**Wyrick Robbins Yates & Ponton LLP**
4101 Lake Boone Trail, Suite 300
Raleigh, NC 27607
919.781.4000
www.wyrick.com

# Update Your Status: Takeaways from Facebook's $100 Million Privacy Settlement with the SEC

*August 8, 2019*

The Federal Trade Commission's historic $5 billion civil penalty against Facebook for the Cambridge Analytica scandal has been the subject of intense coverage in the legal and mainstream media in recent weeks. But on the same day the FTC action was announced, Facebook also agreed to pay $100 million to settle a separate but much less talked about case brought by the Securities and Exchange Commission based on the same scandal.

The SEC case, which alleged that Facebook misled investors about the risks it faced from Cambridge Analytica's misuse of Facebook users' information, teaches some important lessons for companies about privacy and cybersecurity disclosures.

**Case Background**

The relevant facts of the Cambridge Analytica scandal are by now well known. According to the SEC's Complaint, in 2014 and 2015 Cambridge Analytica paid an academic researcher to collect and transfer data from Facebook to create personality scores for approximately 30 million Americans. The researcher then transferred those personality scores, along with those individuals' underlying Facebook user data, including names, genders, locations, birthdays, and "page likes," to Cambridge Analytica in violation of Facebook's policies. Cambridge Analytica used that information in connection with its political advertising activities.

Facebook became aware in December 2015 that the researcher has improperly sold its users' data to Cambridge Analytica. But in its risk factor disclosures in quarterly and annual reports filed with the SEC from January 2016 through March 2018, Facebook, said the SEC, "misleadingly presented the potential for misuse of user data as merely a hypothetical investment risk." To that end, the company's quarterly and annual Form 10-K and Form 10-Q filings cautioned that:

## Related Attorneys

**Alex M. Pearce**
apearce@wyrick.com

- "Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or our user data *could* result in the loss or misuse of such data, which *could* harm our business and reputation and diminish our competitive position" (emphasis added);

and

- If "developers fail to adopt or adhere to adequate data security practices . . . our data or our users' data *may* be improperly accessed, used, or disclosed." (emphasis added).

Those statements were misleading and material, according to the SEC, given that when the company finally acknowledged the Cambridge Analytica incident publicly in March 2018, the price of its shares declined substantially.

According to the SEC, Facebook's conduct violated the Securities and Exchange Acts of 1933 and 1934 by making misleading statements in its filings with the SEC and by failing to maintain adequate controls and procedures to ensure that its disclosures were materially accurate.

**Lessons for Public Companies**

The SEC's allegations—and the $100 million it took for Facebook to resolve them—contain some important lessons for public companies when it comes to privacy and cybersecurity disclosures.

- **Disclosures about privacy and cybersecurity incidents in SEC filings that are technically correct—but incomplete—can lead to SEC enforcement actions.**

The SEC case turned primarily on Facebook's use of the words "could" and "may" to describe the negative impact to its business of improper disclosures and misuse of its users' data. Those statements weren't false—in fact they were prescient given what ultimately happened when the Cambridge Analytica scandal came to light.

But according to the SEC they were misleading because they "created the false impression that Facebook had not suffered a significant episode of misuse of user data by a developer," but faced merely the risk of such misuse.

Those allegations show the significant risks created by the strategic use of ambiguous or hypothetical language in SEC disclosures about privacy and cybersecurity incidents. When there's been an incident that could materially affect a company's business, this case makes clear that the company must disclose it as such.

- **A company's statements to the press about a privacy incident can also be fodder for SEC enforcement.**

The SEC also faulted Facebook for statements the company made to the press

in response to reporters who asked about the Cambridge Analytica investigation. According to the complaint, Facebook's communications group was aware in 2015 that the researcher had improperly transferred user data to Cambridge Analytica. And yet in 2017 the group responded to press inquiries by referring to Cambridge Analytica statements that denied it used data from Facebook, and by claiming that Facebook's investigation "had not uncovered anything that suggests wrongdoing."

Those statements, alleged the SEC, "served to reinforce the misleading impression in Facebook's periodic filings that the company was not aware of any material developer misuse of user data."

The SEC's action thus makes clear that responses that may seem like acceptable "holding statements" to communications professionals can, if they obscure known facts, give the SEC additional grounds for disclosure-related enforcement actions.

- **Companies should update incident response policies and procedures to include reporting to personnel responsible for preparing disclosures in SEC filings and reassessing public statements after any notable privacy and data security incident.**

Finally, the SEC's Complaint faulted Facebook for violating the Exchange Act's requirement to maintain adequate controls and procedures sufficient to ensure that its disclosures were accurate in all material respects. To that end, the SEC alleged that Facebook:

- had no disclosure controls or procedures designed to analyze or assess incidents involving misuse of user data for potential disclosure in periodic filings;
- did not share information regarding incident with independent auditors or outside SEC disclosure counsel; and
- had no mechanism to ensure the accuracy of filings once they were prepared (e.g. by providing drafts to employees responsible for overseeing compliance with Facebook's platform policies).

The SEC's claims thus make clear that the Commission expects companies to have a documented procedure that includes alerting the individuals responsible for preparing disclosures for SEC filings (internal and external), and reassessing public statements, after any notable privacy or data security matter they investigate internally.

Natural places for those procedures are the company's incident response policies and procedures.

**Conclusion**

The Cambridge Analytica scandal underscores that misuse of data can materially impact a company's operations. And as this settlement shows, the

SEC therefore expects public companies to have a plan for ensuring their risk factors and other disclosures accurately describe any significant privacy and data security incidents the company has encountered.