Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy & Cybersecurity Policy To Watch In 2nd Half Of 2019

By **Allison Grande**

Law360 (July 3, 2019, 6:05 PM EDT) -- The race to get up to speed with California's landmark privacy law will heat up in the second half of 2019, while the enactment of more state privacy laws and blockbuster data protection enforcement actions in Europe will deepen companies' compliance obligations.

The focus in the next six months, attorneys say, will be on ensuring that businesses are well versed in the novel requirements set to take effect in California, Nevada and Maine, and on monitoring legislative and regulatory activity at the state, federal and international levels.

"The way these laws are enforced will determine whether they actually have any impact on the privacy and data security of companies doing business in those places," said Casey Quinn, an attorney with Newmeyer & Dillion LLP's privacy and data security practice. "Without enforcement, privacy laws will become paper tigers with no real teeth."

All Eyes on California Privacy Law

Many companies are expected to devote significant time and resources to falling into step with the California Consumer Privacy Act, which was hastily enacted in June 2018 and is set to take effect Jan. 1.

Aloke Chakravarty, co-chair of Snell & Wilmer LLP's investigations, government enforcement and white collar protection practice group, said 2019 "has been in many ways the year of CCPA, and even though it's not in effect yet, everyone in this space is watching that very closely and preparing for it to come into effect at the end of this year."

With less than six months to go until the law takes effect, companies still are largely unsure of their compliance obligations. The state Senate has until Sept. 13 to vote on a dozen proposed amendments that the Assembly has approved. If enacted, the amendments could dramatically affect the scope and reach of the law, attorneys say.

Among the proposed changes are ones that would exclude employee information, job application data, deidentified data and many insurance companies from the law; require brick-and-mortar stores to clearly disclose the use of facial recognition technology; clarify what counts as a "sale" that consumers have the right to opt out of; and allow companies to continue to run customer loyalty programs.

"We are closely watching amendment activity related to the CCPA, in particular the carveout of employees from the definition of 'consumer,'" said Heather Sussman, co-head of the cyber, privacy and data

innovation practice at Orrick Herrington & Sutcliffe LLP. "This has enormous potential impact for California businesses and so many businesses are taking a wait-and-see approach on how to handle their employee data. If the amendment does not pass, we will see a massive scramble as we get closer to the law's effective date."

Companies are also awaiting the issuance of regulations interpreting the law from the California attorney general, which are expected to be released in the coming months. Under amendments enacted last year, the attorney general has until July 1, 2020, to develop and publish rules implementing the act, and enforcement is stayed until either that day or six months after the publication of the regulations, whichever comes first.

"Given the breadth of the statute and ambiguous terms, the regulations will provide an opportunity to add greater clarity on defining 'unique identifiers' under the CCPA, the categories of personal information subject to the CCPA, and how businesses can comply with and verify consumer requests, among many other areas," said Mark Krotoski, co-head of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice.

An onslaught of private litigation is expected to begin immediately after the law takes effect. The bill still includes a narrow private right of action for data breach-related claims, although the state Assembly failed to advance an amendment that would have given consumers the ability to sue for any violation of the law.

"Many people are wondering what enforcement actions are going to look like, but the litigation activity may end up being even more pressing, and how that shakes out will be very interesting for companies who aren't in that first wave to monitor," said Pasha Sternberg, an attorney in the tech transactions and data privacy practice at Polsinelli LLP.

Given these immediate liability risks, companies can't afford to delay compliance efforts, even if they don't have the complete picture yet, attorneys stressed.

"We're at the point now where companies can't wait for clarity in the form of amendments or regulations, because doing so would just not leave enough time to become compliant," said Kristen Mathews, a partner in the global privacy and data security group at Morrison & Foerster LLP.

Even without solid guidance, many companies are already mapping their data, assessing third-party vendor risks and developing procedures to allow consumers to exercise their new data access and deletion rights, experts say.

"The biggest thing for businesses is to really understand where their data is, who has access to it and how to control who has access to it," said Stacy Scott, a managing director in Kroll Inc.'s cyberrisk practice. "The California law is still in place, and any amendments won't affect the need for companies to know where their data is."

Nevada, New York Won't Be Left Out

California is far from the only state that will bear watching in the coming months.

"In the second half of 2019, we'll begin to see whether the CCPA's progeny are likely to gain traction in state legislatures," said Reece Hirsch, the other co-head of Morgan Lewis' privacy and cybersecurity practice.

Privacy proposals that have been "influenced by the CCPA to one degree or another" have been floated in state legislatures across the country, and if several of those bills are enacted, "the U.S. privacy regulatory landscape will in short order become much more complex and challenging for businesses," Hirsch added.

The anticipated spread of state privacy laws has already started, with Nevada and Maine somewhat quietly enacting consumer privacy laws that, while narrower than the California statute, still promise to have a significant impact on companies.

Nevada's Senate Bill 220, which was enacted in May and takes effect Oct. 1, gives consumers the broad right to opt out of the sale of their personal information. While the law doesn't encompass the sweeping data access and transparency requirements contained in the California law, it still potentially affects many of the same companies that will need to comply with the CCPA, Quinn noted.

"This means that if they were already planning to comply with the CCPA by year's end, they will either need to move up their date to October or create a separate method for dealing with Nevada consumers," Quinn said.

The Maine law, which took effect July 1 and is specifically aimed at internet service providers, will also muddle the compliance landscape. The legislation requires ISPs to get users' consent before "using, disclosing or selling" data like consumer browsing history, geolocation information, financial data and health data.

"Everyone knows that they have until Jan. 1 to comply with the California law, and all of a sudden here comes Maine and Nevada with pretty quick turnaround times to get these processes into place," said Sheryl A. Falk, co-leader of the global privacy and data security task force at Winston & Strawn LLP.

The moves by Maine and Nevada demonstrate a growing appetite among state legislatures to act "sooner rather than later," Chakravarty noted. This also signals the high likelihood that more states will soon join the fray, according to attorneys.

"The recent enactment of privacy laws in Nevada and Maine shows that there may yet be additional states that enact new privacy laws before the year is out," said Janis Kestenbaum, a partner in the privacy and security practice at Perkins Coie LLP. "Anything is possible in terms of what actually crosses the legislative finish line this year."

One state to watch in particular is New York, which is considering legislation that would go beyond the California privacy law by establishing a broad private right of action and requiring businesses to act as "data fiduciaries" that are barred from using personal information in a way that benefits them to the detriment of their users. The New York Privacy Act would also apply to all businesses and not just those that have more than $25 million in revenues a year**,** which is the threshold for having to comply with the California law.

"Having a private right of action is always very scary for businesses and potentially opens the door to significant liability," Davis & Gilbert LLP partner Gary Kibel said.

Attempting to manage the more onerous and conflicting elements of this emerging state law patchwork is likely to result in "a compliance nightmare" for businesses, according to Sussman. That drives home the importance for companies in the next six months and beyond to engage in data mapping, inventory and vendor management exercises that are likely to help them bridge the gaps in their compliance obligations, experts said.

"Where many of these laws are overlapping is in their focus on how companies are handling the content that they're maintaining for consumers," said Reggie Pool, senior director at HBR Consulting. "So having good data hygiene, meaning understanding what kinds of data you have, how you're protecting it and how you're getting rid of it once it's past its usefulness, will likely get companies 90% toward meeting their compliance obligations."

Federal Privacy Legislation Still in the Cards

While the momentum that had been building for federal lawmakers to push national privacy legislation across the finish line is beginning to dwindle, attorneys say they aren't quite ready to declare the issue dead for this year.

"The fact that data privacy is a nonpartisan, growing concern means that it is ripe for relatively speedy introduction and passage into law," Quinn said. "Congress has already introduced as least 15 privacy-related bills this year and more are expected. Given the current environment and the numbers of states getting into the regulation of data privacy, it would not be surprising to see new federal laws that complement or even preempt these new state laws."

In the Senate, a bipartisan working group that includes Commerce Committee Chairman Roger Wicker, R-Miss., and Ranking Member Maria Cantwell, D-Wash., has been formed to draft national privacy rules. The group could release a proposal as soon as this month, and their progress will be closely watched as a strong indicator of the prospects for federal privacy legislation.

"Our focus on the federal level is on whether Congress can pass by the end of the year comprehensive privacy legislation that would preempt states and provide a national standard," said Ed Pagano, a partner at Akin Gump Strauss Hauer & Feld LLP.

As always, the devil will be in the details of those bills, Pagano noted, and squabbles over how any comprehensive legislation defines personally identifiable information, the degree to which the law would preempt more stringent state statutes and who should be charged with enforcing the rules are likely to continue to stall these efforts.

"Just like the states, federal lawmakers have a lot of ideas about what they'd like to see in federal privacy legislation," Pagano said. "That's why everyone's so anxious to see what the Senate group comes up with."

Still, several factors are working against the enactment of federal privacy rules in the coming months, including staunch opposition voiced by key lawmakers to a law that would completely preempt stronger state protections and the emergence of other significant privacy-related issues, including antitrust probes into major tech giants and growing election security concerns, according to Mark W. Brennan, a partner in the global regulatory practice group at Hogan Lovells.

"Severe weaknesses with the CCPA spurred much of the drive for comprehensive federal privacy legislation this year, but the chances seem increasingly slim absent additional state activity," Brennan said.

FTC's Facebook Privacy Action Hits Home Stretch

The Federal Trade Commission in March 2018 pounced on reports that Facebook had failed to do enough to keep political consulting firm Cambridge Analytica from harvesting personal data belonging to millions of

unwitting Facebook users, and the commission's closely watched probe into these issues is likely to conclude within the next couple months.

"The FTC's credibility is on the line with this Facebook investigation," said Joel Reidenberg, a professor and founder of the Center on Law and Information Policy at Fordham University School of Law.

Facebook disclosed in an April securities filing that it expects to pay between $3 billion and $5 billion to resolve the FTC's probe, and media reports have indicated that the fine will be accompanied by robust remediation and monitoring provisions.

Given that the commission has been "sitting on" the investigation for more than a year, a failure to put together a deal that's strong enough to appease privacy advocates could call into question the FTC's competence to enforce arrangements such as the transatlantic Privacy Shield data transfer mechanism, according to Reidenberg.

The issue of how much power the FTC should be given to crack down on privacy and data security violations is a major sticking point in discussions over federal privacy legislation. The commission has pushed for Congress to give it enhanced rulemaking authority and the ability to sue for first-time privacy violations, but advocacy groups have argued that the creation of a new independent watchdog is necessary.

"Giving the FTC more powers to enforce privacy laws would be very significant for companies regulated by the agency," Kibel said.

Attorneys are also expecting to see continued activity in the privacy space from agencies such as the U.S. Securities and Exchange Commission, which has been stepping up its scrutiny of both public companies' cybersecurity disclosures and of emerging technologies such as cryptocurrencies, and the Federal Communications Commission.

“The Telephone Consumer Protection Act and robocalls have been getting a lot of attention at the FCC and in Congress lately, and we expect that trend to continue into the second half of the year," Brennan said.

GDPR Enforcement Actions on the Horizon

More than a year after the European Union's sweeping General Data Protection Regulation went live, businesses around the world are still bracing for the first enforcement action that fully capitalizes on national data protection authorities' enhanced power to levy massive fines of up to 4% of companies' global annual revenue.

While regulators have taken a somewhat cautious approach so far, all indications point to major enforcement actions on the horizon, especially in light of Irish Data Protection Commissioner Helen Dixon's recent disclosure that her office is expecting to wrap up GDPR investigations related to Facebook, Twitter, Apple and other U.S.-based tech giants this summer.

"It seems all but certain that regulators on both sides of the Atlantic will be flexing their muscles in the privacy sphere in the latter half of 2019," Kestenbaum said.

Attorneys will particularly be watching to see how the enforcers deal with the influx of data breach notifications they have received under the regulation's requirement to report serious data breaches within 72 hours. Regulators have yet to announce an enforcement action tied to this obligation, and the first such

undertaking will be particularly instructive to companies.
"There is a lot of anticipation to see what kind of consequences will actually happen and whether the type of fines permitted by the GDPR will actually be issued," Quinn said. He added that Ticketmaster and British Airways, both of which experienced credit card skimming breaches, "are awaiting their fates, which will give us a good indication of what to expect."

--Editing by Kelly Duncan and Bruce Goldman.