

DCMS Select Committee – Fake news inquiry

Mike Schroepfer, Chief Technology Officer, Facebook

Written submission – 26th April 2018

I would like to thank the Committee for asking me to come here today to talk about the events that have come to light in recent weeks and the steps we are taking to address them. I wanted to submit some information for the record that can inform our oral session.

First, allow me to introduce myself. My name is Mike Schroepfer, and I am the Chief Technology Officer at Facebook. I am a software engineer by background. I have been with Facebook since 2008 and Chief Technology Officer since 2013.

I want to start by echoing our CEO, Mark Zuckerberg: what happened with Cambridge Analytica represents a breach of trust, and we are deeply sorry. We made mistakes and we are taking steps to make sure it doesn't happen again.

Today we serve more than 2 billion people around the world who use our services to stay connected with the people who matter to them most. We know we have a responsibility to the Facebook community, and that people will only use our products if they trust their data is safe.

The UK is of immense importance to us. There are 40 million monthly active users on Facebook in the UK and more than 2 million active small business Pages as well as 29 million Groups. By the end of this year we will have a total of 2,300 people working for Facebook in the UK. The engineering talent that can be found in this country has made our London office our biggest engineering hub outside of the US. Our office now includes engineers, developers, marketing and sales teams, covering many facets of Facebook's work.

As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they care about, make their voices heard, and build communities and businesses. But it's clear now that we didn't do enough to prevent these tools from potentially being used for harm as well. We didn't take a broad enough view of our responsibility, and that was a mistake.

Cambridge Analytica

While much has been written about the Cambridge Analytica issue over the past month, I wanted to set out the key actions we took over the past few years.

- In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly,

apps like Dr. Aleksander Kogan's "Thisisyourdigitallife" (TIYDL) could no longer ask for data about a person's friends unless their friends had also authorized the app.

- We also required developers to get approval from us before they could request anything more than basic information from people, and we have rejected more than half of the apps requesting approval to seek these extended permissions. These actions would prevent any app like TIYDL from being able to access the data at issue today.
- In late 2015, when we learned Kogan had shared the data, we immediately banned TIYDL from our platform and demanded that he delete all data he obtained from that app. We also demanded deletion from everyone that Kogan identified as having been passed some data, including Cambridge Analytica, and certification from all parties that the deletion had been completed.
- Last month, when we learned from the media that Cambridge Analytica may not have deleted the data as they had certified, we banned them from using any of our services.

Most of the users whose data was collected by TIYDL were in the United States and Kogan has said that he passed data to Cambridge Analytica only for users in the United States. However, we understand that 1,040 people in the UK installed TIYDL, and around 1 million people in UK may have been friends with someone who installed the app, and, therefore, may have been affected. We have now notified all people potentially affected.

Action to prevent this happening again

Although the changes we announced in 2014 would prevent any app like TIYDL from being able to access the same Facebook data today, we know that these changes did not go far enough. In recent weeks, we have taken several other significant steps.

- We are limiting the information developers can access using Facebook Login and we are putting additional safeguards in place to prevent abuse. For example, we are removing developers' access to a person's data if they haven't used their app in 3 months. We will reduce the data someone gives to an app when they sign in to only their name, profile photo, and email address.
- We are investigating all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we are conducting a full review of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps.
- We're making it easier to understand which apps people allowed to access their data. We have shown everyone a tool at the top of your News Feed with the apps they have used and an easy way to revoke those apps' permissions to their data.
- We have launched Facebook's 'data abuse bounty' program so that people can report to us if they find misuses of data by app developers. This program will

reward people with first-hand knowledge and proof of cases where a Facebook platform app collects and transfers people's data to another party to be sold, stolen or used for scams or political influence.

We know there's a lot of work to do here, and that this is just the beginning.

Our work with ICO and the Electoral Commission

We are grateful to the UK's Information Commissioner's Office for their diligent work in investigating the Cambridge Analytica issue. We fully support their work and are providing help and assistance in order that they can complete their work as quickly as possible. This includes technical support where helpful, as well as providing them with information that will be of assistance.

They have asked us a number of questions about Cambridge Analytica, as well as AggregateIQ ("AIQ"), and their connection to the 2016 Referendum, and I know this Committee has also investigated these matters. My team and I met with the Information Commissioner's Office this week to update them on our internal investigations, and I wanted to share with you a short summary of the information we have provided them and also the Electoral Commission.

- **Cambridge Analytica** - We did not find any referendum related ads or pages on Facebook directly managed by Cambridge Analytica or SCL Group.
- **Aggregate IQ** - Our records show that AIQ spent approximately \$2M USD on ads from pages that appear to be associated with the 2016 Referendum. We have provided details on the specific campaigns and related spending to the ICO and Electoral Commission. In the course of our ongoing review, we also found certain billing and administration connections between SCL/Cambridge Analytica and AIQ. We have shared that information with ICO for the purposes of their investigation.
- **Use of TIYDL data** - When an advertiser runs an ad campaign on Facebook one way they can target their ads is to use a list of email addresses (such as customers who signed up to their mailing list). AIQ used this method for many of their advertising campaigns during the Referendum. The data gathered through the TIYDL 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 TIYDL gathered from Facebook. AIQ must have obtained these email addresses for British voters targeted in these campaigns from a different source. We also conducted an analysis of the audiences targeted by AIQ in its Referendum-related ads, on the one hand, and UK user data potentially collected by TIYDL, on the other hand, and found very little overlap (fewer than 4% of people were common to both data sets, which is the same overlap we would find with random chance). This further suggests that the data from TIYDL was not used to build AIQ's data sets in connection with the Referendum campaigns, although only AIQ has access to complete information about how it generated these data sets.

Ad transparency and integrity

We share the Committee's goals around election integrity and believe that there is more that we can do as a platform to increase transparency around elections.

When it comes to advertising on Facebook, people should be able to see all the ads that a page is running – and when it comes to political ads, all advertisers should be verified and any ads that they run should be clearly labeled to show who paid for them.

We are working hard to build out these transparency tools and to roll them out globally, but it takes time to do that and, most importantly, to get that right. I can tell the committee that we will be able to roll out the first phase of our transparency efforts — the view ads tool — in the UK by 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.

I would also like to inform the committee that the following measures will be rolled out in the UK 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;
- Ads that are political adverts will be required to be labeled as “political” and to display who paid for them;
- Ads to 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).

Furthermore, to promote transparency, any labeled political ad that ran will be available for seven years in the archive. The archive will offer:

- Search functionality for ads that will enable you to see ads from a rolling four-year period – starting from when we launch the archive.
- General information about the amount spent on the ad.
- General information about the number of impressions that were delivered.
- Demographic information (e.g. age, general location, gender) about the audience that the ads reached.

While we will continue to improve our tools, we also believe that bringing more transparency to the political process is a project that is bigger than one company, or one industry. In that spirit my colleagues met with the UK Electoral Commission on Tuesday, and I will be meeting Government ministers later today to offer our support and cooperation in their consultation to develop an update to current electoral law on transparency in the UK.

The matters we will be discussing today are as important to us at Facebook as they are to you and your inquiry. I look forward to answering your questions.