FUTURE TENSE

Who Is to Blame for the Cambridge Analytica–Facebook Scandal?

There's lots of places to point the finger.

By TIFFANY C. LI
MARCH 19, 2018 • 7:52 PM

A picture taken on Dec. 28, 2016, in Vertou, western France, shows logos of Facebook.
LOIC VENANCE/Getty Images

On Friday, Facebook announced that it was suspending Cambridge Analytica, a controversial research and data analysis firm, due to unauthorized access and use of Facebook's user data. Facebook's announcement came the day before two explosive reports in the Guardian and the New York Times showed that Facebook had had knowledge of Cambridge Analytica's so-called "unauthorized" use of user data for years and yet had done nothing in response. The story is still developing, and it's not yet clear who should be held responsible for any harms to consumers.

But who is at fault for what Facebook claims is an "unauthorized" use of Facebook user data? To put it more simply: Who should we blame for this? Is Facebook or Cambridge Analytica (or perhaps, another party) responsible? This question is more complicated than it might appear at first glance. Ultimately, responsibility should fall on the shoulders of Cambridge Analytica, Facebook, the U.S. government, and even ourselves as consumers.

Facebook's Friday announcement appears to be an attempt to get ahead of the news that broke on Saturday. (Reporters from the Guardian note that both they and the New York Times had been in contact with Facebook before the articles were published.) Facebook's statement also arrived on the same day as a new lawsuit filed in the U.K. from a professor alleging harms from Cambridge Analytica using his Facebook data to profile him. Even more controversially, Cambridge Analytica has been, at times, linked to the Trump presidential campaign and to foreign interests, potentially in violation of U.S. election laws.

In various statements by Facebook and its executives, the company has claimed that there was no "data breach" involved, but that user data was used in an unauthorized manner. This distinction is important for legal and ethical reasons.

If there had been a data breach, Facebook could be held responsible. State laws on cybersecurity and data breaches would apply to Facebook in that case. It could be forced to pay fines, and the company would have to follow certain obligations, including notifying users and providing remedies that could include identity protection services. The Federal Trade Commission would also likely enforce a fine or other legal consequences on Facebook, as it regularly does for organizations that suffer data breaches. Admitting there

was a data breach would effectively be the equivalent of admitting that Facebook was at least somewhat at fault.

If there was no breach, it would seem to follow that data was accessed with permission. However, Facebook has stated that Cambridge Analytica's access of Facebook user data was "unauthorized." This is likely because admitting that it allowed Cambridge Analytica to access the data could also open Facebook to liability. In response to Facebook's statements, Cambridge Analytica has claimed that it only accessed and used data in authorized ways. This distinction matters because lawmakers will likely be looking for someone to blame for whatever privacy harms were caused by Cambridge Analytica's data profiling. If Cambridge Analytica was not authorized to use Facebook's data, the blame would likely fall solely or mostly on Cambridge Analytica. If Facebook authorized Cambridge Analytica's use of data, that would mean at least some of the blame would be allocated to Facebook.

By claiming that Cambridge Analytica's data use was both not a breach and yet also unauthorized, Facebook is making a shrewd move that may help the company avoid or ameliorate some liability. However, it's likely that even Facebook would admit that it is somewhat at fault here.

Facebook's core defense rests on the fact that Facebook did not directly transfer user data to Cambridge Analytica. Rather, it appears that Aleksandr Kogan, who wore dual hats as a psychology researcher with Cambridge University and as an entrepreneur, collected the data through a third-party app on the Facebook platform, using Facebook's API under the auspices of being an academic. He then sold or transferred the data to Cambridge Analytica. This, in effect, is a failure in what privacy expert Ann Cavoukian terms "privacy by design." In designing its app developer tools and permissions, Facebook should have created more protections for user privacy and taken into account the risks of third-party data use. Another way Facebook could have prevented this scandal is giving users more information on how third-party apps use their data and offering more choices to users on how to manage it. Users should be able to understand where their data goes and who has access to it.

To be fair, Facebook faces a difficult battle here. Without user data, advertisers would be less inclined to advertise on Facebook. The site's features would also be less personalized to users, which would likely make

their experiences less engaging. One could also argue that consumers simply don't care that much about privacy and don't care to learn more. Tech companies like Facebook also have to navigate a confusing array of different, often conflicting privacy laws from different countries.

Governments could also do more to stop this kind of privacy violation. Lawmakers have long been pressuring tech companies to do more to solve a wide variety of problems, including harassment, privacy violations, media manipulation, and election interference. These pressures have intensified in the wake of the 2016 election, as exemplified by the tense Senate tech hearings last fall. In response to this scandal, policymakers, including U.S. Sen. Amy Klobuchar and Massachusetts Attorney General Maura Healey, are now calling for investigations into Facebook and Cambridge Analytica. Some, including Rep. Adam Schiff, the ranking member of the House Intelligence Committee, are even calling for Facebook CEO Mark Zuckerberg to testify before Congress. However, blaming Facebook and other tech companies for privacy harms is not effective if the government doesn't create consistent, actionable standards—both rights and regulations for companies.

Ultimately, some responsibility should also fall to us, as consumers. We have created the privacy environment that allows for these violations to happen. We freely give up our data to various apps, websites, and companies. In return, we reap the benefits of many new technologies, including technologies that rely on use of personal data. You can blame Cambridge Analytica for using your data, or Facebook for collecting your data, or the government for not regulating either. But if the public really cares about preventing this kind of privacy violation, we need to change our social understanding of privacy and how data should be collected and used. Otherwise, we should stop being surprised when our most personal information is inevitably misused.

Read more from Slate on Cambridge Analytica.

Cambridge Analytica Facebook Social Media