CCPA Litigation Update: How the CCPA (and other Privacy Risks) Raise the Risk of Potential Shareholder Claims

Michael C. Lynch, Alysa Z. Hutnik

October 30, 2020

California became the first U.S. state with a comprehensive consumer privacy law when the California Consumer Privacy Act ("CCPA") became operative on January 1, 2020. The CCPA provides for broad privacy rights for residents of California and imposes data protection obligations on companies doing business in California that meet certain criteria. For further background on the CCPA, see our prior CCPA blog posts here.

Privacy Risks Trigger Public Disclosure

While many businesses continue to work on their CCPA privacy compliance strategies and risk mitigation measures, those subject to the law also should consider whether their data practices prompt any material disclosures. Item 105 of Securities and Exchange Commission ("SEC") Regulation S-K requires public companies to disclose the most significant factors that make investing in their securities speculative or risky.

The SEC published a proposed rule for public comment in the Federal Register on August 23, 2019, that sets forth amendments to modernize the description of business, legal proceedings, and risk factor disclosures that registrants are required to make pursuant to Regulation S-K. In a public comment to the proposed rule, the World Privacy Forum advised the SEC that the privacy and security risks and obligations that companies face today require that there be more disclosure of those risks in public disclosures. Thus, it requested that the SEC expressly require the appropriate disclosure of material privacy and security risks faced by regulated companies.

In support of its request to the SEC, the World Privacy Forum pointed not only to the risk of data breaches, but also to the material impact that privacy regulations, including the CCPA, can have on a company's operations. Specifically, it pointed to a $5 billion fine that the Federal Trade Commission imposed on Facebook for its failure to comply with a privacy-related FTC consent decree and the potential for a fine of up to four percent of a company's worldwide revenues for violations of the European Union's General Data Protection Regulation ("GDPR").

The comment continues, however, by noting that fines are not the only risk that companies face from privacy regulations. Compliance with privacy and security regulations can also have a material risk on a company's operations, with the comment specifically citing:

- Loss of markets, customers, and opportunities;

- Failure of business models to be consistent with privacy requirements;
- Charges for responding to data breaches; and
- Loss of key personnel.

Because privacy and security risks are unique to each company, boilerplate disclosures will not suffice to warn investors of these risks. As noted in the comment, a company that collects and uses consumer data as part of its business model faces a significantly larger threat to the continuity of its operations by privacy regulations than a company that maintains only its employees' data.

These and other privacy law developments are a good reminder for public companies that their CCPA-related exposure extends beyond the CCPA's monetary provisions, which are limited to a narrow private right of action for data breaches, as well as enforcement by the California Attorney General. Class action plaintiffs have used similar data privacy statutes to support securities fraud claims, and companies should expect to see similar claims predicated on compliance with the CCPA. Rather than basing the claim on a direct violation of the privacy statute at issue, such as the CCPA, the complaints are rooted in violations of federal securities laws and claim that the company did not accurately disclose its compliance with regulatory obligations under the privacy law or disclose the impact that the privacy law would have on its business.

Privacy Shareholder Litigation Examples

For example, shareholders of Nielsen Holdings PLC ("Nielsen") brought a securities class action against the company and some of its officers and directors alleging securities fraud under the federal securities laws based on false or misleading statements made by the company regarding how the GDPR would impact its business and financial performance. The consolidated complaint alleges that the defendants misled investors by stating that the GDPR would not have any major impact on the company, assuring investors that the company was ready for the GDPR's effective date, and assuring investors that the company would continue to have access to data from Facebook and others, which it relied upon for many of its products and services. The defendants went as far as to call the GDPR a "non-event" for the company.

In reality, however, the GDPR had a material effect as soon as it became effective by preventing Nielsen from getting the data it needed from large data providers. The truth was revealed to the market on July 26, 2018, the complaint alleges, when Nielsen reported its 2Q18 earnings and disclosed a significant decline in its performance. Nielsen attributed its poor performance to the GDPR, and admitted that Nielsen no longer had access to the data from Facebook and other data providers for its analytical products, including data that helped advertisers target individual consumers. Following this disclosure, Nielsen's stock price declined 25% in one day.

In another securities class action predicated in part on the GDPR, investors alleged that Facebook made false and misleading statements regarding its compliance with the GDPR and the impact that the legislation would have on its business and operations. Specifically, the operative complaint alleges that Facebook made materially false and misleading statements when: "(i) it falsely and without a reasonable basis assured investors that GDPR had not caused, and would not cause, a decline in active use of Facebook's solid [sic] media platforms; and (ii) it portrayed Facebook as adhering to and prepared to meet the requirements of the GDPR, when in reality Facebook was not."

The investors claim that the truth was revealed to the market on July 25, 2018, when Facebook released its 2Q18 earnings report and revealed "a significant decline in users in Europe, zero user

growth in the United States, decelerating worldwide growth of active users (i.e., those most responsible for generating data used in targeted advertising), lower than expected revenues and earnings, ballooning expenses affecting profitability, and reduced guidance going forward." The company's stock dropped by nearly 19% the following day.

The complaint alleges that the GDPR contributed to Facebook's declining revenue growth by limiting the data that users share with the company, which lead to a reduction in spending by advertisers, and by requiring the company to "incur billions in expenses to become privacy compliant." The complaint alleged this was in contrast to the company's prior reassurances that the GDPR would not have a material impact on Facebook's business because the vast majority of users were opting into data sharing and because the company's privacy practices were already compliant with the regulation.

Facebook and *Nielsen* are examples of a growing trend of cases in securities class action litigation that allege class-wide harm to shareholders based on violations of the federal securities law, in these cases sections 10(b) and 20(a) of the Securities Exchange Act of 1934 and Rule 10b-5, rather than harm to consumers based on direct violations of privacy statutes like the GDPR or CCPA. Also notable is that neither of these class actions was preceded by regulatory action prosecuting a breach of the privacy regulation by the company. The *Facebook* plaintiffs recently filed their Third Amended Complaint and *Nielsen* has a pending motion to dismiss, therefore it remains to be seen whether this theory of securities fraud will prove successful for plaintiffs' attorneys.

Public Company Privacy Disclosure Considerations

These developments raise several considerations for public companies. At a minimum, public companies should ensure that they have accurately assessed and disclosed their compliance with and exposure under privacy statutes, including the CCPA. Companies should not attempt to rely on generic risk disclosure provisions but instead should provide thoughtful, tailored disclosures of the impact that newly-enacted data protection legislation—including the CCPA—will have on their businesses.

Companies also would do well to consider the extent to which:

- The company's data practices trigger compliance with U.S. and international privacy laws (often this means becoming familiar with the broadening definition of personal information under such laws);
- Increased consumer rights concerning the sharing of personal information may limit or preclude the company's ability to use the personal information in a manner that is material to its business practices, which could impact the company's growth strategies or financial condition;
- Data protection laws and industry changes will require the company to delete or remove consumer information from its records or otherwise materially increase the costs of doing business to ensure compliance;
- The company's failure to comply with privacy or data protection obligations could result in governmental investigations, enforcement actions or litigation, resulting in monetary penalties to the company, restrictive injunction terms, or a general loss of trust in the company, which in turn could have an adverse effect on a company's reputation and business;

- Data protection laws and industry changes will result in changes to the company's data sources that, in turn, could affect the company's ability to procure the data necessary for the company's operations and thereby limit sources of revenue for the company;
- Data protection laws and industry changes will result in business clients or consumer users choosing to limit or not adopt and use the company's products, affecting the company's ability to acquire customers and thereby limiting sources of revenue for the company.

While privacy laws in the U.S. are clearly at an inflection point, the trend line demonstrates that data strategies must be evaluated both for their possibilities and potential risks to the company. Public companies that routinely perform rigorous internal privacy analyses and continue to closely monitor these quick moving legal and industry changes will be better positioned to address their transparency obligations, and in so doing, mitigate the risk of facing privacy shareholder suits.

For more information on the CCPA and other topics, see:

- Advertising and Privacy Law Resource Center
- Ad Law News and Views Newsletter
- Ad Law Access Blog
- CCPA Practice Page