**Federal Data Privacy Legislation Is Likely Next Year, Tech Lawyers Say**

by Dan Clark

If federal data privacy legislation is ever going to be passed, it may be in 2019, according to James Shreve, a partner and head of the cybersecurity practice at Thompson Coburn in Chicago, explained that a number of proposals for comprehensive data privacy and security legislation failed to get off the ground. As early as 2009, for instance, U.S. Rep. Peter DeFazio, D-Vermont, introduced a bill for the Personal Data Privacy and Security Act. The bill never received a floor vote. Why now? More companies appear to be growing concerned with the idea of having a jumble of federal and state data privacy and cybersecurity laws, especially with the passage of the California Consumer Privacy Act of 2018 in June of this year. However, the California law will not fully take effect until 2020. There are also several different types of pending data privacy by sectors, such as the Health Insurance Portability and Accountability Act and The Fair Credit Reporting Act. David Hoffman, associate general counsel and global privacy officer at Intel Corp., based in Santa Clara, California, said that with the CCPA comes more of a patchwork of different regulations with which companies would have to work to comply.

“It’s the patchwork issue that people are most worried about,” Hoffman said. The European Union’s earlier General Data Protection Regulation of 2016. Intel released its draft proposal in early November with the hopes of amending the Federal Trade Commission Act to allow the commission to enforce data privacy and security standards and allow executives to be jailed for 10 to 20 years if they are found to be in violation of the standards.

**Tech Companies Weigh In**

Tech companies also have gotten into the act, releasing their own opinions and model federal legislation for data privacy and security in response, not only to the California Privacy Act but also to the European Union’s earlier General Data Protection Regulation of 2016.

• Intel released its draft proposal in early November with the hopes of amending the Federal Trade Commission Act to allow the commission to enforce data privacy and security standards and allow executives to be jailed for 10 to 20 years if they are found to be in violation of the standards.

• IBM previously has said it would like to see a public-private approach rather than government mandates when it comes to data privacy and cybersecurity, according to an earlier report on Law.com.

• Dan covers cyber security, legal operations and intellectual property for Corporate Counsel. Follow him on Twitter @Danclarkalm.