BUSINESS INSIDER

Facebook may have broken the law by harvesting 1.5 million users' email contacts, experts say

Rob Price

April 18, 2019

Facebook harvested 1.5 million users' email contact data without their consent, and experts say that in doing so the company may have violated American and European Union laws.

On Wednesday, Business Insider revealed that the social network had since May 2016 been scraping some new users' email contact books after asking for their email passwords to "verify" their accounts. About 1.5 million users ultimately had their data taken without permission; Facebook said this was done "unintentionally" and it is now deleting the data.

Experts who spoke with Business Insider on Thursday said that they believed Facebook's actions had potentially violated multiple laws including a US Federal Trade Commission (FTC) consent decree; the EU General Data Protection Regulation (GDPR), the European Union's data-privacy regulation; and while there would likely be a strong defense for Facebook, perhaps even the Computer Fraud and Abuse Act (CFAA), a US criminal statute involving computer fraud and abuse.

If their theories are accurate, and regulators ultimately decide to take action against Facebook over the issue, then it could further exacerbate the legal headaches plaguing the company, which has been battling scandals on multiple fronts for the past two years — from Cambridge Analytica's misappropriation of tens of millions of users' data to the social network's role spreading hate speech that fueled genocide in Myanmar.

Democratic Senator Mark Warner, the vice chair of the Senate Intelligence Committee, said in an email: "These latest revelations are very disturbing and, according to a number of experts, even raise the prospect that Facebook engineers may have violated federal laws concerning unauthorized access. Facebook continually attributes these mistakes to simple errors; even in the most charitable reading, these continual errors seem to indicate an engineering and product development culture that prioritizes growth and profit above privacy or user security."

A Facebook spokesperson declined to comment.

Facebook is already under investigation by the FTC

Since 2011, Facebook has been subject to a consent decree by the FTCafter it settled charges that alleged it had misled users on privacy issues. The FTC is now investigating Facebook over its subsequent privacy practices, namely the Cambridge Analytica scandal. The FTC is inquiring whether the incident violated the 2011 consent decree and is reportedly close to negotiating a settlement with Facebook that may be in the billions of dollars.

Ashkan Soltani, the former chief technologist for the FTC, said he believed Facebook's actions with users' email contacts may itself have broken the terms of the consent decree if it was using the data. "In my opinion, Facebook's collection and use of users' address books would be another clear violation of the Consent decree and merit an investigation," he said.

"The FTC enforces unfair and deceptive trade practices. On its own, downloading and using users' address books under a deceptive pretext of 'security' would constitute a deceptive practice, even IF the company wasn't under order," he said, speaking in the abstract.

Dina Srinivasan, a Yale Law graduate who recently wrote a paper called "The Antitrust Case Against Facebook," said that the company's behavior was potentially illegal "on the grounds that Facebook was deceiving consumers when it came to their data and privacy. This can be a violation of 3 things. (1) Federal antitrust laws. (2) Unfair competition laws which every state has a version of. (3) The FTC consent decree."

That said, it's not yet clear whether the FTC will ultimately attempt to take any action against Facebook on this issue, and a spokesperson for the organization didn't respond to a request for comment.

"There are so many different potential violations at this point that I don't know that FTC will investigate this latest ... particularly because it's under a lot of pressure to act on the Cambridge Analytica [incident]," said Sally Hubbard, the director of enforcement strategy at the Open Markets Institute, a research and advocacy group that focuses on issues around corporate power.

She said that even if this did constitute a violation, it would be difficult to investigate. "Once there's a revised consent decree in place, it will be hard for the FTC to go back and investigate any misconduct that came before it (depending on the terms of the negotiated agreement settling the claims — it likely will resolve all liability for violations up to the date it's agreed to)."

The Silicon Valley firm could face trouble in Europe too

In May 2018, the European Union started enforcing GDPR, its tough new data-protection legislation. Facebook hasn't yet said if any of the affected users signed up in Europe after that date, but it seems extremely likely — in which case some believe Facebook may have fallen afoul of GDPR.

"It is especially problematic because it was not just data of the user being verified that was ... processed, but the personal data of their contacts too," Michael Veale, a London-based data-protection researcher and Alan Turing institute fellow, said in an email.

"It might just have been 1.5m users that were directly affected, but considering the number of unique emails that were harvested and the network information linking them, the total number of individuals affected is likely in the hundreds of millions," he added.

He suggested there may have been multiple breaches of the law, including not informing users and processing people's data for advertising purposes without informing them. "This could be construed as a general security breach, as Facebook were not aware their system was effectively compromised," he said.

The Irish Data Protection Commission, which is responsible for regulating Facebook's data practices in the EU under GDPR, said it's now in contact with Facebook over the issue and is considering its next move.

"We are currently engaging with Facebook on this issue and once we receive further information we will decide what steps to take," Graham Doyle, the head of communications at the Irish Data Protection Commission, said.

The question of intent

Julian Sanchez, a senior fellow at the Cato Institute, discussed the possibility that Facebook had potentially violated the Computer Fraud and Abuse Act — which would veer into criminal territory.

"It's an offense under 18 USC 1030 to, among other things, intentionally exceed authorized access to a protected computer. A 'protected computer' is, for practical purposes, any computer connected to the Internet," he said. "So with respect to Facebook's access to users' e-mail contacts, the relevant questions are whether there's any viable argument that it was 'authorized,' which seems like a very hard sell when it's represented as being specifically for the purpose of authentication, and if not, whether the access in excess of authorization was intentional."

He added: "If we were talking about a rapidly-corrected coding mistake that had removed language about scraping the user's contacts, you'd have a plausible case for saying this was access in excess of authorization, but not intentional. But that becomes more difficult to buy the longer they were doing it."

Facebook said that the action was purely unintentional — that it previously notified users it would be accessing their contacts, but a change inadvertently stripped that warning out. Such an argument would be a defense under the CFAA.

"Can they plead incompetence? In principle, though boy is that embarrassing," Sanchez said. "You'd need to look through internal correspondence to see whether anyone noticed the issue and Facebook decided not to fix it."