Westlaw Today
powered by Reuters

Are you a data broker? Chances are high that state and federal regulators think so

By Cynthia Cole, Esq., Brendan Quigley, Esq., and Natalie Sanders, Esq., Baker Botts LLP

JANUARY 3, 2022

On both the national and the state level, regulators have been increasingly interested in data privacy and security issues. This includes enforcement actions not only by states' attorneys general but also the U.S. Securities and Exchange Commission ("SEC") and the Federal Trade Commission (the "FTC"). As discussed further below, the SEC recently brought its first enforcement action against a data broker, signaling a deeper move into the data privacy space.

SEC settles fraud charges with alternative data provider

Earlier this fall, the SEC announced its settlement with San Francisco-based company App Annie. Notably, this is the first enforcement proceeding that the SEC has brought against a provider of "alternative data."

App Annie, a data broker, sells market data on mobile app performance. For example, mobile app creators may purchase competitor app information or trending app information from App Annie to help increase user engagement or sales. The information provided is known as "alternative data" because it is not found in traditional data sources, such as SEC filings, press releases, or financial statements.

This App Annie enforcement action further extends the SEC's reach into cybersecurity and data privacy.

According to its website, App Annie "is the first company to offer a mobile performance suite that provides app market, advertising analytics and data science driven insights derived from benchmarking data[.]" App Annie's website also boasts that over one million users rely on it for mobile market data.

In its enforcement action, the SEC found that "App Annie and [its co-founder and former CEO and chairman Bertrand] Schmitt misrepresented to their trading firm customers that App Annie generated the estimates in a way that was consistent with the consents it obtained from companies that shared their confidential data, and that App Annie had effective internal controls to prevent the misuse of confidential data and to ensure that it was in compliance with the federal securities laws."

Additionally, the SEC found that "App Annie and Schmitt were aware that trading firm customers were making investment decisions based on App Annie's estimates, and App Annie also shared ideas for how the trading firms could use the estimates to trade ahead of upcoming earnings announcements."

In the United States, data privacy has long been the subject of state regulation.

In the press release, Gurbir S. Grewal, Director of the SEC's Enforcement Division described the "deceptive conduct" and "misrepresentation" of App Annie and Schmitt, saying that they "lied to companies about how their confidential data was being used and then not only sold the manipulated estimates to their trading firm customers, but also encouraged them to trade on those estimates — often touting how closely they correlated with the companies' true performance and stock prices."

This App Annie enforcement action further extends the SEC's reach into cybersecurity and data privacy. Notably, the SEC charged App Annie and Schmitt with violating Section 10(b) of the Exchange Act and Rule 10b-5, i.e., under an intentional fraud theory, as opposed to more negligence-based theories of liability.

App Annie consented to a cease-and-desist order and to pay a $10 million penalty. Schmitt agreed to pay a penalty of $300,000 and is prohibited from serving as an officer or director of any public company for three years. App Annie's new CEO Theodore Krantz released a statement assuring customers that it had "established a new standard of trust and transparency for the newly created alternative data market."

He furthered warned that "[m]any businesses may be unknowingly leveraging data reliant on confidential public company information without explicit consent which we believe puts companies using digital/mobile market data at significant risk. It is our opinion that the entire alternative data space needs to be regulated."

What this means for the data privacy space

In the United States, data privacy has long been the subject of state regulation. California, in particular, has long been the leader in the privacy regulation arena with the passage of the most comprehensive privacy law in the country, the California Consumer Privacy Act (the "CCPA") which went into effect on January 1, 2020.

Additionally, under California law, data brokers are required to register with the Attorney General online (Vermont also has a similar data broker registration law). As part of the registration, the business must pay a fee and provide information concerning its "data collection practices." Cal. Civ. Code § 1798.99.82.

On the federal level, the FTC has also been active in the data privacy enforcement space, but the App Annie action shows that the SEC — as in other areas — will use its pre-existing statutory enforcement tools (such as Section 10(b) of the Exchange Act in the App Annie case) to focus on cyber and data privacy issues.

On the federal level, the FTC has also been active in the data privacy enforcement space.

Public companies and other SEC-regulated entities should thus be aware that such data privacy procedures and the company's response to data privacy incidents, as well as the disclosures to investors surrounding those issues, may generate SEC attention, in addition to attention from other regulators as well.

About the authors



Cynthia Cole (L) is a partner at **Baker Botts LLP** and the deputy department chair of the corporate section in the San Francisco and Palo Alto, California, offices. Her practice focuses on corporate, strategic and technology transactions and data privacy. She can be reached at cynthia.cole@bakerbotts.com. **Brendan Quigley** (C) is a partner in the New York office. His practice focuses on SEC and DOJ securities and commodities enforcement matters, FCPA-related investigations and counseling, and matters arising under the False Claims Act, as well as commercial disputes. He is a former federal prosecutor in the Southern District of New York. He can be reached at brendan.quigley@bakerbotts.com. **Natalie Sanders** (R) is a litigation associate in the Palo Alto office. She represents clients in a variety of complex commercial matters including consumer class actions, and has experience with disputes regarding trade secrets, breach of contract, and breach of fiduciary duty. She can be reached at natalie.sanders@bakerbotts.com.

This article was first published on Westlaw Today on January 3, 2022.