FinReg
Davis Polk Insights on Financial Regulation

Regulators and Plaintiffs Aren't Waiting for Privacy Legislation: Companies Face Potential Liability Now and Can Take Steps to Reduce Risks

By Avi Gesser, Eric McLaughlin, Greg Swanson & Clara Y. Kim on April 29, 2019
POSTED IN SEC

Momentum is building in Congress for federal privacy legislation and several states have their own privacy laws in the works. But, as concerns grow that companies are collecting and sharing personal information about U.S. residents without their knowledge and not adequately protecting that data, regulators and plaintiffs aren't waiting for new laws. Instead, they are refitting existing laws to meet their data privacy and security objectives.

The SEC

We have previously written on the **SEC's use of traditional internal accounting controls** and the **Safeguards Rule** for cybersecurity enforcement. On April 16, 2019, the SEC's Office of Compliance Inspections and Examinations (the OCIE) issued a **risk alert** indicating that it is also focused on privacy compliance under its existing rules. Based on examinations of registered investment advisers and broker-dealers, the SEC identified several compliance issues relating to Regulation S-P—a 2000 SEC rule requiring firms to adopt privacy policies and to notify customers regarding the firm's privacy practices, as well as the customers' right to opt out of third-party data disclosures. The SEC highlighted several privacy-related violations of Reg. S-P that it has observed, including:

- Not having privacy notices or policies, or having insufficient notices or policies.
- Having policies that were not implemented, or for which there was inadequate training.
- Not having an inventory of all systems on which personal information is maintained.

- Not requiring vendors to protect customer data to which they are given access.
- Not having sufficient incident response plans.
- Allowing departed employees to have continued access to company systems.
- Storing personal information in unsecured physical locations.
- Allowing employees to send client information in unencrypted emails to unsecured computers outside of the firm and to keep such information on unsecured personal devices.

Like with its Section 21(a) report from October, this SEC risk alert is likely a warning of future enforcement actions against registered investment advisers and broker-dealers that do not have adequate privacy practices.

The FTC

We have previously written about regulators **using unfair business practice legislation to bring cybersecurity and privacy cases**. On April 24, 2019, **the FTC settled allegations against i-Dressup.com** for failing to obtain parental consent before collecting personal information for children under 13 and failing to provide reasonable security for the data it collected in violation of the Children's Online Privacy Protection Act (COPPA). On the same day, the FTC also settled allegations against ClixSense, an online rewards website, for failing to take reasonable steps to secure customer data. The FTC alleged that ClixSense has engaged in deceptive practices under the FTC Act for making misrepresentations about its encryption and data security, and in unfair practices for failing to employ reasonable data security practices to protect the customer data that it collected. In a press release about the settlement, **the FTC also provided some tips for companies**, including:

- Following through on their security representations to the consumer regarding protection of personal information.
- Monitoring for suspicious activity and investigating events quickly.
- Making sure login credentials are protected.

Last year, **the FTC also reached a settlement with BLU Products, Inc. (BLU)** over allegations that it had allowed ADUPS Technology Co. LTD to collect

detailed personal information about BLU's consumers without their knowledge or consent, despite BLU's assurances that it would keep the information secure and private. Further, the FTC alleged that BLU generally failed to implement appropriate security procedures to oversee the security practice of its service providers, in violation of the FTC Act.

Private Plaintiffs

Plaintiff lawyers and private individuals are also not waiting around for new privacy laws. **Last year, Vizio settled claims** consolidated from 20 class action lawsuits that accused the electronics manufacturer of collecting information about plaintiffs' viewing habits from their Vizio smart TVs and selling that information to advertisers. The claims were brought under a variety of state laws including California's Unfair Competition Law, Florida's Deceptive and Unfair Trade Practices Act and Massachusetts' Unfair and Deceptive Trade Practices Act. Plaintiffs are also pursuing cyber claims through traditional negligence actions, and **as we have previously written**, they've had some success convincing courts that a data breach is a "foreseeable risk" and that companies owe a "duty of care" to take reasonable measures to protect personal information.

Businesses too aren't waiting for new laws. Currently pending before the Ninth Circuit is hiQ's lawsuit against LinkedIn. hiQ is a startup that uses bots to pull and analyze data from websites like LinkedIn and sells that data to other companies. LinkedIn had issued a cease-and-desist letter and tried to block hiQ's access to this information. **hiQ then sued LinkedIn**, alleging unfair competition. LinkedIn alleges that hiQ's continued access of its site after attempts to block hiQ amounts to hacking in violation of the Computer Fraud and Abuse Act.

Reducing Risks

In light of these developments, companies that gather and sell personal information are taking steps to reduce their legal risk under such existing laws, including:

- Having clear data security and privacy policies that are implemented, tested and updated as appropriate.
- Collecting only the customer personal information that is needed, making sure that information is secured, and getting rid of that information when it is no longer being used.

- When sharing customer personal information: (1) making sure it is being done in a way that is authorized, and is consistent with applicable policies and customer expectations, (2) sharing it on a de-identified basis where possible, and (3) making sure that whoever is receiving the information will take appropriate steps to protect it.

Other examples of the ways companies can reduce cybersecurity and privacy risks are available at the Davis Polk Cyber Portal, which is available to help clients navigate the evolving data requirements for businesses.