UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, *Plaintiff*, v. FACEBOOK, INC., *Defendant*.	Civil Action No. 19-2184 (TJK)

MEMORANDUM OPINION

Almost eight years ago, the Federal Trade Commission and Facebook agreed to settle allegations that Facebook's information-sharing and privacy practices violated Section 5 of the Federal Trade Commission Act because they were unfair and deceptive. As part of that agreement, memorialized in an administrative order entered by the FTC, Facebook committed to maintaining a privacy program and to not misrepresenting the privacy protections it afforded its users. But according to the United States, Facebook did not keep its word, and over the next months and years it violated both the FTC Act and the order in many ways. Last year, the parties agreed to settle these fresh allegations about Facebook's privacy practices. Before the Court is their consent motion to enter a proposed stipulated order. Among other things, the order would require Facebook to pay a $5 billion civil money penalty—by far the largest penalty ever won by the United States on behalf of the FTC—and impose injunctive relief in the form of an amended administrative order to be entered by the FTC that would require Facebook to take a variety of additional measures to protect its users' personal information.

In the Court's view, the unscrupulous way in which the United States alleges Facebook violated both the law and the administrative order is stunning. And these allegations, and the

briefs of some amici, call into question the adequacy of laws governing how technology companies that collect and monetize Americans' personal information must treat that information. But those concerns are largely for Congress; they are not relevant here. Mindful of its proper role, and especially considering the deference to which the Executive's enforcement discretion is entitled, the Court will grant the consent motion and enter the order as proposed.

I. Background

A. Facebook

Facebook, Inc. ("Facebook") operates a social-networking service through its website and mobile applications. ECF No. 3 ("Compl.") ¶ 2. Those applications connect Facebook's users, who each create a profile that includes their personal information, with "Friends" who also have Facebook accounts and profiles. *Id*. Through its service, Facebook collects and maintains huge amounts of its users' information. *Id.* As of 2018, Facebook had more than 2.2 billion monthly active users worldwide. *Id*. And over 100 million Americans use Facebook every day to share personal information, such as their name, date of birth, hometown, current city, employer, relationship status, political views, photos of minor children, and membership in health-related and other support groups. *Id.* In addition, Facebook users may install and use applications developed by third parties that allow users to share information with each other. *Id*. The collection and maintenance of its users' personal information is an essential part of Facebook's business model. That model monetizes users' personal information by deploying it for advertising; indeed, almost all of Facebook's revenue comes from advertising. *Id.* ¶ 3.

B. 2012 Consent Agreement and Order

In 2012, the Federal Trade Commission (FTC) filed an administrative complaint alleging that Facebook engaged in unfair and deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a) ("FTC Act"). *See In the Matter of Facebook,*

Inc., Dkt. No. C-4365, 2012 WL 3518628 (F.T.C.) (July 27, 2012) ("2012 Action"). The FTC brought eight counts alleging, among other things, that Facebook misled its users about (1) its privacy settings and privacy policy changes, *see id.* ¶¶ 10–29; (2) how much it shared its users' personal information with third-party application developers; *id.* ¶¶ 30–33; (3) how much it shared its users' personal information with outside advertisers, *see id.* ¶¶ 34–42; (4) the steps it took to verify the security and privacy practices of third-party application developers, *see id.* ¶¶ 43–49; (5) how much it shared its users' personal information, including photos and videos, with third parties after a user deleted its account, *see id.* ¶¶ 50–55; and (6) its compliance with international privacy protocols, *see id.* ¶¶ 56–63.

Facebook and the FTC reached a settlement in August 2012. Compl. ¶ 28. The FTC then issued an order ("2012 Order")—which Facebook's General Counsel signed on the company's behalf—outlining remedial actions Facebook had to take. *See id.* ¶¶ 28–34. Facebook was prohibited from making misrepresentations about the extent to which it maintains the privacy or security of its users' personal information; the extent to which its users can control the privacy of that information, and how they can do so; and the extent to which it makes its users' personal information accessible to third parties. *See id.* ¶ 29. Facebook was also required to establish and maintain "a comprehensive privacy program that [was] reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of [its users' personal] information." *Id.* ¶ 31. Facebook's privacy program was also required to consider reasonably foreseeable risks to users' privacy, and Facebook had to monitor and evaluate the program on an ongoing basis. *See id.* The order expires in July 2032, or 20 years from the date the FTC filed its administrative complaint. *See* 2012 Action at *83.

C. This Action

1. Complaint

The United States now alleges that Facebook violated the 2012 Order by "subvert[ing] users privacy choices to serve its own business interests" in several ways, starting almost immediately after agreeing to comply with the 2012 Order. Compl. ¶ 4. Although Facebook led its users to believe they could restrict who could view their personal information, it allegedly shared that information with third parties without the user's knowledge. *See* Compl. ¶¶ 35–50. For example, Facebook allegedly told its users that they could limit those who could see their posts to just "Friends," when in reality—and without warning to the user—doing so would also allow developers of third-party applications used by their "Friends" to access the post. *See id.* 46–48. Facebook allegedly permitted third-party developers to access these posts even though it was aware of how that practice compromised its users' privacy interests. *See id.* ¶¶ 81–91. And Facebook allegedly continued to allow a subset of third-party developers to access its users' personal formation in this way without their users' knowledge even after it announced, *two different times*, that it would stop doing so. *See id.* ¶¶ 92–100; 106–13. Facebook also allegedly automatically activated certain facial recognition technologies on a subset of about 60 million user accounts and maintained that technology's activation while telling its users that it would only do so if a user requested it. *See id.* ¶¶ 144–54.

The United States also alleges that Facebook's privacy settings and policies compromised its users' privacy in various other ways. For example, Facebook allegedly misled its users through its desktop and mobile interfaces by causing them to default to settings that were not privacy-protective; removing key disclaimers; and making interfaces hard to navigate, especially when it came to users' ability to stop the sharing of their personal information with developers of third-party applications used by their "Friends." *See id.* ¶¶ 51–80. Moreover, Facebook's so-

called "Privacy Checkup," a tool that it represented would allow users to control who had access to their information, allegedly failed to alert users that third-party developers could continue to view their information no matter what settings were selected through the "Privacy Checkup." *See id.* ¶¶ 101–105. And even though Facebook agreed to maintain a reasonable privacy program, it allegedly failed to screen third-party application developers before giving them access to users' information and did not consistently enforce the few policies it had about the protection and use of its users' information when developers violated those policies. *See id.* ¶¶ 114–24. In fact, Facebook's enforcement decisions allegedly "took into account the financial benefit that Facebook considered the developer to offer." *Id.* ¶ 123. Moreover, because of Facebook's deficient controls, the company allegedly still did not know at the time the Complaint was filed how much data it improperly released to third-party application developers, exactly to which developers the data was released, or the purposes for which the developers used it. *See id.* ¶¶ 126–27.

Facebook is also alleged to have misled users about what information it shared with advertisers. Facebook purportedly encouraged users to provide their telephone numbers so that they could protect their accounts with two-factor authentication. *See id.* ¶¶ 128–30. Facebook did not, however, warn these users that it would also use these telephone numbers for advertising purposes. *See id.* ¶¶ 131–43.

Based on this alleged conduct, the Complaint filed by the United States includes five counts accusing Facebook of violating the 2012 Order by misrepresenting to its users how much control they had over their personal information and how much third-party application developers could access that information, *see id.* ¶¶ 155–75, 183–86, and by failing to maintain a reasonable privacy program, *see id.* ¶¶ 176–82. The Complaint also includes one count alleging

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.