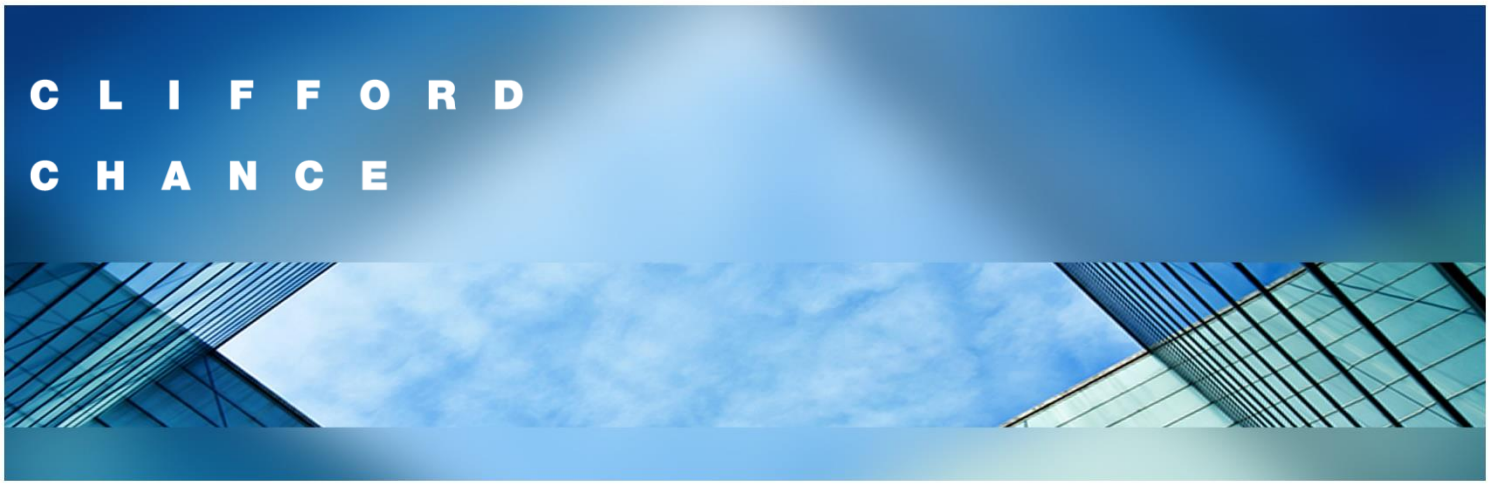

FTC'S $5 BILLION PENALTY AGAINST FACEBOOK: MOMENTUM BUILDS FOR INCREASED U.S. REGULATORY FOCUS ON DATA PRIVACY

Recently, the Federal Trade Commission (FTC) announced a record-breaking $5 billion penalty against Facebook for a series of data privacy violations culminating in last year's Cambridge Analytica scandal. The fine is far larger than any that has ever been imposed globally for data privacy or cyber security violations, and one of the largest penalties that has ever been assessed by the U.S. government for any type of violation. The settlement requires Facebook to put into place a series of controls designed to enhance privacy protections in addition to paying the fine. On the same day as the FTC settlement was announced, the SEC also announced penalties against Facebook for making misleading disclosures regarding the risk of misuse of user data. The FTC order came just days after the FTC announced a settlement with Equifax in which the consumer credit reporting agency agreed to pay up to $700 million to consumers and state and federal authorities for its 2017 data breach. These enforcement actions are indicative of the increased scrutiny by U.S. regulators on data privacy, and may well be a harbinger of more frequent aggressive actions to come.

Background: U.S. Data Privacy and Cybersecurity Regulatory Landscape

Data privacy and cybersecurity regulation in the United States consists of a patchwork of overlapping state and federal laws. At the state level, all 50 states have data breach laws governing responses to cyber security incidents. A handful of states have also enacted comprehensive data privacy and cybersecurity regulatory regimes, such as the California Consumer Privacy Act (CCPA) and New York's recently-passed SHIELD Act. At the federal level, regulation is mainly sector-specific and includes laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA).

The FTC enjoys the broadest enforcement authority pursuant to its mandate under Section 5 of the FTC Act to police "unfair or deceptive acts or practices in or affecting commerce."[1] While this statute does not explicitly refer to cybersecurity or data protection, the FTC has interpreted the prohibition against unfair or deceptive commercial practices to include failing to provide reasonable protections for sensitive consumer data. A company's failure to comply with its own public statements, such as privacy policies or notices about security measures, may also be considered "deceptive." The FTC uses its authority under the Act to regulate all companies and individuals doing business in the United States that are not specifically regulated by other federal agencies (such as banks regulated by the Consumer Financial Protection Bureau, or CFPB).

Facebook's 2012 Consent Order

Facebook's history with the FTC began in 2011, when the social media company first agreed to settle FTC charges that the company had engaged in deceptive trade practices by promising users they could keep their information private and then repeatedly allowing that information to be shared and made public. As is generally the case with FTC enforcement actions against first-time offenders, the settlement did not impose monetary penalties. Instead, the settlement barred Facebook from making further misrepresentations about the privacy or security of consumer personal data and required the company to put in place a comprehensive privacy program designed to safeguard the privacy of user data. The consent order also required the company to undergo biennial independent third-party audits for 20 years to certify that the company was maintaining its privacy obligations agreed-to with the FTC. The settlement was first announced in 2011 but was not finalized until 2012, following a year-long public comment period.

Cambridge Analytica

In early 2018, reports surfaced revealing that Facebook had allowed U.K. consultancy firm Cambridge Analytica to harvest the personal information of millions of its users for political advertising purposes. The information included names, locations, e-mail addresses, and details of "likes" gathered through a personality survey that was used by only approximately 270,000 individuals. Because of Facebook's liberal privacy policies, the third-party application provided access to personal data of everyone in its users' social networks, allowing it to collect information on as many as 87 million users globally, over 70 million of which were from the United States. The app developer, Cambridge Analytica, used the information collected to build psychological profiles of users which were then deployed for targeted political advertisements during the 2016 U.S. presidential election. Media reports allege that the data was also used in other countries, including for targeted advertising in connection with the Brexit "Leave" campaign.

Facebook claims that its third-party application policy during this time only allowed friend data to be used for the purpose of improving user experience, and expressly forbade using or selling the information for advertising purposes. As a result, Facebook has maintained that Cambridge Analytica violated Facebook's

[1] 15 U.S.C. 45(a).

terms by improperly receiving and using friend data. The FTC alleges, however, that Facebook had been aware since 2015 that app developers had been using friend data improperly, but took only limited steps to address these violations and failed to inform affected users about how their information was being used by third parties.

The scandal prompted the FTC to investigate whether Facebook had violated any of its covenants under the 2012 consent order. Meanwhile, shortly after reports surfaced of the Cambridge Analytica scandal, Facebook publicly acknowledged that user information had been shared with over 50 other hardware and software developers, including Amazon, Spotify, Huawei and Hinge in ways that a user might not realize or expect.

The 2019 Settlement: Repeated Misrepresentations and Violations

According to the FTC, Facebook has repeatedly violated the provisions of the 2012 order by misrepresenting the extent to which users could control the privacy of their data. For example, the FTC alleges in its complaint that Facebook used the mobile phone numbers users provided for two-factor authentication for advertising purposes. Facebook also allegedly misled consumers about its use of facial recognition technology, suggesting that it would be "opt-in" when in fact it used the technology to suggest "tagging" in photos and videos, a setting that was turned on by default.

The most severe violation of the FTC's 2012 order related to Facebook's handling of third-party applications. In response to user concerns over privacy, Facebook launched services such as "Privacy Shortcuts" and "Privacy Check-up" that it claimed would help users manage their settings and limit who had access to their data. However, the FTC alleges that even users who opted for the most restrictive settings these tools offered still were not able to limit the sharing of their information with third-party applications. This data included the news and books users read, their relationship details, religious and political views, work history, photos, and videos watched. According to the FTC, a setting did exist to prevent the sharing of this information, but the setting was not easily or intuitively accessible, especially in contrast with the "Privacy Shortcuts." As for the developers themselves, the FTC complaint charges Facebook with failing to conduct adequate vetting: rather than carrying out a thorough assessment of the potential privacy risks of an application, Facebook would simply require developers to click and agree to the platform's terms and conditions. And despite announcing that it would no longer allow third-party developers to collect data about friends of application users, Facebook continued to facilitate such practices for several years. The FTC claims that Facebook's decision-making regarding how to enforce its terms and conditions was often driven by how much advertising revenue a developer generated.

The 2019 Settlement: Terms and Conditions

While the $5 billion civil penalty has captured headlines, perhaps more burdensome are the litany of mechanisms Facebook will be required to put into place over the next 20 years to protect its users' data. The settlement requires Facebook to restructure its approach to privacy from the board level down,

establishing new mechanisms to ensure that executives are accountable for the decisions they make about privacy and that those decisions are subject to oversight.

New Privacy Committee and Personnel

The order requires Facebook to create an independent privacy committee of the board and appoint privacy compliance personnel. The privacy committee will be independent from Facebook management and consist of members of the company's board of directors appointed by an independent nominating committee. It will be tasked with reviewing all material privacy issues and decisions. It will also have authority over privacy compliance officers, who, along with other high-level Facebook staff, will have responsibility for implementing the company's privacy program, including conducting privacy reviews, certifying compliance with the FTC order, and providing reports to Facebook's CEO, the FTC, and an independent assessor. This independent assessor will conduct reviews of Facebook's privacy program and report to the Privacy Committee as well as the FTC, which will have approval authority over appointment or removal over that individual. CEO Mark Zuckerberg will also be required to personally certify Facebook's compliance with the order, potentially exposing him to civil and criminal penalties for violations.

Enhanced Privacy Program

The order also requires Facebook to implement specific enhancements to its privacy program to achieve greater transparency and security. All new or modified products, services, or practices will undergo privacy reviews, which will be shared with the independent assessor and the FTC (upon request). Facebook will also be required to engage in closer monitoring and vetting of third-party developers. In addition, Facebook is prohibited from misrepresenting to its users how the company uses personal information and required to adhere to its disclosed policies, especially with regard to particularly sensitive information such as biometric data and phone numbers. And to improve its internal security controls, Facebook must implement strict employee-access restrictions to user information and delete from its servers personal information that is deleted by users. Facebook's privacy program will also be expanded to cover other services that use and share Facebook's information, including WhatsApp and Instagram.[2]

Implications

Reactions to the FTC order have been mixed, with many decrying the penalty as insufficient. Critics point out that the fine, while massive, only amounts to less than 10% of the company's 2018 revenue. Indeed, when news leaked of the $5 billion fine earlier last month, Facebook shares actually rose, closing at their highest price in nearly a year as investors were encouraged by certainty over the impact of the FTC's investigation on Facebook's bottom line. Privacy advocacy group EPIC (the Electronic Privacy Information Center) filed a motion to intervene

[2] As noted above, in a parallel action the SEC also settled charges against Facebook for making misleading disclosures regarding the risk of misuse of user data. The SEC alleged that Facebook stated that its user data "may" be improperly accessed, when in fact Facebook had discovered actual misuse as early as 2015. Facebook did not admit or deny the allegations but agreed to pay a $100 million penalty and refrain from future disclosure violations.

with the U.S. district court in the District of Columbia shortly after the order was announced, asking the court to reject the deal.[3]

Even the FTC itself was split over the deal. The FTC order was approved in a 3-2 vote along party lines, with the two Democratic commissioners voting against the deal as too lenient. In lengthy statements excoriating the deal, the dissenters argued that the fine should have been bigger and that Facebook should have been forced to make more fundamental changes to its approach towards consumer data. In particular, the dissenting commissioners argued that the FTC should have held CEO Mark Zuckerberg personally liable for the violations, instead of allowing him and other senior officers to be released from liability. Even FTC Chair Joe Simons admitted that it "would have been nice" to have exacted a stiffer penalty. Notably, Simons blamed the commission's "limited authority" in the realm of data privacy, explaining that the settlement was the "only real world choice" when faced with the alternative of years of costly litigation. Simons echoed prior statements by the FTC calling for a comprehensive federal data privacy law.[4]

Simons's comments reflect a growing national consensus that the United States needs a federal law governing data privacy and cybersecurity. Last year, California enacted the California Consumer Privacy Act (CCPA), sweeping legislation that enhances privacy rights for California residents. Since then, several other states have tightened privacy and cybersecurity laws, including New York by passage of the New York SHIELD Act. Differing state standards present difficult challenges for national and international companies. Yet privacy compliance is more important than ever, as evidenced by Facebook's massive fine and potential class action liability. Businesses should review their privacy policies and practices to ensure they are prepared for increased regulatory scrutiny.

---

3 Even though the DOJ and FTC have approved the settlement, the order is not final until it has been approved by the court.

4 *See, e.g.*, Joseph Simons, Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission (May 8, 2019), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Commissioners%20Testimony_05.08.19%20%28002%29_0.pdf ("The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation.")

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Andrei Mikes
Law Clerk (Expatriate)

T +1 212 880 5643
E andrei.mikes
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.