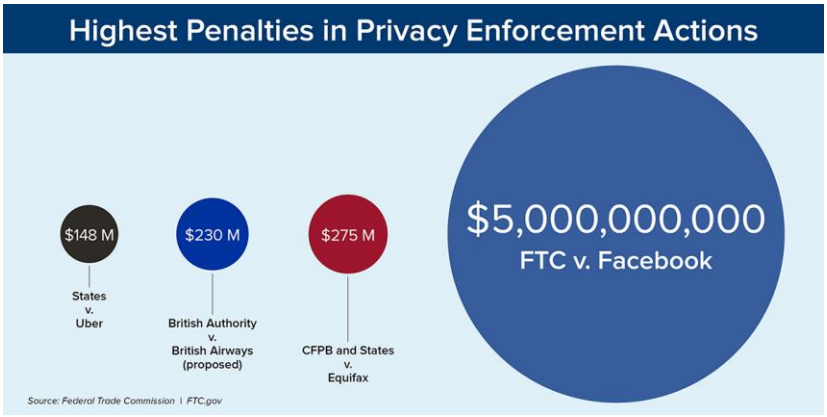
FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook

FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency

NOTE: The FTC hosted an IN-PERSON press conference at FTC Headquarters, 600 Pennsylvania Ave, NW, Washington D.C., at 11 am ET TODAY (July 24). Watch archival video of the press conference.

Participants included: FTC Chairman Joe Simons, FTC Commissioners Noah Joshua Phillips and Christine S. Wilson, and Gustav W. Eyler, Director of the Department of Justice Civil Division's Consumer Protection Branch.

Facebook, Inc. will pay a record-breaking $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle Federal Trade Commission charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.



The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide. It is one of the largest penalties ever assessed by the U.S. government for any violation.

The settlement order announced today also imposes unprecedented new restrictions on Facebook's business operations and creates multiple channels of compliance. The order requires Facebook to restructure its approach to privacy from the corporate board-level down, and establishes strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy, and that those decisions are subject to meaningful oversight.

"Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers' choices," said FTC Chairman Joe Simons. "The magnitude of the $5 billion penalty and sweeping conduct relief are unprecedented in the history of the FTC. The relief is designed not only to punish future violations but, more importantly, to change Facebook's entire privacy culture to decrease the likelihood of continued violations. The Commission takes consumer privacy seriously, and will enforce FTC orders to the fullest extent of the law."

"The Department of Justice is committed to protecting consumer data privacy and ensuring that social media companies like Facebook do not mislead individuals about the use of their personal information," said Assistant Attorney General Jody Hunt for the Department of Justice's Civil Division. "This settlement's historic penalty and compliance terms will benefit American consumers, and the Department expects Facebook to treat its privacy obligations with the utmost seriousness."

More than 185 million people in the United States and Canada use Facebook on a daily basis. Facebook monetizes user information through targeted advertising, which generated most of the company's $55.8 billion in revenues in 2018. To encourage users to share information on its platform, Facebook promises users they can control the privacy of their information through Facebook's privacy settings.

Following a yearlong investigation by the FTC, the Department of Justice will file a complaint on behalf of the Commission alleging that Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of its 2012 FTC order. These tactics allowed the company to share users' personal information with third-party apps that were downloaded by the user's Facebook "friends." The FTC alleges that many users were unaware that Facebook was sharing such information, and therefore did not take the steps needed to opt-out of sharing.

In addition, the FTC alleges that Facebook took inadequate steps to deal with apps that it knew were violating its platform policies.

In a related, but separate development, the FTC also announced today separate law enforcement actions against data analytics company Cambridge Analytica, its former Chief Executive Officer Alexander Nix, and Aleksandr Kogan, an app developer who worked with the company, alleging they used false and deceptive tactics to harvest personal information from millions of Facebook users. Kogan and Nix have agreed to a settlement with the FTC that will restrict how they conduct any business in the future.

New Facebook Order Requirements

To prevent Facebook from deceiving its users about privacy in the future, the FTC's new 20-year settlement order overhauls the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance.

The order creates greater accountability at the board of directors level. It establishes an independent privacy committee of Facebook's board of directors, removing unfettered control by Facebook's CEO Mark Zuckerberg over decisions affecting user privacy. Members of the privacy committee must be independent and will be appointed by an independent nominating committee. Members can only be fired by a supermajority of the Facebook board of directors.

The order also improves accountability at the individual level. Facebook will be required to designate compliance officers who will be responsible for Facebook's privacy program. These compliance officers will be subject to the approval of the new board privacy committee and can be removed only by that committee—not by Facebook's CEO or Facebook employees. Facebook CEO Mark Zuckerberg and designated compliance officers must independently submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order. Any false certification will subject them to individual civil and criminal penalties.

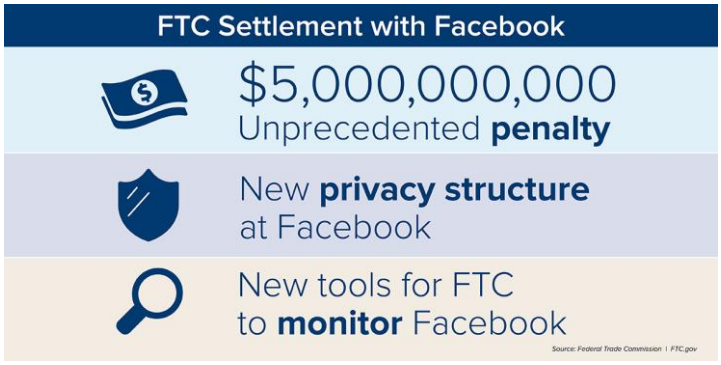
The order also strengthens external oversight of Facebook. The order enhances the independent third-party assessor's ability to evaluate the effectiveness of Facebook's privacy program and identify any gaps. The assessor's biennial assessments of Facebook's privacy program must be based on the assessor's independent fact-gathering, sampling, and testing, and must not rely primarily on assertions or attestations by Facebook management. The order prohibits the company from making any misrepresentations to the assessor, who can be approved or removed by the FTC. Importantly, the independent assessor will be required to report directly to the

new privacy board committee on a quarterly basis. The order also authorizes the FTC to use the discovery tools provided by the Federal Rules of Civil Procedure to monitor Facebook's compliance with the order.

As part of Facebook's order-mandated privacy program, which covers WhatsApp and Instagram, Facebook must conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy. The designated compliance officers must generate a quarterly privacy review report, which they must share with the CEO and the independent assessor, as well as with the FTC upon request by the agency. The order also requires Facebook to document incidents when data of 500 or more users has been compromised and its efforts to address such an incident, and deliver this documentation to the Commission and the assessor within 30 days of the company's discovery of the incident.

Additionally, the order imposes significant new privacy requirements, including the following:

- Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data;
- Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
- Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
- Facebook must establish, implement, and maintain a comprehensive data security program;
- Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
- Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services.



Alleged Violations of 2012 Order

The settlement stems from alleged violations of the FTC's 2012 settlement order with Facebook. Among other things, the 2012 order prohibited Facebook from making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information, such as names and dates of birth, with third parties. It also required Facebook to maintain a reasonable privacy program that safeguards the privacy and confidentiality of user information.

The FTC alleges that Facebook violated the 2012 order by deceiving its users when the company shared the data of users' Facebook friends with third-party app developers, even when those friends had set more restrictive privacy settings.

In May 2012, Facebook added a disclosure to its central "Privacy Settings" page that information shared with a user's Facebook friends could also be shared with the apps used by those friends. The FTC alleges that four months after the 2012 order was finalized in August 2012, Facebook removed this disclosure from the central

“Privacy Settings” page, even though it was still sharing data from an app user’s Facebook friends with third-party developers.

Additionally, Facebook launched various services such as “Privacy Shortcuts” in late 2012 and “Privacy Checkup” in 2014 that claimed to help users better manage their privacy settings. These services, however, allegedly failed to disclose that even when users chose the most restrictive sharing settings, Facebook could still share user information with the apps of the user’s Facebook friends—unless they also went to the “Apps Settings Page” and opted out of such sharing. The FTC alleges the company did not disclose anywhere on the Privacy Settings page or the “About” section of the profile page that Facebook could still share information with third-party developers on the Facebook platform about an app users Facebook friends.

Facebook announced in April 2014 that it would stop allowing third-party developers to collect data about the friends of app users (“affected friend data”). Despite this promise, the company separately told developers that they could collect this data until April 2015 if they already had an existing app on the platform. The FTC alleges that Facebook waited until at least June 2018 to stop sharing user information with third-party apps used by their Facebook friends.

In addition, the complaint alleges that Facebook improperly policed app developers on its platform. The FTC alleges that, as a general practice, Facebook did not screen the developers or their apps before granting them access to vast amounts of user data. Instead, Facebook allegedly only required developers to agree to Facebook’s policies and terms when they registered their app with the Facebook Platform. The company claimed to rely on administering consequences for policy violations that subsequently came to its attention after developers had already received data about Facebook users. The complaint alleges, however, that Facebook did not enforce such policies consistently and often based enforcement of its policies on whether Facebook benefited financially from its arrangements with the developer, and that this practice violated the 2012 order’s requirement to maintain a reasonable privacy program.

The FTC also alleges that Facebook misrepresented users’ ability to control the use of facial recognition technology with their accounts. According to the complaint, Facebook’s data policy, updated in April 2018, was deceptive to tens of millions of users who have Facebook’s facial recognition setting called “Tag Suggestions” because that setting was turned on by default, and the updated data policy suggested that users would need to opt-in to having facial recognition enabled for their accounts.

In addition to these violations of its 2012 order, the FTC alleges that Facebook violated the FTC Act’s prohibition against deceptive practices when it told users it would collect their phone numbers to enable a security feature, but did not disclose that it also used those numbers for advertising purposes.

The Commission vote to refer the complaint and stipulated final order to the Department of Justice for filing was 3-2. The Department will file the complaint and stipulated final order in the U.S. District Court for the District of Columbia. Chairman Simons along with Commissioners Noah Joshua Phillips and Christine S. Wilson issued a statement on this matter. Commissioners Rohit Chopra and Rebecca Kelly Slaughter issued separate statements on this matter.

NOTE: The Commission files a complaint when it has “reason to believe” that the named defendants are violating or are about to violate the law and it appears to the Commission that a proceeding is in the public interest. Stipulated final orders have the force of law when approved and signed by the district court judge.