

Vaste Kamercommissie voor Veiligheid en Justitie
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Amsterdam, May 23rd 2018

Dear members of Parliament,

I would like to thank the Justice and Security Committee for inviting me to the Round Table on Internet Company and Privacy Protection and giving me the opportunity to submit some information for the record that can inform our oral session.

First, allow me to introduce myself. My name is Stephen Deadman, and I am the Global Deputy Chief Privacy Officer at Facebook.

I want to start by echoing our CEO, Mark Zuckerberg: what happened with Cambridge Analytica represents a breach of trust, and we sincerely apologize.

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.

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, we announced that we were changing our Platform for app developers to dramatically limit the data apps could access and to enhance its granular data permissions for users. 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 introduced an App Review process that 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 improperly shared the data he obtained from users, we immediately banned TIYDL from our platform and demanded that he delete all data he obtained with his app. We also demanded deletion from everyone whom Kogan identified as having been passed data, including SCL Elections Ltd.

("SCL"), Cambridge Analytica's parent company, and obtained certifications from those parties that the deletion had been completed.

- When we learned from the media in March 2018 that Cambridge Analytica may not have deleted the data it obtained from Kogan, we banned them from using any of our services.

Most of the users whose data was collected by TIYDL were in the United States. We understand that 28 people in the Netherlands installed TIYDL, and almost 90,000 people in the Netherlands may have been friends with someone who installed the app, and, therefore, may have been affected. We have now notified all people who may potentially have been affected. However, as we have seen in documents publicly posted by the U.K. House of Commons Digital, Culture, Media and Sport Committee, Alexandr Kogan, the app developer in this case, contracted with SCL to license information of people in the United States – not people in the EU –and Kogan has testified that he only provided the data of US users. We have seen no evidence that Kogan shared data about European users with SCL or Cambridge Analytica. We will conduct a forensic audit of Cambridge Analytica as soon as we have confirmed that it will not interfere with the investigation by the UK's Information Commissioner.

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 busy 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. To date thousands of apps have already been investigated and around 200 have been suspended — pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and notify people.
- 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 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.

GDPR

In addition to the above, we have taken many more steps in the last weeks to put people more in control of their personal data. Most of these updates have been in the works for some time, but the events of the past several months underscore their importance. For an overview of our Facebook Privacy Updates, I'd like to refer to the attached one pager, in Dutch.

We have also announced at our developer Conference F8, one more step which we are building: "Clear History". This new feature will enable you to see the websites and apps that send us information when you use them, to clear this information from your account, and turn off our ability to store it associated with your account going forward. This is similar in concept to the "clear cookie cache" provided by many browsers.

Thanks again for your invitation and I hope to see you all on the 24th of May.

Kind regards,

Stephen Deadman
Global Deputy Chief Privacy Officer