July 26, 2019

FTC Settlement with Facebook Over Privacy Policies Imposes Unprecedented Penalties and Restrictions

Proposed Settlement Requires Facebook to Pay a Record-Breaking $5 Billion Penalty, Modify Its Corporate Governance Structure, and Submit to Third-Party Oversight of Its Privacy Program

SUMMARY

On July 24, 2019, the Federal Trade Commission ("FTC") announced the settlement of its investigation into the privacy practices of Facebook, Inc. ("Facebook") arising from the Cambridge Analytica scandal, in which Cambridge Analytica, a British political consulting firm, as well as other application developers, were permitted to harvest personal information from Facebook users without their consent. The FTC alleged that Facebook deceived users about its data sharing and privacy policies, and that its conduct violated an existing consent order from 2012 that prohibited Facebook from misrepresenting the extent to which users could keep their personal information private. As part of the settlement, Facebook has agreed to pay a record-breaking $5 billion penalty, restructure its privacy program, and submit to independent monitoring of that program by a third party. The proposed settlement order (the "Proposed Order") has been submitted for approval to the U.S. District Court for the District of Columbia and, once approved, would become effective upon the date it is published on the FTC's website as a final order (the "Final Order").

BACKGROUND

In 2012, Facebook entered into a consent decree with the FTC which, among other things, required Facebook to obtain users' express consent to share personal information beyond their established privacy settings and to establish a reasonable privacy program to protect consumers' information.[1]

The FTC's investigation of Facebook's alleged violations of the 2012 consent order began in March 2018, after reports that Facebook's data sharing practices and security policies enabled Cambridge Analytica, a British political consulting firm, to harvest the personal data of 87 million Facebook users without their

permission for purposes of voter profiling and targeting. The data originated from a personality quiz application created by a third-party developer that collected data from Facebook users who installed it as well as those users' Facebook friends, while Facebook allegedly made it difficult for users to find or modify the settings that would have prevented access via a friend's use of a third-party application (which was a practice permitted by Facebook's privacy policy at the time). The third-party developer then transferred the data to Cambridge Analytica. The revelation, three years later, about the data collected by Cambridge Analytica led to widespread public concern about Facebook's privacy practices, and Congressional hearings into Facebook's handling of user data. At those hearings, Mark Zuckerberg, Facebook's CEO, conceded that Facebook had failed in its "basic responsibility of protecting people's information" and advocated a national privacy and data protection regulation in the U.S. based on the protections provided by Europe's new General Data Protection Regulation ("GDPR"), which would "establish a way to hold companies such as Facebook accountable by imposing sanctions when we make mistakes."

According to the complaint filed by the Department of Justice on July 24, 2019 as part of the FTC's settlement (the "Complaint"), Facebook violated the 2012 consent order in connection with the Cambridge Analytica events by, among other things, repeatedly making misleading statements about users' ability to control the privacy of their personal information.[2] For example, Facebook disclosed to users that they could restrict the sharing of their data to limited audiences, such as "Friends Only," without disclosing to those users that selecting "Friends Only" did not prevent Facebook from sharing the users' personal information with third-party applications used by those friends, such as the quiz application involved in the Cambridge Analytica scandal. In addition, the Complaint alleges that Facebook violated its obligation under the consent order to maintain a reasonable privacy program by failing to appropriately screen third-party developers before granting them access to user data. Facebook further allegedly allowed financial considerations to affect its enforcement decisions when third-party developers violated its privacy policies. Finally, separate from the allegations regarding violations of the consent order, the Complaint also alleges that Facebook made other misleading statements about how it used facial recognition technology, users' cell phone numbers and other personal data.

In addition to assessing a $5 billion civil penalty, the Proposed Order has several key components that are addressed in detail in the following paragraphs. As a threshold matter, the Proposed Order enhances the privacy of Facebook users by prohibiting Facebook from making any misrepresentations about how it may collect, utilize or disclose consumers' personal information. Facebook must also, among other things, exercise greater oversight over third-party application developers, obtain consumers' affirmative consent before using facial recognition information and ensure that information deleted by users cannot be accessed later except in limited circumstances. Most notably, the Proposed Order requires that Facebook implement, maintain and document a comprehensive information security and privacy program, including evaluating on an annual basis any internal or external risks associated with the collection or disclosure of user personal information. Additionally, the Proposed Order requires modifications to Facebook's corporate governance

practices to enhance the independence and effectiveness of its privacy program and mandates the use of a third-party assessor to provide ongoing monitoring and oversight of the privacy program.

The $5 billion penalty against Facebook is the largest privacy or data security penalty ever imposed on a company and one of the largest civil penalties ever assessed by the U.S. government for any violation.[3] The size of the fine suggests that future fines sought by the FTC may converge or exceed the scale of penalties that may be imposed under the GDPR, which permits the imposition of a penalty of up to 4% of a company's global annual revenue. In fact, in a joint statement, FTC Chairman Joe Simons and two Commissioners stated, "For purposes of comparison, the [GDPR] is touted as the high-water mark for comprehensive privacy legislation, and the penalty the [FTC] has negotiated is *over 20 times greater* than the largest GDPR fine to date."[4] Moreover, the Complaint and the Proposed Order touch on some of the core issues that GDPR was designed to address: a purpose limitation on the collection of data (the FTC alleged that Facebook collected telephone numbers under the auspices of enhancing security while using that information to target advertisements to those users); data deletion or the "right to be forgotten" (Facebook would be required to delete user data within 30 days of a user deleting data or terminating an account); and the notion of consent that is freely given, specific, informed and unambiguous (the FTC alleged Facebook suggested to users it would use facial recognition "[i]f you have it turned on," while Facebook defaulted to turning it on).

The Proposed Order would overhaul how Facebook makes privacy decisions in the future, requiring that Facebook restructure its approach to privacy from the board-level down, through the management and compliance function. Under the Proposed Order, prior to implementing any new or modified product, service or practice, Facebook must conduct a privacy review with respect to its collection, use or sharing of personal information. If Facebook determines that any new or modified product, service or practice presents a material risk to the privacy, confidentiality or integrity of personal information, it must prepare a written privacy review statement—submitted quarterly to the third-party assessor, discussed further below—describing the types of information involved, the notice to be provided to users, the risks to privacy, confidentiality and integrity, and existing and new safeguards and procedures implemented to control or mitigate these risks.

The Proposed Order also requires that Facebook's board of directors establish a new privacy committee comprised only of independent directors with relevant privacy and corporate compliance expertise. The directors serving on the privacy committee may, with certain exceptions, only be removed from the Facebook board of directors by a two-thirds vote of the outstanding shares of the company. In order to effect this change, Facebook must amend its certificate of incorporation within 180 days of the entry of the settlement order. The Proposed Order mandates that the privacy committee meet at least four times per year and specifies action items for those meetings. Facebook must also designate "compliance officers" who would be responsible for Facebook's privacy program and who could only be removed by the privacy

committee. These designated compliance officers, along with Mark Zuckerberg, must certify to the FTC, on behalf of Facebook, on a quarterly basis that the company is in compliance with the Proposed Order.

The Proposed Order imposes significant external oversight conditions, including the appointment of an independent third-party "assessor," who would be subject to approval and removal by the FTC. To ensure adequate monitoring of Facebook's compliance, the Proposed Order requires that Facebook provide the assessor, the FTC and the Department of Justice with access to all documentation of Facebook's privacy decisions, including quarterly privacy review reports and any incident reports. Moreover, Facebook cannot withhold any documents from the assessor on the basis of a claim of proprietary or trade secrets, work product protection, attorney-client privilege or any similar claim. The assessor must meet with the privacy committee on a quarterly basis, both with and without the presence of management, to discuss the state of Facebook's privacy program and related risks and must provide the FTC with an independent biennial assessment of Facebook's data privacy program that does not rely on any assertions or attestations by management.

The Proposed Order requires that Facebook submit a report to the FTC within 30 days of Facebook verifying or confirming that the personal information of 500 or more users has or may have been accessed, collected, used or shared by a third party, with certain exceptions, in violation of company privacy policies. The report must include, to the extent possible, the date or estimated date range of when the incident occurred, an overview of the incident, a description of the information accessed, collected, used, destroyed or shared without the user's consent, the number of users affected, and an overview of acts taken to remediate the incident and protect information from further exposure or access. Facebook must update reports every 30 days thereafter until the incident is fully investigated and remediation efforts are fully implemented.

Finally, the Proposed Order requires that Facebook create certain records, including any public or widely-disseminated statements about Facebook's privacy and security policies and all documentation regarding the means by which user personal information was conveyed to a third-party developer, for 20 years after the entry of the Final Order, and to retain each record for five years. Facebook must also submit certain compliance notices whenever there is a change in Facebook's corporate structure or the structure of an entity in which it has an ownership interest or controls that may affect its compliance obligations for 20 years from entry of the Final Order.

In remarking on the settlement's unprecedented requirements for Facebook's privacy program, FTC Chairman Simons stated, "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."[5]

IMPLICATIONS

The FTC's settlement with Facebook has important implications and considerations for businesses that handle consumer information.

First, while the FTC was clearly motivated by the particular facts at issue in Facebook's case, the record-breaking fine and sweeping program requirements may signal the start of a more aggressive privacy enforcement regime by the FTC, particularly where companies have been subject to prior consent orders concerning data privacy. The FTC has made clear that it intends that this case serve as a warning to other companies, as FTC Chairman Simons and two Commissioners stated in announcing the settlement: "The magnitude of this penalty resets the baseline for privacy cases—including for any future violation by Facebook—and sends a strong message to every company in America that collects consumers' data: where the FTC has the authority to seek penalties, it will use that authority aggressively."[6] The FTC's explicit comparison of the size of the penalty imposed on Facebook with the large size of the penalties permitted under the GDPR may signal an increased willingness by the FTC to impose much greater fines on companies for data privacy violations than it has in the past.

Second, the unprecedented program requirements imposed on Facebook may signal a greater willingness by the FTC to direct and control company corporate governance concerning data privacy, particularly for companies that have been the subject of previous enforcement actions. The FTC's requirement that Facebook establish a board-level privacy committee with oversight of privacy officers who will operate with independence from the CEO, and its imposition of a third-party "assessor" with substantial oversight responsibilities and powers, impose significant obligations on the company for the term of the Proposed Order. Companies should assess their own privacy policies and practices in light of the Proposed Order, including the importance of having sufficient independence in the privacy decision-making process. This is particularly true where, as here, the U.S. government might be concerned that financial incentives are driving privacy and security considerations. It remains to be seen whether the measures imposed through the Proposed Order should be seen as targeted measures taken to address significant non-compliance by Facebook in these circumstances or as the FTC's new privacy baseline for other companies going forward, particularly where those companies have made certain promises to users and the FTC.

Third, separate from the FTC's settlement, the U.S. Securities and Exchange Commission reached a settlement where Facebook agreed to pay $100 million for alleged misstatements in its disclosure, which described the risk of misuse of user data as hypothetical, when the SEC alleged that such misuse had already occurred.[7] The SEC's settlement serves as a reminder to companies that when a disclosed cybersecurity or privacy risk materializes into an actual event, the company should evaluate and possibly update its disclosures.

* * *

ENDNOTES

1 Federal Trade Commission, Consent Order, *In the Matter of Facebook, Inc.* (Aug. 10, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

2 Federal Trade Commission, Complaint, *In the Matter of Facebook, Inc.* (July 24, 2019), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

3 Federal Trade Commission, Press Release, *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 ("FTC Press Release").

4 Federal Trade Commission, Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, *In re Facebook, Inc.* (July 24, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf ("FTC Joint Statement").

5 *See* FTC Press Release, n.3.

6 *See* FTC Joint Statement, n.2.

7 Securities and Exchange Commission, *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.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Kamil R. Shields	+1-212-558-7996	shieldska@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Robert A. Sacks	+1-310-712-6640	sacksr@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com