Bloomberg Law®

Privacy and Security Law Report®

Will Facebook Firestorm Yield Tougher U.S. Data Privacy Standards?

Data Privacy

States could reform their various laws to implement new data protection and breach notification standards, but this would be a piecemeal effort that could be years in the making and would still retain a balkanized system with laws of varying scope and effectiveness, warn Joseph Moreno and Keith Gerver of Cadwalader, Wickersham & Taft LLP.

BY JOSEPH MORENO AND KEITH GERVER

Following the discovery that Facebook was aware an outside researcher polled and improperly shared personal information of roughly 87 million of its users with U.K. consulting firm Cambridge Analytica, apparently in violation of Facebook policies, U.S. regulators and lawmakers have stepped up efforts to assert themselves in the data privacy space. The Federal Trade Commission has confirmed it is investigating Facebook's privacy practices and looking into whether the company violated a 2011 settlement in which it pledged to give its users greater control over how their personal information is shared. Facebook CEO Mark Zuckerberg appeared for two days of marathon hearings before the U.S. Senate and the House of Representatives, and has reportedly been invited to appear for similar hearings before the European Parliament. The question is whether this firestorm will ultimately blow over, or if public outcry will lead lawmakers in the U.S. to implement tougher state-by-state laws or even a national data privacy standard to govern how customers' personal information is protected and when it may be shared with outside parties.

Joseph Moreno (@JosephMoreno) and Keith Gerver (@kgerver) are attorneys with Cadwalader, Wickersham & Taft LLP based in Washington. The views expressed herein are their own and not their employer's, and this article does not constitute legal advice.

The Existing 50-State Strategy

The U.S. lacks a national policy dictating how companies must safeguard customer data, how data may be shared, and when customers must be notified if their personal information is hacked. When federal authorities get involved in a cybersecurity incident, that task generally falls to the FTC to enforce Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC has used this pre-cyber era law to bring civil enforcement actions against companies (including Facebook) for misrepresenting how they use customer data, and for failing to adequately safeguard that data against hackers. How-

 ISSN 1538-3423

ever, the law does not set standards for how customer data is to be handled, and serves effectively as a reactive tool after an incident has occurred.

To make matters worse, the FTC is not the only federal regulator that may get involved in a data breach situation. The Securities and Exchange Commission, Commodity Futures Trading Commission, Department of Justice, and Department of Health and Human Services (Office for Civil Rights) have investigated companies in various industries for data breach-related incidents. While this is warranted in some cases, it leaves companies never quite certain to which enforcement agency they will be answering, and which standards will apply.

In the absence of a national standard, each of the 50 states and the District of Columbia maintains its own laws, rules, and regulations to address the obligations of companies to their customers in the event of a cybersecurity incident. While many of these laws share the same focus on customer data that could lead to identity theft or fraud, they differ somewhat in how they define ''personal information,'' what they consider a ''breach,'' and when a company is required to notify customers (and, in some instances, state regulators) that a cyber incident has occurred. For example, most states define a breach as unauthorized access and exfiltration of customer information, meaning there must be some indication that data was taken. However, a handful of state laws, including New Jersey, require only unauthorized access, not exfiltration. So, for example, a successful ransomware attack in which customer data was accessed but not taken may constitute a breach in some jurisdictions but not others. Similarly, while Florida's data breach law requires notification to be made to affected customers no later than 30 days from discovery of the cyber incident, most states do not set a deadline so long as notification is made ''without unreasonable delay.'' Thus, companies that find themselves the victims of a hack must comply with dozens of state data breach laws, and consumers cannot point to a single unified standard to understand their rights if their data is compromised.

No Breach, No Notification

The Facebook incident was not a data breach as contemplated by the various state laws. The researcher in question developed an application programming interface that asked users to provide personal information about themselves and their personal contacts. The researcher then, in violation of Facebook's user policies, shared that information with Cambridge Analytica, which is believed to have provided services to Donald Trump's 2016 campaign for president. Facebook became aware of the issue in 2015 and asked the parties to delete the information, but aside from suspending the accounts, it failed to confirm or otherwise follow up on the request.

Under existing state laws, there is no prohibition on sharing customer or user data with third parties. As a result, apart from any obligations it may have under its 2011 settlement with the FTC, Facebook likely was not obligated to notify its customers about the Cambridge Analytica incident. Several states, such as New York and Massachusetts, have nonetheless opened investigations into how Facebook handled this matter, but they will likely focus on whether the company misrepresented its data sharing policies, not on whether it should have notified its customers about what happened. This disconnect is what has triggered much of the consumer outrage, as Facebook users are coming to the realization that existing laws fail to address how their information may be shared and ultimately used.

Potential Reform Efforts

One possible result of this Facebook fiasco is that individual states may revisit their data breach laws. This could include expanding the definition of ''personal information'' to include any information associated with an identifiable user, and requiring companies to more explicitly notify users about how personal information may be shared with third parties. States could also require companies to obtain a customer's ''informed consent'' before data may be shared, similar to measures going into effect in May under the European Union's General Data Protection Regulation. Of course, this would have to be done on a state-by-state basis and would not address the fact that every jurisdiction would continue to have different standards going forward.

Another possibility is that Congress could react by enacting its own version of the GDPR in the U.S. Like the GDPR, a national data privacy standard could set forth a single standard for what constitutes protected personal information, how this information must be safeguarded (*i.e.*, use of adequate encryption to protect personal information), and how quickly companies must notify customers in the event of a data breach. A federal standard could also clarify which regulator would have primary responsibility for policing data privacy and use practices, and could require companies to notify that regulator in the event of a cyber incident (the GDPR will require regulator notification within 72 hours).

Conclusion

Zuckerberg indicated during his congressional testimony and in subsequent statements that Facebook would voluntarily extend GDPR-like protections such as informed consent to users worldwide — not only to those in the EU. However, even if Facebook adheres to this promise, there is no certainly that other companies will follow suit. Further, in the days since Zuckerberg's testimony, the notion has been raised that his generally well-received performance, coupled with a general lack of focused and pointed questioning from lawmakers, means this could all blow over with no action at all.

This would be an unfortunate missed opportunity to tackle an issue that has finally come to the forefront of public attention. States could reform their various laws to implement new data protection and breach notification standards, but this would be a piecemeal effort that could be years in the making and would still retain a balkanized system with laws of varying scope and effectiveness. A national data privacy regime would instruct companies that hold personal data what is uniformly expected of them, and at the same time inform customers of how their data may be used and what their rights are in the event a breach takes place. Hopefully, legislators will tackle this issue and explore potential solutions to this problem, which is not going away anytime soon.