July 30, 2019

FTC Imposes Record-Setting $5 Billion Penalty to Resolve Allegations that Facebook Violated User Data Privacy

On July 24, 2019, the Federal Trade Commission ("FTC") announced that Facebook, Inc. ("Facebook" or the "Company") would pay a record-setting penalty in the amount of $5 billion to resolve allegations that it violated a 2012 FTC Order ("the 2012 Order") by misleading Facebook users about how the Company handled user personal data.[1] The Securities and Exchange Commission ("SEC") separately announced a $100 million settlement of allegations that Facebook's public disclosures about the potential for data misuse were misleading in light of its knowledge of misuse by Cambridge Analytica.[2] The settlement highlights the growing risks facing many U.S. companies with respect to innovative uses of data.

Background

According to a complaint filed by the Department of Justice ("DOJ") on behalf of the FTC in U.S. District Court for the District of Columbia (the "Complaint"), Facebook allegedly violated the 2012 Order by using deceptive disclosures and opt-out settings to share user personal data with third-party apps so that the data could be used in advertising.[3] In particular, the Complaint alleges that Facebook users relied on the Company's privacy statements and settings to limit how their information was shared with and used by third parties. However, the Complaint further alleges that the Company improperly shared user data with third-party apps downloaded by users' Facebook friends when users were not aware of this practice. As a result, according to the Complaint, users were allegedly misled. Among other things, the Complaint also alleges that the Company failed to ensure that third-party apps complied with the Company's privacy practices, terms, and conditions and failed to properly vet third-party app developers before allowing them to access Facebook user data. In addition, Facebook allegedly misled users about their ability to control the platform's facial recognition technology through the "Tag Suggestions" setting, which was turned on by default when the Company's privacy policy allegedly suggested that users would need to opt in to enable facial recognition.

In addition to the steep penalty, the FTC's settlement order also imposes significant restrictions on Facebook from a corporate compliance perspective, requiring the Company to substantially revise its privacy program. Among other things, such modifications include:

- Creating an independent Privacy Committee of the Company's Board of Directors.
- Designating independently nominated compliance officers tasked with overseeing Facebook's privacy program; notably, the compliance officers can only be removed by the Privacy Committee.
- Requiring the Company to review new or modified services, products, and practices before implementation and to memorialize decisions regarding user privacy relating to the same.

[1] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, July 24, 2019, *available at* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
[2] Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, July 24, 2019, available at https://www.sec.gov/news/press-release/2019-140.
[3] *United States v. Facebook, Inc.*, 19-cv-2184, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

- Adding additional external oversight of Facebook's privacy program by:
    - allowing an independent third-party assessor to base its biennial review of the Company's privacy program on an independent fact-gathering record, sampling, and testing.
    - enabling the FTC to use discovery mechanisms under the Federal Rules of Civil Procedure to ensure that the Company complies with the order.
- Mandating that Facebook document breaches of user data to the FTC where 500 or more users are affected and provide documentation regarding the breaches to the FTC and independent assessor within 30 days.[4]

In addition to the FTC settlement, Facebook also agreed to enter into a settlement agreement with the SEC over allegations that Facebook's disclosures in public filings about the risks surrounding data misuse were misleading. Facebook disclosed in its risk factors that "our users' data may be improperly accessed, used or disclosed," (emphasis added) despite allegedly knowing for two years that Cambridge Analytica had made allegedly improper use of Facebook data of approximately 57 million users.

Takeaways

These settlements highlight the increasing risk of regulatory actions by U.S. regulators premised on data-sharing, including the SEC's growing focus on public company disclosures regarding privacy and cybersecurity risks. Only last year, the SEC issued its first ever fine against a public company for failing to disclose a data breach—the $35 million settlement with Altaba, formerly known as Yahoo!.

Considerable attention has been paid to European privacy requirements, in particular the General Data Protection Regulation with its potential fines of up to four percent of global revenue. The largest EU fine so far is a £183 million proposed monetary penalty, although numerous investigations into Facebook's practices are still pending in Europe and we may not have seen EU regulators fully flex their new authority. Nonetheless, the U.S. regulators are clearly trying to make the case that U.S. enforcement is more rigorous.

The Facebook FTC fine also reemphasizes the risks that still exist for companies under existing U.S. federal and state privacy laws, especially where a company has entered into a consent settlement. In initial enforcement actions in the privacy and data security area, the FTC generally has no civil penalty authority and is limited to seeking injunctive relief. The settlement of those initial actions, however, typically requires that the company enter into a stipulated FTC order that often imposes broad conduct restrictions on the company for an extended period of time (often 20 years). Once in place, the settlement gives the FTC enormous leverage because the FTC Act grants the FTC direct enforcement authority to seek civil penalties for violation of its orders,[5] and alleged violation of the stipulated settlement order between Facebook and the FTC in 2012 was the main legal basis for the enormous penalty sought and obtained in the Facebook case. The FTC's success in achieving this settlement with Facebook should well caution any company negotiating an FTC settlement in the privacy or data security context – or, indeed, any company dealing with state regulators that may similarly have enhanced penalty authority for violations of its orders – to make sure the company appreciates the risks faced by entering into such settlements and agreeing to such terms.

The settlement also sheds light on the FTC's approach to corporate compliance moving forward. Although at least one privacy group has challenged the settlement as too lenient, the resolution suggests that the Commission may impose significant governance measures on companies. As in the context of DOJ corporate monitorships, such measures could prove to be costly when coupled with the burden of independent oversight, including potential information requests from

[4] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, July 24, 2019.
[5] *See* 15 U.S.C. § 45(l) ($10,000 for each violation).

the FTC to ensure compliance with a settlement order and perhaps, more significantly, the costs related to a company's ability to innovate when constrained by direct oversight – with the potential for even harsher penalties for any further issues.

For more information on the Facebook settlement or to discuss privacy or data security issues generally, please contact a member of our data practice group.