315 W. 11TH AVE., DENVER, CO 80204 | 720–328–1418 | www.LAWWEEKCOLORADO.com VOL. 16 | NO. 49 | $6 | DECEMBER 3, 2018

LAW WEEK COLORADO

Congress Makes New Attempt at Data Privacy Legislation

Consumer Data Protection Act would install 'Do Not Track List,' major penalties for companies and executives

BY **DOUG CHARTIER**
LAW WEEK COLORADO

Congress is once again trying to create federal cybersecurity standards, and a bill introduced last month, if it passes, would put powerful tools in the hands of both consumers and the Federal Trade Commission.

In November, Democratic Sen. Ron Wyden introduced the Consumer Data Protection Act, which would allow consumers to opt out of letting companies share or sell their data through a federal "Do Not Track" list. The bill would also empower the FTC to police companies' data privacy practices, directing the agency to set cybersecurity standards and requirements as well as beef up its enforcement staff in that area.

"My bill creates radical transparency for consumers, gives them new tools to control their information and backs it up with tough rules with real teeth to punish companies that abuse Americans' most private information," Wyden said in a press release.

The Do Not Track system, which would function similar to the FTC's Do Not Call Registry, would let consumers prohibit third parties from sharing or selling their data as well target them with ads based on personal information. It would allow companies to charge consumers who use their (otherwise free) products and services if the consumers decline to let the companies share or sell their data.

The bill would also give the FTC the authority to set and enforce "reasonable cyber security and privacy policies, practices and procedures to protect personal information." The agency currently prosecutes companies for substandard cybersecurity practices, pursuing them as unfair trade practices under Section 5 of the Federal Trade Commission Act. A federal standard would instill more consistency in cybersecurity regulation, whereas companies currently must adhere to a variety of data privacy and security laws across the 50 states.

The Consumer Data Protection Act would apply to companies that collect at least $50 million in annual revenue and personal data on at least one million consumers. The bill defines consumers as "individuals" and doesn't specify whether it includes both U.S. and foreign consumers.

But companies that generate at least a billion dollars in revenue and handle data on a million consumers, as well as companies of any size that handle data on 50 million consumers, would be on the hook for extra reporting requirements. Senior executives of those companies would have to file annual reports regarding whether they complied with the act's data privacy and security standards. These reports would carry criminal exposure, however. If executives sign off on these reports and they turn out to contain false information, those executives could face up to 20 years in prison and a $5 million fine.

For companies that violate the act's privacy standards, the FTC could impose civil fines of up to 4 percent of the companies' global annual revenue, and on the first offense. That is the potential penalty companies currently face under the European Union's General Data Protection Regulation, or GDPR.

For companies, what's most concerning about the bill isn't just the heavy penalties it proposes but how those penalties might arise, said Camila Tobón, of counsel with Shook Hardy & Bacon and director of the firm's International Privacy Task Force. The bill appears to place the enforcement accountability not on the FTC so much as on the companies themselves, who must then self-report any non-compliance, she noted. By contrast, the GDPR holds companies accountable for maintaining detailed records of how they handle consumer data, but it doesn't require them to certify each year — at the risk of fines and prison time — that they're meeting EU regulatory standards. The Wyden bill would require companies to be their own watchdog in a sense, as opposed to the government agency, Tobón said.

"That puts the onus on the company for really intense recordkeeping," she said.

Tobón, who works extensively with GDPR compliance issues, said the Consumer Data Protection Act is proposing certain requirements that even go beyond what the EU imposes. Under the bill, companies must provide individual consumers a way to see, on request, what information they're storing about that consumer, how it was collected, who it's been shared with, and what data they have on the consumer that they didn't receive directly.

"It's really granular information that you have to provide," Tobón said. In order to respond to such data access requests by the bill's 30 business day deadline, companies would have to set up an automated process, "which is going to be a heavy lift for companies," she added.

Should the Consumer Data Protection Act stall in Congress like so many federal cybersecurity bills before it, the issues it addresses won't go away; companies will continue to see growing demand for transparency in how they handle consumer data, Tobón said. "The time has come for companies to have a streamlined and unified approach to cybersecurity," she added, which includes systems for data mapping, data inventory and risk assessment.

CAMILA TOBON

Even if they aren't subject to the robust requirements in the GDPR or California's new state cybersecurity law, companies should be ready to comply with them in case more states eventually adopt the higher standards or Congress enacts them. "It's coming," she said.

Meanwhile, U.S. senators are also discussing another separate draft bill that would allow the FTC to set cybersecurity standards and enforce them across all 50 states. Democratic Sen. Richard Blumenthal told Reuters that the bill should be introduced in the Senate early next year.•

— Doug Chartier, DChartier@circuitmedia.com