

Facebook: Most users may have had public data 'scraped'

6 April 2018, by Barbara Ortutay



In this April 18, 2017, file photo, conference workers speak in front of a demo booth at Facebook's annual F8 developer conference, in San Jose, Calif. Facebook CEO Mark Zuckerberg will testify before Congress next week as authorities investigate allegations that the political data-mining firm Cambridge Analytica inappropriately accessed data on millions of Facebook users to influence elections. (AP Photo/Noah Berger, File)

Facebook's acknowledgement that most of its 2.2 billion members have probably had their personal data scraped by "malicious actors" is the latest example of the social network's failure to protect its users' data.

Not to mention its apparent inability to even identify the problem until the company was already embroiled in scandal.

CEO Mark Zuckerberg told reporters Wednesday that Facebook is shutting down a feature that let people search for Facebook users by phone number or email address. Although that was useful for people who wanted to find others on Facebook, it turns out that unscrupulous types also figured out years ago that they could use it to identify individuals and collect data off their profiles.

The scrapers were at it long enough, Zuckerberg said, that "at some point during the last several years, someone has probably accessed your public information in this way."

The only way to be safe would have been for users to deliberately turn off that search feature several years ago. Facebook had it turned on by default.

"I think Facebook has not been clear enough with how to use its [privacy settings](#)," said Jamie Winterton, director of strategy for Arizona State University's Global Security Initiative. "That, to me, was the failure."



In this Nov. 9, 2017, file photo, Facebook CEO Mark Zuckerberg meets with a group of entrepreneurs and innovators during a round-table discussion at Cortex Innovation Community technology hub in St. Louis. Facebook said Wednesday, April 5, 2018, that it has shut down a feature that let people search for Facebook users if they had their phone number or email address. In a call with reporters on Wednesday, Zuckerberg said the company had tried "rate limiting" the searches. This restricted how many searches someone can conduct at one time, based on their device's IP address. But Zuckerberg said this was circumvented by bad actors cycling through multiple IP addresses. (AP Photo/Jeff Roberson, File)

The breach was a stunning admission for a company already reeling from allegations that the political data-mining firm Cambridge Analytica inappropriately accessed data on as many as 87 million Facebook users to influence elections.

Over the past few weeks, the scandal has mushroomed into investigations across continents, including a probe by the U.S. Federal Trade Commission. Zuckerberg himself will be questioned by Congress for the first time on Tuesday.

"The FTC looked the other way for years when consumer groups told them Facebook was violating its 2011 deal to better protect its users. But now the Cambridge Analytica scandal has awoken the FTC from its long digital privacy slumber," said Jeffrey Chester, executive director for the Washington-based privacy nonprofit Center for Digital Democracy.

Neither Zuckerberg nor his company has identified those who carried out the data scraping. Outside experts believe they could have been identity thieves, scam artists or shady data brokers assembling marketing profiles.

Zuckerberg said the company detected the problem in a data-privacy audit started after the Cambridge Analytica disclosures, but didn't say why the company hadn't noticed it—or fixed it—earlier.

headquarters in Menlo Park, Calif. Australian authorities say they are investigating whether Facebook breached the country's privacy law when personal information of more than 300,000 Australian users was obtained by Cambridge Analytica, a Trump-linked political consulting firm, without their authorization. (AP Photo/Marcio Jose Sanchez, File)

Facebook did not immediately respond to a request for comment Thursday on when it discovered the data scraping.

In his call with reporters Wednesday, Zuckerberg said the company had tried "rate limiting" the searches. This restricted how many searches someone can conduct at one time from a particular IP address, a numeric designation that identifies a device's location on the internet. But Zuckerberg said the scrapers circumvented that defense by cycling through multiple IP addresses.

The scraped information was limited to what a user had already chosen to make public—which, depending on a person's privacy settings, could be a lot—as well as what Facebook requires people to share. That includes full name, profile picture and listings of school or workplace networks.

But hackers and scam artists could then use that information—and combine it with other data in circulation—to pull hoaxes on people, plant malware on their computers or commit other mischief.

Having access to such a massive amount of data could also pose national security risks, Winterton said.



In this June 7, 2013, file photo, the Facebook "like" symbol is on display on a sign outside the company's



In this Nov. 9, 2017, file photo, Facebook CEO Mark Zuckerberg meets with a group of entrepreneurs and innovators during a round-table discussion at Cortex Innovation Community technology hub in St. Louis. Facebook said Wednesday, April 5, 2018, that it has shut down a feature that let people search for Facebook users if they had their phone number or email address. In a call with reporters on Wednesday, Zuckerberg said the company had tried "rate limiting" the searches. This restricted how many searches someone can conduct at one time, based on their device's IP address. But Zuckerberg said this was circumvented by bad actors cycling through multiple IP addresses. (AP Photo/Jeff Roberson, File)

A foreign entity could conceivably use such information to influence elections or stir up discord—exactly what Russia is alleged to have done, using Facebook and other social media, in the 2016 presidential elections.

Privacy advocates have long been critical of Facebook's penchant for pushing people to share more and more information, often through pro-sharing default options.

While the company offers detailed privacy controls—users can turn off ad targeting, for example, or face recognition, and post updates that no one else sees—many people never change their settings, and often don't even know how to.

The [company](#) has tried to simplify its settings multiple times over the years, most recently this week.

Winterton said that for individual Facebook users, worrying about this data scraping won't do much good—after all, the [data](#) is already out there. But she said it might be a good time to "reflect on what we are sharing and how we are sharing it and whether we need to."



In this Jun 7, 2013, file photo, the Facebook "like" symbol is illuminated on a sign outside the company's headquarters in Menlo Park, Calif. Australian authorities say they are investigating whether Facebook breached the country's privacy law when personal information of more than 300,000 Australian users was obtained by Cambridge Analytica, a Trump-linked political consulting firm, without their authorization. (AP Photo/Marcio Jose Sanchez, File)

"Just because someone asks us information, it doesn't mean we have to give it to them if we are not comfortable," she said.

She added that while she no longer has a Facebook account, when she did she put her birth year as 1912 and her hometown as Kuala Lumpur, Malaysia. Neither is true.

© 2018 The Associated Press. All rights reserved.

APA citation: Facebook: Most users may have had public data 'scraped' (2018, April 6) retrieved 29 November 2020 from <https://phys.org/news/2018-04-facebook-users.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.