Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Facebook's $5 Billion Privacy Settlement with the Federal Trade Commission

Chris D. Linebaugh
Legislative Attorney

August 8, 2019

On July 24, 2019, the Federal Trade Commission (FTC) announced a "record-breaking" settlement with the social media company Facebook. The settlement order (2019 Order) is still subject to court approval. But if it is approved, Facebook will be required to pay a $5 billion civil penalty and make several changes to its privacy practices and corporate management structure. In exchange for this relief, the FTC has agreed to resolve any allegations that Facebook or its officers violated an earlier 2012 settlement agreement (the 2012 Order) or otherwise violated the Federal Trade Commission Act (FTC Act).

The FTC has described the 2019 Order as imposing "one of the largest penalties ever assessed by the U.S. government for any violation," stating that the penalty is "almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide." The Commission did not unanimously adopt the 2019 Order, however. Two of the five FTC commissioners dissented, expressing concerns about the order's ability to effectively constrain Facebook's privacy practices. This Sidebar summarizes the 2019 Order and discusses its potential implications for Congress. First, the Sidebar provides background by explaining the legal framework governing the FTC's privacy enforcement and by discussing the 2012 Order that Facebook was alleged to have violated as the basis for the 2019 Order. Next, the Sidebar surveys the 2019 Order, including its allegations and the new obligations it would impose on Facebook. Lastly, the Sidebar discusses some potential considerations for Congress.

Federal Privacy Law and the FTC

As discussed in more detail in this report, there is no single comprehensive federal law governing companies' data privacy practices. Instead, there are a variety of laws that are primarily directed at particular categories of entities, requiring these entities to adopt specific privacy practices. For instance, under the Children's Online Privacy Protection Act (COPPA), operators of online services directed at children (or online operators who knowingly collect children's information) must obtain parental consent

Congressional Research Service
7-5700
www.crs.gov
LSB10338

before collecting, using, or disclosing such information. Other privacy laws include (but are not limited to) the Gramm-Leach Bliley Act (GLBA), which applies to financial institutions, and the Health Insurance Portability and Accountability Act (HIPAA), which applies to certain healthcare entities.

While the FTC has an enforcement role under some of these laws (such as COPPA), its primary enforcement authority comes from more general provisions within the FTC Act. Under Section 5 of the FTC Act, companies and individuals are prohibited from engaging in "unfair or deceptive acts or practices" (UDAPs) "in or affecting commerce." Other than certain exempted companies—such as banks, common carriers, and nonprofits—the FTC is empowered to enforce this UDAP prohibition against all entities. Furthermore, the FTC can bring UDAP enforcement actions against individuals, such as company executives, if it can show that the individual directly participated in the unfair or deceptive acts or practices or "had authority to control them." By bringing UDAP enforcement actions against companies that, like Facebook, are generally not covered by the entity-specific privacy laws discussed above, the FTC has used the UDAP prohibition to fill in some gaps left by these laws. However, its UDAP enforcement notably diverges from enforcement under the entity-specific privacy statutes. Unlike laws like COPAA, the UDAP prohibition does not require companies to affirmatively adopt specific privacy practices, such as getting consumers' consent before collecting or sharing their data. Rather, companies only run afoul of the UDAP prohibition if they act in a way that is "deceptive" or that unjustifiably harms consumers to such an extent that it is "unfair" under the FTC Act.

Along with these substantive limits to UDAP liability, there are also limits to the remedies the FTC may seek. In particular, it may not seek monetary penalties for stand-alone UDAP violations. Instead, for such violations, it is largely limited to obtaining either administrative cease-and-desist orders or equitable relief, such as an injunction or disgorgement, in a federal district court. The agency may, however, seek significant monetary penalties (along with equitable relief) for violating previous FTC orders, including settlement orders. Under the Act and as adjusted for inflation, these penalties may be up to $42,530 per violation. Within these statutory boundaries, however, courts enjoy broad discretion to fashion appropriate remedies. Courts have, nonetheless, articulated limiting principles to guide the exercise of this discretion. For instance, courts have said that injunctive relief (i.e., relief that either prohibits or requires certain conduct) should be designed to prevent future violations that are "likely to recur" and should bear a "reasonable relation to the unlawful practices found to exist." Furthermore, when determining the amount of penalty to impose within the statutory cap, courts have considered factors such as: (1) the good or bad faith of the defendants; (2) the injury to the public; (3) the defendant's ability to pay; (4) the desire to eliminate the benefits derived by a violation; and (5) the necessity of vindicating the authority of the FTC.

2012 Order

With the 2012 Order, Facebook settled FTC claims that the company's privacy practices violated the FTC Act. While the allegations in the FTC's complaint accompanying the 2012 Order concerned several matters, one key issue was how Facebook gave third-party application developers access to user information. According to the FTC, whenever Facebook users downloaded a third-party application on Facebook—such as a game or a birthday reminder application—Facebook's default settings allowed the third-party developer to access not only the users' information but also their friends' information. Moreover, third-party developers were able to access this information even if the users' friends changed their privacy settings so that "Only Friends" or "Friends of Friends" could see their personal information. The FTC maintained that these privacy settings were, consequently, deceptive in violation of the UDAP prohibition.

The 2012 Order did not impose monetary penalties because it alleged stand-alone UDAP violations rather than a violation of an already existing order. However, it did impose several obligations on Facebook. In particular, the 2012 Order prohibited Facebook from misrepresenting "the extent to which it maintains the privacy or security" of users' information. The 2012 Order specified that this broad prohibition includes, among other things, misrepresenting how much users "can control the privacy" of their information, the "steps a consumer must take to implement such controls," and the extent to which the company makes user information available to third parties. Along with prohibiting misrepresentations, the 2012 Order affirmatively required Facebook to obtain users' consent before sharing their information in a manner materially exceeding "the restrictions imposed by a user's privacy setting(s)." Facebook was further obligated to adopt a "comprehensive privacy program" designed to assess privacy risks and to "protect the privacy and confidentiality of [consumers'] information." The order also required an independent third party to audit this privacy program every two years for a twenty-year period.

2019 Order

Allegations

The 2019 Order, if approved by the court, would resolve any claims that Facebook's past actions violated the 2012 Order or violated the FTC Act. While the complaint accompanying the 2019 Order addresses several issues (including Facebook's facial recognition practices and its use of its users' phone numbers that the company ostensibly obtained for security reasons), the allegations primarily focus on Facebook's practices regarding third-party application developers. According to the complaint, Facebook's practices with these developers did not change much after the 2012 Order. Facebook allegedly continued to allow third-party developers to access application users' friends' information, even if those friends changed their privacy settings to "Friends Only" or "Friends of Friends." Facebook at first added a disclaimer on its privacy settings, warning users that their friends could still share their information with third-party applications. However, the company allegedly removed this disclaimer about four months after the 2012 Order became effective. Without this disclaimer, according to the complaint, Facebook violated the 2012 Order's prohibition on misrepresentations because its privacy settings falsely represented that consumers could control the privacy of their data with respect to third parties simply by changing those privacy settings. Beyond Facebook's conduct over its privacy settings, the complaint also alleges that the company made misleading public statements. In 2014, Facebook announced at a conference that it would no longer allow third-party developers to collect data on app users' friends. But, pursuant to the complaint, the company continued to allow some developers to access the information. In particular, Facebook allegedly allowed "more than two dozen developers"—so called "Whitelisted Developers"—to continue to collect such information, in some cases until June 2018. As with Facebook's privacy settings, the complaint alleged these public statements violated the 2012 Order's prohibition on misrepresenting its privacy practices.

In addition to the alleged misrepresentations, the complaint alleges that Facebook failed to adequately implement and maintain a comprehensive privacy program, as required by the 2012 Order. While Facebook required third-party developers to comply with its policies and terms, the complaint alleges that Facebook generally did not screen third-party developers before allowing them to access user data. Instead, the company allegedly only enforced its platform policies after becoming aware of a violation. Moreover, the complaint alleges that even after becoming aware of a violation, the severity of the consequences Facebook imposed depended on the financial benefit that Facebook received from the developer. According to the complaint, these practices conflicted with the 2012 Order's requirement that Facebook implement and maintain a "comprehensive privacy program" designed to assess privacy risks.

Remedies

Along with the $5 billion civil penalty—which, per the Miscellaneous Receipts Statute, will be paid to the Treasurer of the United States and deposited into the U.S. Treasury's "General Fund"—the 2019 Order imposes injunctive relief that requires Facebook to implement certain privacy practices and organizational changes. This relief includes some requirements similar to those in the 2012 Order, as well as some new obligations. Among other things, Facebook:

- May not misrepresent the extent to which it maintains the privacy or security of users' nonpublic information and certain other specified types of information (Covered Information);
- Must notify users and obtain their consent before sharing their Covered Information with third parties in a manner that materially exceeds the restrictions imposed by their privacy settings;
- Must monitor third party developers' compliance with Facebook's platform policies and enforce any violations based solely on factors such as the severity of the violation and history of violations;
- Must implement and maintain a "comprehensive" privacy program; among other things, the privacy program must include annual privacy risk assessments and must implement and document safeguards designed to control for risks identified in the assessments; the privacy program also must be overseen by a designated compliance officer, who is removable only by the independent privacy committee;
- Must select an independent third-party assessor, subject to FTC approval, to conduct biennial assessments of its privacy program;
- Must name a new independent privacy committee made up of independent directors; the committee must meet four times a year to receive briefings on the state of Facebook's privacy program and compliance with the 2019 Order;
- Must submit quarterly certifications to the FTC that Facebook's privacy program complies with the 2019 Order, signed by the CEO and the designated compliance officer.

Arguments of the Commissioners

The 2019 Order was not unanimously adopted by the Commission. Two of the five commissioners—Rohit Chopra and Rebecca Kelly Slaughter—dissented. Both expressed concerns with the effectiveness of the injunctive relief. Commissioner Chopra criticized the injunctive relief as amounting to "documentation requirements, rather than bright line rules." Chopra noted, in particular, that the injunctive relief does "not actually place any substantive limit on Facebook's collection, use, or sharing of personal information," but "allows Facebook to evaluate for itself what level of user privacy is appropriate." Commissioner Slaughter similarly argued the injunctive relief should have imposed more specific privacy limitations, such as restricting exactly when Facebook can collect consumer information and share it with third parties. Along with criticizing the injunctive relief, Commissioners Chopra and Slaughter said that the $5 billion civil penalty was too small. For example, Commissioner Chopra maintained that the amount Facebook unlawfully made through its violations likely was "well above $5 billion," and, in any case, a "civil penalty should *exceed* unjust gains—otherwise we are allowing a defendant to break even or even profit by breaking the law." Chopra further argued that the five factors courts typically consider when imposing civil penalties all support a penalty "beyond the disgorgements of ill-gotten gains." Finally, both commissioners faulted the 2019 Order's treatment of Facebook's officers. Commissioner Chopra criticized the 2019 Order for releasing the chief executive officer Mark Zuckerberg and other executives from personal liability without thoroughly investigating their involvement in the alleged violations. Commissioner Slaughter similarly took issue with the broad liability release and argued that Zuckerberg should have been named in the complaint and the order.

Formatted: Body Text, Space Before: 0 pt, After: 0 pt

The three majority commissioners, however, defended the 2019 Order as "substantially greater" than what the FTC "realistically might have obtained" in court. On the injunctive relief, the commissioners maintained that it was far beyond the typical relief awarded by courts in consumer protection cases. According to the commissioners, even if the FTC prevailed in litigation, a court would not give it "carte blanche" to reorganize Facebook's governance structures and business operations because the FTC would not be able to show that such changes are necessary to comply with the 2012 Order and the FTC Act. Further, the commissioners argued that it was unlikely a court "would have imposed a civil penalty even remotely close" to the $5 billion penalty, given that courts "often depart, dramatically and downwardly," from the maximum allowed under the statute. To illustrate their point, the commissioners cited to a case in which a court awarded $168 million in civil penalties, even though the "maximum theoretical penalty was over $727 billion." Lastly, the majority commissioners defended the 2019 Order's treatment of Zuckerberg and other executives. They maintained that the 2019 Order extinguishes "the ability of Mr. Zuckerberg to make privacy decisions unilaterally" and solves "concrete problems, rather than venting frustration with individuals."

Considerations for Congress

Along with the record-setting penalties and high-profile nature of Facebook's privacy dispute, the 2019 Order highlights the strengths and limitations of the FTC's role as a privacy regulator. On the one hand, the 2019 Order underscores that the UDAP prohibition can be used to impose substantive restraints on companies' privacy practices. In particular, when a company like Facebook makes statements about how it treats consumers' data, departures from those statements can be the basis for liability as a deceptive practice under the FTC Act. Further, the 2019 Order shows that the UDAP violations can result in extensive injunctive relief and—once there is a violation of a previous order—significant monetary penalties. However, the 2019 Order also demonstrates that there are limitations to the FTC Act being used to regulate informational privacy rights. First, unlike the entity-specific privacy statutes previously discussed, such as COPPA, the FTC Act's UDAP prohibition does not require companies to adopt particular privacy practices. Instead, it broadly prohibits conduct that is deceptive or unfair, applying that general standard on a case-by-case basis. As a result, companies whose privacy practices are primarily subject to FTC oversight may be able to use consumer information in ways that might be prohibited if they were covered by one of the more targeted privacy laws. For instance, Facebook's actions were problematic not because it shared consumers' information with third-party applications without their consent, but because it misrepresented this practice to consumers. As a result, the FTC Act is largely a reactive statute as opposed to a proactive one, imposing liability once a company fails to live up to the privacy promises it voluntarily made to consumers. Further, as discussed by the three majority commissioners, the FTC Act's limited focus on deceptive or unfair conduct may cabin the scope of remedial relief that courts will impose (and the FTC can seek) in enforcement actions. To the extent Congress considers whether to enact specific privacy requirements applicable to companies like Facebook, these aspects of FTC's UDAP enforcement, as exemplified in the 2019 Order, may be helpful to keep in mind.

Formatted: Body Text

Formatted: Body Text Char

Formatted: Hyperlink

Formatted: Body Text Char