Luxury Daily®

The News and Intelligence You Need on Luxury

LEGAL AND PRIVACY

Facebook makes privacy push following FTC fine

July 29, 2019

Facebook founder Mark Zuckerberg. Image credit: Facebook

By SARAH JONES

Tech company Facebook is rolling out a new privacy framework after being hit with a record $5 billion fine from the Federal Trade Commission.

Subscribe to Luxury Daily
Plus: Just released State of Luxury 2019
Save $246

As part of its settlement with the FTC, Facebook has agreed to launch more stringent data privacy policies within its organization, including setting up more oversight within its leadership. Facebook has recently announced its vision for more privacy on its platforms, but this FTC-ordered plan is on a bigger organization-wide scale than earlier efforts.

"I hope that the settlement and fines from the FTC will finally be Facebook's wakeup call," said Dan Goldstein, president and owner of Page 1 Solutions, Lakewood, CO. "Zuckerberg previously announced that Facebook is pivoting to a privacy-focused platform, and now it has two major motivations to do so.

"If earning back users' trust, restoring its public image and staying competitive with other social media platforms is the carrot of a more privacy-focused Facebook, the federal government just offered a pretty big stick if Facebook fails to deliver on its promise," he said.

Mr. Goldstein is not affiliated with Facebook, but agreed to comment as an industry expert. Facebook was reached for comment.

Privacy plan

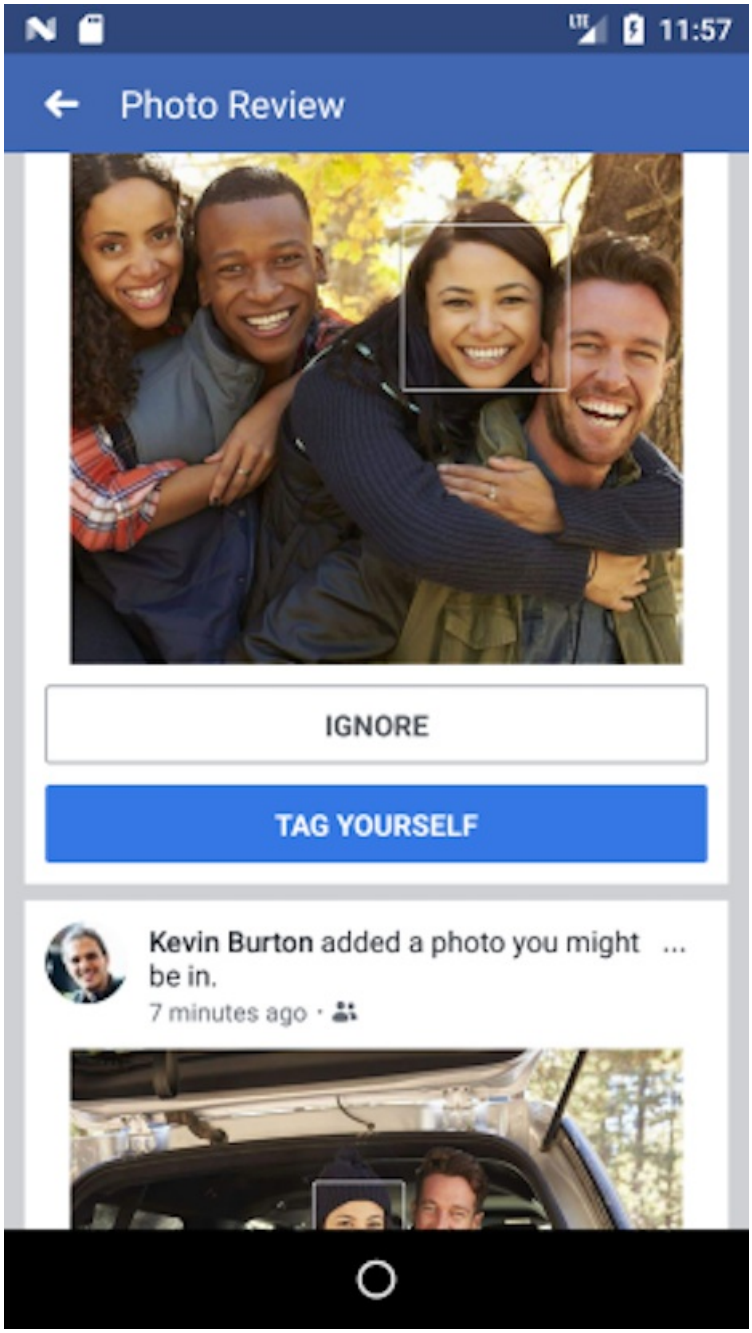
The FTC's case against Facebook is centered on the claim that the social network broke a 2012 settlement order from the commission. The earlier settlement ordered Facebook to not mislead consumers about the amount of control they have over their data and the level to which their information is shared.

Facebook is said to have enabled third-party applications to access information about users' friends, even if those friends did not consent. The FTC also alleged that after the settlement order in 2012, Facebook deleted a portion of its privacy disclosure that included a disclaimer that information could be shared with apps that friends use.

The FTC also notes that while Facebook said it would stop the practice of allowing developers access to the data

about users' friends in 2014, it did not actually cease sharing until 2018.

Another aspect of the case revolves around facial recognition. The social network enables tag suggestions as the default, and the FTC says it made it seem as though users needed to have the setting enabled for their accounts.



Facebook's facial recognition feature. Image courtesy of Facebook

The FTC also claims Facebook collected phone numbers under the guise of a security feature, but used them for advertising purposes.

As part of Facebook's settlement announced on July 24, it will have to pay a $5 billion fine. This is about 20 times larger than any privacy-related fine that has been issued worldwide, and is the greatest amount that a company has had to pay in an FTC violation.

Facebook's revenues totaled $55.8 billion in 2018.

Similarly to the 2012 agreement, the settlement includes an order of steps that must be taken to improve Facebook's privacy protections, which covers Facebook as well as Instagram and WhatsApp.

Per the FTC, Facebook is now prohibited from using phone numbers that it received for security for advertising. It is also banned from asking for passwords to email services when consumers sign up for its platforms, and it needs to encrypt all user passwords.

Facebook is also being told to have more oversight of its third-party developers and be clearer with consumers about

its use of facial recognition.

The order establishes a committee on Facebook's board that will oversee privacy, intending to extend the decision-making beyond CEO Mark Zuckerberg.

This portion of the board will be independent, and will be nominated by an unaffiliated committee. Once part of the board, these committee members can only be fired by a supermajority vote of the board.

The board's privacy committee will be in charge of approving candidates for a new compliance officer role. These individuals and Mr. Zuckerberg will separately report to the FTC each quarter and year about the company's compliance with the FTC's mandate.

Compliance officers can only be fired by the privacy committee, placing them independent of Facebook's executive oversight.

Facebook's privacy policies will also be overseen by an external assessor.

When Facebook develops new software, it will need to document each decision it makes about user privacy.

Additionally, if data from at least 500 users is compromised, the company will need to report that to the FTC and to the assessor within 30 days.

Facebook statement from Mark Zuckerberg

"Over the past year we've made large strides on privacy," Mr. Zuckerberg said in a statement. "We've given people more control over their data, closed down apps and applied more resources to protecting people's information.

"But even measured against these changes, the privacy program we are building will be a step change in terms of how we handle data," he said. "We will be more robust in ensuring that we identify, assess and mitigate privacy risk.

"We will adopt new approaches to more thoroughly document the decisions we make and monitor their impact. And we will introduce more technical controls to better automate privacy safeguards."

Data responsibility
Regulatory commissions are getting serious about consumers' data privacy.

Hospitality group Marriott International is facing potential fines from the U.K. Information Commissioner's Office (ICO) tied to the data breach in its Starwood Hotels systems.

ICO announced an intent to fine Marriott 99.2 million pounds, or about $123.7 million, for infringing the E.U.'s GDPR regulations. The ICO's decision is not final, and Marriott intends to fight against the fines by presenting its side to the authority (see story).

"Be careful. Consumers are more conscious about their data security and online privacy than ever before, and lawmakers are starting to take notice," Mr. Goldstein said. "No business wants to weather the storm of bad PR that Facebook has experienced over the last year-plus; very, very few could afford the combination of bad press and, now, financial blows.

"So, if your business handles user data, know the rules and laws about how you can use it," he said. "This means reading up on state laws based on where you do business, as well as knowing international regulations like GDPR."

For technology companies, data privacy means a delicate dance between serving consumers and helping marketers.

Technology giant Apple is continuing its pro-privacy crusade, but its latest features may alienate many developers and advertisers.

With Apple's forthcoming iOS 13, announced during its Worldwide Developers Conference on June 3, it will be easier than ever for consumers to protect their personal information and prevent third parties from exploiting user data. This places Apple in direct opposition to technology companies Google and Facebook, who have drawn user and government scrutiny over their use of consumer data (see story).

As Facebook also makes a privacy push, its own advertisers may need to adjust.

"Savvy advertisers already know how to navigate changes to categories of data available in Facebook Ads Manager," Mr. Goldstein said. "As a result, advertisers must take it on themselves to understand their audience and create ads that align with what they know about their target consumers.

"Generally, I suspect that Facebook will still provide overall demographic information that doesn't compromise users' privacy," he said. "Experienced advertisers will still be able to create effective ads with this type of data."

© 2020 Napean LLC. All rights reserved.

Luxury Daily is published each business day. Thank you for reading us. Your feedback is welcome.