NOW + NEXT

PRIVACY LAW ALERT | NIXON PEABODY LLP

DECEMBER 21, 2018

D.C. attorney general borrows from FTC playbook in case against Facebook

By Brian Donnelly, Jenny Holmes and Karina Puttieva

The District of Columbia attorney general sued Facebook Wednesday in connection with the well-publicized Cambridge Analytica scandal, alleging the company violated the District's consumer protection statute by failing to protect user privacy. The action is the first significant state-level action against Facebook relating to the harvesting of millions of users' personal information, which was then used by a political consulting firm to influence the 2016 presidential race.

The lawsuit highlights the potential exposure of companies to multiple state-level enforcement actions in the absence of federal preemption in the data privacy space. It also borrows from the playbook of the Federal Trade Commission (FTC) by applying general consumer protection enforcement tools that were not designed with data industries in mind. The D.C. lawsuit, as well as recent reports of further disclosures by Facebook of user information, may increase already mounting pressure from both consumer rights groups and the tech industry itself for standardized federal privacy laws and stronger federal enforcement authority.

The D.C. lawsuit

In its complaint, D.C. alleges that Facebook violated the District's Consumer Protection and Procedures Act (CPPA), D.C. Code § 28-3901, et seq.—which generally prohibits unfair or deceptive trade practices—by failing to keep users' personal information secure despite promising to do so. Facebook allegedly permitted a Cambridge University researcher to use a third-party application to harvest the personal data of about 70 million users in the United States, including more than 340,000 D.C. residents. The researcher then sold the data to Cambridge Analytica, a political consulting firm that used it to target individual voters based on their personal characteristics. Facebook also allegedly allowed certain partner companies to override users' privacy settings to collect consumer data.

D.C. claims Facebook violated the CPPA by misrepresenting the extent to which it and third-party developers protected users' personal information, as well as how users' agreements with third-party applications controlled the use of their data. Facebook also allegedly failed to adequately disclose to users that third-party applications downloaded by their Facebook friends could access their data without the users' own knowledge or consent. D.C. also alleges that Facebook violated the CPPA by

failing to notify users when their data was improperly harvested and used by third-party applications, as in the case of Cambridge Analytica, and did not tell users that it granted certain companies—many of whom were mobile device makers—special permissions that enabled those companies to access consumer data and override privacy settings.

If the lawsuit is successful, Facebook could be liable for at least $1.7B—$5,000 for each of the 340,000 D.C. residents affected by the alleged data harvesting—in addition to other damages under the CPPA.

Exposure to multiple claims

The D.C. lawsuit emphasizes the multiple levels of exposure companies face for data privacy violations. Currently, there is no comprehensive federal law regulating the collection and use of personal data, and since no federal statute preempts all state laws in the consumer privacy space, states are free to independently regulate the collection and use of many types of consumer data. The result is a patchwork of state legislation—some that specifically regulates data privacy, and some, like the CPPA, that only generally prohibit harmful business practices. Since most tech companies serve a nationwide market, they are potentially exposed to numerous and varied state enforcement actions in the event of a single data privacy incident.

Ex post enforcement

The D.C. lawsuit also is notable insofar as it does not seek to enforce any data-specific laws or regulations, but rather D.C.'s all-purpose consumer protection statute. The CPPA was enacted in 1976, long before anyone was paying attention to data security and privacy issues. Rather than specifically regulating data, the CPPA broadly prohibits any "unfair or deceptive trade practice." D.C. Code § 28-3904.

In bringing suit against Facebook under the CPPA, the D.C. attorney general is borrowing a page from the FTC's playbook at the federal level. Since the FTC lacks rulemaking authority to preemptively regulate data privacy and security practices, it instead relies on its authority under Section 5 of the FTC Act to punish "unfair or deceptive acts or practices." 15 U.S.C. § 45. Just like the D.C. lawsuit, most FTC enforcement actions do not seek to punish unauthorized data disclosures *per se*, but rather rely on the theory that a company's failure to abide by its own published data privacy policies constitutes an unlawfully deceptive trade practice.

Indeed, that is exactly what happened to Facebook in 2011, when it entered into an FTC consent agreement to resolve allegations that it engaged in unfair and deceptive trade practices in connection with its data privacy policies. The FTC is now investigating whether Facebook violated the 2011 consent agreement in connection with the Cambridge Analytica scandal and other recently publicized disclosures of user information.

Stronger federal regulation on the horizon?

In the wake of the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), the idea of federal privacy legislation has enjoyed an unprecedented level of support from lawmakers and tech industry leaders. In November, for instance, Senator Wyden (D-Or) introduced a bill that would create a national Do-Not-Track system for websites and expand the FTC's funding and staff as well as its power not only to fine but to jail senior executives who knowingly mislead regulators (see our recent NP Privacy Partner blog post). Around the same time, Intel Corporation released a draft bill aimed at enacting nationwide standards for collecting

and sharing personal data, based on the FTC's Fair Information Practices Principles. While many speculate that the push for a federal privacy law is fueled in part by the hopes of preempting California's far-reaching CCPA with a more industry-friendly standard, others see a fundamental shift in the way consumers think about privacy and the value of their personal information.

The FTC held a series of data privacy hearings in November 2018, and lawmakers continue to consider whether greater federal rulemaking and enforcement authority is warranted. In the meantime, companies whose business involves the collection of consumer data should continue to monitor state-law developments and routinely assess their data privacy policies and procedures.

What should companies do now?

As the Cambridge Analytica scandal clearly shows, transparency in data collection and use is always the best practice, even if there is no federal law requiring it. Companies that collect, use, process or store any personal information should make sure that reasonable privacy practices are in place. But more importantly, companies must make sure that the policies governing data collection and use align with their actual practices. In today's world, consumers are on high alert when it comes to the privacy of their personal information. While companies have already had to face the reputational consequences of deceptive practices, the added threat of enforcement actions, whether at the state or federal level, shines an even brighter light on the need for legitimate privacy practices.

The D.C. attorney general's complaint against Facebook is available here. For more information on the content of this alert, please contact your regular Nixon Peabody attorney or:

- Brian Donnelly at **bdonnelly@nixonpeabody.com** or (202) 585-8191
- Jenny Holmes at **jholmes@nixonpeabody.com** or (585) 263-1494
- Karina Puttieva at **kputtieva@nixonpeabody.com** or (213) 629-6091
- Jason Gonzalez at **jgonzalez@nixonpeabody.com** or (213) 629-6019
- Steven Richard at **srichard@nixonpeabody.com** or (401) 454-1020