups of the data.

Facebook also contacted Dr Kogan on 11 December 2015, demanding an explanation of what data he provided to Cambridge Analytica. Facebook subsequently retained outside counsel to handle settlement negotiations with Dr Kogan. As part of the settlement agreement with Facebook, Dr Kogan certified that he deleted all of the Facebook data collected by his app and derivative data.

Additional Questions to Response #26

- **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.**

Facebook's legal team and platform enforcement team knew about Cambridge Analytica in 2015, when Facebook banned Dr Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Dr Kogan, GSR, Cambridge Analytica and SCL declaring that all such data they had obtained was accounted for and destroyed at the close of lengthy enforcement and settlement negotiations. Facebook, and Mr Zuckerberg, became aware from media reporting in March 2018 that the certifications we received may not have been accurate. Facebook immediately banned Cambridge Analytica and SCL from using our services.

Additional Questions to Response #28

- **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.**

We are committed to tackling fraudulent adverts, and have explained the efforts we are making to remove them from our platform and prevent them appearing in the first place. We are spending such significant sums on security efforts that our profitability may be impacted. We believe however that annual revenue that is attributable to inauthentic or false accounts is not material to our profitability.

Additional Questions to Response #29:

- **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 paid for them?**

As explained in our prior response to you, AIQ incurred approximately $2 million USD advertising on Facebook for the Vote Leave Facebook Page, the BeLeave Facebook Page, the Veterans for Britain Facebook Page and the DUP Vote to Leave Facebook Page. The invoices for the ads run on all of these pages were settled with Facebook by AIQ. We are in the process of identifying and compiling these adverts.

Additional Questions to Response #33

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

As we said in our prior response, we have already hired more people and taken other steps to help address this challenge, and we are continuing to do so.

Additional Questions to Response #34

- **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.**

It is not meaningful to provide an average figure for response times across all types of content, as our approach to different types of content varies considerably depending on the nature of the content in question. The vast majority of the content reported to us gets reviewed

within 24 hours; however we try to optimise our processes to be able to respond much faster for specific types of sensitive content where this is required, such as credible threats or suicide prevention. Conversely, our response time may be longer for reports that give rise to complex legal issues.

In the latest round of testing under the European Commission code of conduct countering hate speech online (available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086), Facebook assessed 89.3% of notifications in under 24 hours. We have also been working hard on how we use technology to help in our enforcement efforts against content that violates our Community Standards. For example, for content related to terrorism, in Q1 2018, 99% of the ISIS and al-Qaeda content we took action on was before a user reported it. In May we released our first transparency report to detail our enforcement efforts on content that violates the Community Standards. The report can be found at the following link: https://transparency.facebook.com/community-standards-enforcement.

Additional Questions to Response #35

- **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.**

We're looking into ways we might be able to provide country-level breakdowns; our focus has been on detecting and removing fake accounts, which does not require precise measurements by country. Generating confident breakdowns beyond estimates is complicated because fake accounts use various techniques to attempt to disguise their location, including redirecting their traffic from remote locations, using proxies, VPNs and botnets. Our approach has therefore focused instead on how these fake accounts are created and how they operate, no matter where the accounts are created.

In our recent Community Standards Enforcement Report (which can be found at: can be found at the following link: https://transparency.facebook.com/community-standards-enforcement), we shared the following details about Q1 of 2018 (though these metrics are still in development):

- We estimate that fake accounts represented approximately 3% to 4% of monthly active users (MAU) on Facebook;

- We disabled 583 million fake accounts; and

- 98.5% of fake accounts acted on were flagged by Facebook before users reported them.

Additional Questions to Response #36

- **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?**

We comply with all applicable company and revenue disclosure requirements. This means that, like any other company, we publish regular company reports and revenue figures for our legal entities in line with the specific requirements of the country. We provide all required information to tax authorities which they may share with other tax authorities according to their agreed protocols.

Additional Questions to Response #37

- **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.**

AIQ incurred approximately $2 million USD advertising on Facebook for the Vote Leave Facebook Page, the BeLeave Facebook Page, the Veterans for Britain Facebook Page, and the DUP Vote to Leave Facebook Page. The invoices for the ads run on all of these Pages were settled with Facebook by AIQ, beyond which we cannot know who decided on targeting criteria. We are in the process of identifying and compiling these ads.

Additional Questions to Response #39

- **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.**

As you state, generally speaking the GDPR applies to all processing of personal data by entities within the EU, as well as to processing of data about people within the EU by companies located outside of the EU, in particular circumstances. If Facebook Ireland were to serve as data controller to users outside the EU, our practices in relation to their data would be subject to regulation under the GDPR within the EU, and the Irish DPC would be the lead supervisory authority for users in regions serviced by Facebook Ireland. In our previous reply, we articulated our desire to be responsive to local regulatory concerns outside of Europe, which was a significant factor in our decision to change this structure.

Now, Facebook Ireland is responsible for data processing in respect of all European users, and complies with GDPR. Facebook, Inc. will be responsible for data processing in respect of all other users of the Facebook service, and whilst the GDPR is not directly applicable to this processing, Facebook Inc. will apply the same controls, protections and principles as Facebook Ireland, globally.

- **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?**

Facebook is delivered to people around the world over a global infrastructure. Facebook Ireland is legally responsible for the processing of EU users' data, including sending their messages to other Facebook users in accordance with GDPR and it uses this global infrastructure for this purpose. This is explained in the "How do we operate and transfer data as part of our global services?" section of our Data Policy at: https://www.facebook.com/policy

Where we have indicated that we will follow up in more detail we will do so as soon as possible.

We first made a written submission to the former incarnation of this inquiry in March 2017, we have responded 8 times in writing to your questions, and appeared twice before the committee. I hope these answers are helpful in your inquiry.

Yours Sincerely

Rebecca Stimson
UK Head of Public Policy

facebook

Attachment to Question 10 (IRA adverts given to U.S. Congress also targeted at UK)

1. P(1)0001209
2. P(1)0003149
3. P(1)0003155
4. P(1)0003157
5. P(1)0003159
6. P(1)0003161
7. P(1)0003163
8. P(1)0003173
9. P(1)0003175
10. P(1)0003177
11. P(1)0003183
12. P(1)0003189
13. P(1)0003193
14. P(1)0003195
15. P(1)0003203
16. P(1)0003209
17. P(1)0003211
18. P(1)0003213
19. P(1)0003215
20. P(1)0003217
21. P(1)0003219
22. P(1)0003221
23. P(1)0003223
24. P(1)0003231
25. P(1)0003233
26. P(1)0003339
27. P(1)0003341
28. P(1)0003343
29. P(1)0003345
30. P(1)0003347
31. P(1)0003349
32. P(1)0003351
33. P(1)0003353
34. P(1)0003355
35. P(1)0003357
36. P(1)0003359
37. P(1)0003361
38. P(1)0003401
39. P(1)0003405
40. P(1)0003409
41. P(1)0003413
42. P(1)0003417
43. P(1)0003421
44. P(1)0003425
45. P(1)0003429
46. P(1)0003433