



Do you trust Facebook to protect your privacy?

Stephen Loiaconi

March 26, 2018

A number of Facebook users are changing their status with the social media giant from "It's Complicated" to "Separated" after learning the company mishandled user data and shared it with third-party developers.

For any public company, trust is its currency. The latest revelations of a massive user privacy breach at Facebook have raised new questions about whether the company can and should be trusted to responsibly manage the personal data of its more than 2.1 billion users.

#DeleteFacebook began trending last week after reports that Facebook allowed the data-mining firm Cambridge Analytica to improperly access the personal data of as many as 50 million users. According to admissions by Cambridge Analytica, the data was used to develop psychographic profiles to help political campaigns target voters.

In the aftermath of these revelations, Facebook CEO Mark Zuckerberg has gone on a charm offensive, speaking with reporters, apologizing for mishandling user data and promising to do better in the future.

On Sunday, Zuckerberg took out a full-page ad in multiple U.S. newspapers that read, "We have a responsibility to protect your information. If we can't we don't deserve it."

We have a responsibility
to protect your information.
If we can't, we don't deserve it.

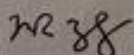
You may have heard about a quiz app built by a university researcher that leaked Facebook data of millions of people in 2014. This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again.

We've already stopped apps like this from getting so much information. Now we're limiting the data apps get when you sign in using Facebook.

We're also investigating every single app that had access to large amounts of data before we fixed this. We expect there are others. And when we find them, we will ban them and tell everyone affected.

Finally, we'll remind you which apps you've given access to your information -- so you can shut off the ones you don't want anymore.

Thank you for believing in this community. I promise to do better for you.



Mark Zuckerberg



The ad referred to the Cambridge Analytica operation and the actions of a "university researcher," Aleksandr Kogan, who developed a quiz app in 2014 on behalf of Cambridge

Analytica. Under Facebook's policy at the time, Kogan was able to pay for a feature called "friends permission." That allowed him to harvest the data of 270,000 quiz-takers, who gave explicit consent to use their data, as well as the data that could be gleaned from their friend networks.

In his ad, Zuckerberg admitted that Kogan's app was not the only one that trawled large amounts of user information. "We expect there are others. And when we find them, we will ban them and tell everyone affected," Zuckerberg said. He concluded, "Thank you for believing in this community. I promise to do better for you."

Some have taken note of the CEO's apology and applauded the company for taking steps to make its data-sharing policies more transparent. Zuckerberg and other executives at Facebook have published notices explaining steps they're taking to crack down on platform abuses as well as their efforts to make privacy settings more user-friendly.

Others have pointed to the fact that Facebook's business model is based on monetizing user data.

"Facebook says we don't sell your data, but they certainly provide access to it," observed Michelle De Mooy, director of the privacy and data project at the Center for Democracy and Technology.

Moreover, Facebook acknowledged that it knew about Cambridge Analytica's questionable contract with Kogan in 2015. At that time, they suspended Kogan and asked him to confirm that he had deleted the user data. According to reports, that user data remained accessible to Cambridge Analytica for years.

"Facebook has been dragged, seemingly kicking and screaming into being more transparent," said Dave Levine, a fellow at the Center for Internet and Society at Stanford University.

"Facebook has not done nearly as much as it could, simply by way of explanation to the public about its behaviors, about how your information or posts are curated, about what kind of data it collects and how it shares it."

The Cambridge Analytica breach is only the latest example of the company's opacity and delayed response to public outcry. Facebook has been at the center of the fake news controversy and spreading misinformation during the 2016 election. The company has been called before Congress over their role in facilitating Russian election interference and online terrorist recruitment. And the company finally acknowledged and changed their newsfeed policy after being caught suppressing conservative content.

Each scandal has temporarily hurt Facebook, but the latest scandal over violating users' privacy could be the one that tips the scales and imposes real costs and consequences on the social media giant.

"Ultimately the problem here is one of trust," explained Julian Sanchez, privacy and technology fellow at the Cato Institute. If users no longer believe the company is responsibly handling their information or feel they cannot understand the company's policies for sharing their data, Zuckerberg's apologies will be "too little, too late," Sanchez noted.

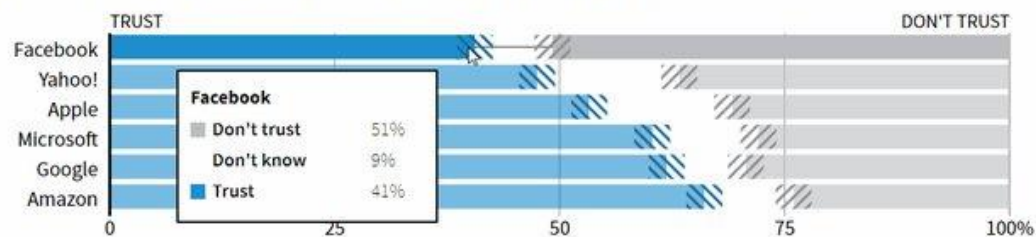
"Once that's burned, once people don't have a sense of trust, I don't know if the specific policy changes will help much," he continued. "Even if they really are making genuine improvements, as it appears they are, once that trust is gone, it's hard to get back."

In a new poll conducted in the days after the data sharing scandal erupted, [Reuters/Ipsos](#) found that the majority of respondents do not trust Facebook to handle their data.

Who trusts Facebook?

When it comes to protecting their information, more people trust Apple, Google, Amazon, Microsoft and Yahoo! than those who trust social media giant Facebook.

HOW MUCH, IF AT ALL, DO YOU TRUST THESE COMPANIES TO OBEY LAWS THAT PROTECT YOUR PERSONAL INFORMATION?



Note: The poll was conducted between March 21-23, and has a sample size of 2,237 respondents. The credibility interval is 2 percentage points.

Source: Reuters/Ipsos public opinion poll

By Travis Hartman | REUTERS GRAPHICS

Facebook was deemed the least trustworthy when it came to obeying laws that protect American's personal information when compared to other companies that gather user data like Apple, Google, Amazon, Microsoft and Yahoo.

"Maybe the poll is new, but the sentiment is not," De Mooy explained. The reason, she said, is that social media platforms "are designed for opacity," intentionally making it harder for users to understand and make informed decisions about their data.

Facebook and other companies that rely on selling access to user data have had to walk a thin line between protecting their users' data and monetizing it. Consistently over recent years, polls have shown that even as users sign up and sign away some of the rights to their data, they are wary of how that information is being used.

Periodically, this concern has translated into relatively short-lived calls for people to deactivate their Facebook accounts, but it is not clear that those efforts have caused the company to fundamentally change how it operates.

"If a few hundred-thousand people delete their Facebook accounts that will have a marginal impact on their bottom line," Levine noted. "However if there is a reputational hit at the trust

level, which is what Facebook needs to maintain in order to be a viable business, that cumulatively could create problems."

In recent weeks, Facebook has taken a significant hit with the markets valuing the breach of privacy and trust in the tens of billions. Since the story broke earlier this month, Facebook's stock has plunged more than 15 percent in a selling spree that has cost the company over \$75 billion in market value.

Facebook could also be facing even more costs as the consumer protection watchdogs at the Federal Trade Commission (FTC) announced on Monday that they had opened a non-public investigation into Facebook's privacy and data use policies based on the reports about the company's relationship with Cambridge Analytica.

Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices

SHARE THIS PAGE



FOR RELEASE

March 26, 2018

TAGS: [Technology](#) | [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#)

Tom Pahl, Acting Director of the Federal Trade Commission's Bureau of Consumer Protection, issued the following statement regarding reported concerns about Facebook's privacy practices:

"The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices."

The Federal Trade Commission works to promote competition, and [protect and educate consumers](#). You can [learn more about consumer topics](#) and [file a consumer complaint online](#) or by calling 1-877-FTC-HELP (382-4357). Like the FTC on [Facebook](#), follow us on [Twitter](#), read our blogs and [subscribe to press releases](#) for the latest FTC news and resources.

CONTACT INFORMATION

MEDIA CONTACT:

[Peter Kaplan](#)

FTC Office of Public Affairs

202-326-2334

The FTC already brought charges against Facebook in 2011 for what it termed "deceptive privacy claims." At the time, Facebook reached a settlement with the FTC and signed a consent

decree which, among other things, required the company to obtain a user's explicit consent before allowing third parties to access their data. Moreover, the agreement required Facebook to inform users if they discovered they were unable to protect their data.

"Facebook can look forward to multiple investigations and potentially a whole lot of liability here," former director of the FTC's Bureau of Consumer Protection Jessica Rich told the Washington Post last week. "Depending on how all the facts shake out, Facebook's actions could violate any or all of these provisions, to the tune of many millions of dollars in penalties."

If the FTC finds Facebook in violation of the consent decree, the company could face a \$40,000 fine per violation. It is not clear whether that fine would apply to the alleged 50 million users whose data was shared inappropriately with Cambridge Analytica. In a statement to the Post, a Facebook spokesperson said the company rejects "any suggestion of violation of the consent decree."

De Mooy said she is encouraged by the FTC investigation, emphasizing that "the consent decrees need to be meaningful." However, she worries that regulators simply lack the enforcement authority when it comes to protecting consumer data.

In the United States, consumer data is largely governed by contracts and terms of use agreements between the consumer and the company. This approach is vastly different from the European Union, which will be implementing a new regime of privacy protections, the General Data Protection Regulation, beginning in May.

The new privacy regime will directly impact U.S. tech companies that will be required to be more transparent in informing consumers about their sharing practices in order to get consent. Companies that fail to protect user data can also expect to see millions of dollars in fines.

It is yet to be seen whether U.S. lawmakers, who have traditionally taken a lax approach to regulating internet companies, will take steps to strengthen data privacy protections.