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

Cybersecurity & Privacy Policy To Watch In 2019

By **Allison Grande**

Law360 (January 1, 2019, 12:03 PM EST) -- Momentum is expected to build significantly in 2019 for the enactment of a comprehensive federal privacy framework in the U.S., while the pair of laws that played a major role in fueling these efforts — California's landmark Consumer Privacy Act and the European Union's General Data Protection Act — will continue to loom large, according to attorneys.

Here, experts flag the top policy developments in the privacy and cybersecurity world that they'll be tracking closely in the upcoming year.

Federal Privacy Legislation Picking Up Steam

Privacy law in the U.S. has long consisted of a patchwork of state-level protections and federal statutes that regulate certain industries, such as health care and financial services. But attorneys say momentum is steadily building for a uniform federal approach to privacy regulation, and 2019 may finally be the year that this vision comes to fruition.

"We've had all these false starts over the past half dozen years or so, with data breach notification bills being proposed at the federal level but going nowhere," said McDermott Will & Emery LLP partner Mark E. Schreiber. "But now, there seems to be a bit more appetite to do something in the current Congress and to try to reach some compromise on a federal privacy law."

The momentum has largely been fueled by recent developments in the European Union, where the sweeping General Data Protection Regulation took effect in May, and in California, where a first-of-its-kind consumer privacy law was passed in June. Both laws have forced companies to rethink the way they collect, use and share consumer data, and have further expanded the global patchwork of privacy requirements for businesses.

"With GDPR and now the new California law, what we're seeing is greater complexity when it comes to cybersecurity and privacy regulations," Schreiber said. "What has the potential to alleviate, at least on the corporate side, some of these complexities is if things could be simplified, and the easiest way to do that is to formulate some uniform standard."

While companies have traditionally either opposed or kept quiet on the topic of creating a federal privacy standard, many in the corporate world have recently begun speaking up and throwing their weight behind the idea.

A broad coalition of more than 200 retailers, banks and technology companies in December released recommendations for national privacy legislation, and the privacy advocacy community, White House and Federal Trade Commission have also pushed Congress to act by floating their own proposals about what shape federal privacy legislation should take.

"With all these stakeholders seemingly getting on the same wavelength, there could finally be a meeting of the minds about what's necessary to craft a U.S. approach to comprehensive federal legislation," said Alan Charles Raul, leader of the privacy and cybersecurity practice at Sidley Austin LLP.

Federal lawmakers have also been demonstrating an increased appetite for privacy legislation. Senate Commerce Committee Chair John Thune, R-S.D., held a pair of hearings beginning in late September to hear from businesses such as Google and Amazon and privacy advocates including the Center for Democracy and Technology, and the incoming Democratic leaders of key House committees have signaled in recent weeks their interest in this area.

"Since privacy isn't a highly partisan issue — or at least has not been to this point — it's possible that there could be a basis for consensus across the aisle for federal privacy legislation," Raul said. "But as always, the devil is in the regulatory details."

The extent to which any federal law should preempt more stringent state-level laws, including California's new Consumer Privacy Act, and whether consumers should be allowed to bring lawsuits are likely to be the most fertile areas for disagreement, attorneys say.

"The major wild card that could change this would be if three to five states beyond California pass their own state privacy laws — that might 'force' a broader consensus as a defensive measure," Wiley Rein LLP privacy practice chair Kirk Nahra said.

But regardless of where the debate ends up, companies and other interested stakeholders would be wise to stay engaged and involved in these efforts in the upcoming year, attorneys say.

"I encourage companies across the board to get involved in this debate — it is going to be extensive and loud for several years, with real ramifications for a broad range of data practices across virtually every industry," Nahra said.

California Consumer Privacy Act Takes Center Stage

California lawmakers took the privacy world by storm in June, when they hastily enacted stringent consumer privacy rules to head off a more stringent ballot initiative. The landmark statute, known as the California Consumer Privacy Act, hands consumers the ability to control how companies use and share their personal information online, to request the deletion of this information and to opt out of the sale of their data to third parties.

"The California law is a game-changer because it introduces to the U.S. several concepts of the GDPR regime, including the right to be forgotten and other consumer rights that we haven't seen yet in the U.S.," said Locke Lord LLP partner Ted Augustinos.

While the law isn't slated to take effect until Jan. 1, 2020, companies will have their hands full in 2019 getting in step with the new regime, which is widely expected to undergo at least some revisions by

lawmakers before it comes into force.

"2019 is going to be the year when the battle is waged over what the CCPA is ultimately going to look like, and whether concessions are made to business interests to make the law less burdensome or whether it remains more or less the same," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

Both business groups and consumer advocates have already begun pressing lawmakers over the more contentious issues, including the statute's current broad definition of "personal information" and the scope of the private right of action that consumers would gain to wield against companies that suffer data breaches. Most recently, a coalition of more than a dozen privacy groups rallied against the business community's efforts to scale back the law, arguing in a December letter that consumers' data access and control rights need to remain strong and that their ability to bring lawsuits should be broadened.

"The battle is on, and it will be interesting to see where it ends up," Hirsch said.

However, even with uncertainty swirling over what the final version of the law will look like, attorneys agreed the basic principles of the law — particularly elements for providing notice and obtaining consent from consumers and allowing them to access and delete their data — are likely to remain unchanged, and that companies' compliance efforts need to begin now.

"January 2020 will be here soon enough, and it's important for companies to start thinking about what data they hold and how to comply with the many new consumer rights in the statute," said Mark Krotoski, the other co-head of Morgan Lewis' privacy and cybersecurity practice. "Starting early in 2019 will allow companies to do this in a measured way rather than waiting until the end of the year and racing toward compliance."

Attorneys recommend beginning with the task of understanding what data the company holds, how it's being used and with whom it's being shared, and letting go of any data that isn't necessary to retain in order to reduce data security risks.

"Without knowing what you have and what you're doing with it, you can't build a compliance program," said Alexander Bilus, vice chair of Saul Ewing Arnstein & Lehr LLP's cybersecurity and privacy practice. Bilus added that this exercise will also prove useful in complying with the requirement that businesses be able to provide consumers with their data going back to January 2019, or one year before the act takes effect.

These data inventory and mapping efforts are similar to what companies undertook in advance of the May launch of the GDPR, attorneys said, and are likely to go a long way toward helping to reduce their liability under the new California law, no matter what form it ultimately takes.

"These are key tenets of the California law that are unlikely to change, and focusing on what data they're collecting, how they're using it and who they're sharing it with will help them not only get a head start on the CCPA but will also be important for them in operationalizing certain aspects of other privacy laws," said Erin Illman, co-chair of Bradley Arant Boult Cummings LLP's cybersecurity and privacy practice group.

Companies will also need to keep an eye on how other states respond to California's groundbreaking

move, according to attorneys.

"It will be interesting to watch how the CCPA develops and whether more states start stepping in and passing additional privacy laws that are similar to or inspired by it," said Seth Berman, leader of Nutter McClennen & Fish LLP's privacy and data security group, adding that statutes like the CCPA are "likely to be the next frontier of privacy law in America."

As state legislatures develop these laws, attorneys said, all eyes will be on whether they decide to take an approach that's in step with the stringent California law, which creates the opportunity for consumers to bring data breach claims and collect damages of between $100 and $750 per violation from companies that allegedly fail to implement reasonable security, or if they decide to follow the lead of Ohio, which in 2018 also enacted a first-of-its kind law that provides a liability shield for some claims in data breach litigation for companies that implement a written cybersecurity program that "reasonably conforms" to at least one of 11 industry-recognized cybersecurity frameworks.

"There have clearly been a lot of new ideas getting introduced, like the Ohio law and the CCPA, so it will be interesting to see other states looking at some of these models and trying them out a little bit," Hirsch said.

The adoption of these types of laws is likely to be similar to, but quicker than, the adoption of state data breach notification statutes, which began in California in 2003 and finished spreading to all 50 states in early 2018, when Alabama became the last state to enact such requirements, attorneys added.

"Until there's some sort of federal regulation, states are going to continue to regulate to protect their citizens," Crowell & Moring LLP partner Evan Wolff said.

GDPR Will Still Loom Large

Multinationals with a presence in the EU had their world shift dramatically on May 25, when the sweeping GDPR put new restrictions on their handling and use of a wide range of personal data. But while the compliance date has come and gone, there's still plenty for companies to consider under the groundbreaking regulation in 2019, attorneys say.

"GDPR is already pretty hot, but it's going to be even hotter in 2019 as some companies are still waking up and realizing that even though it's been in effect for six months, they may be subject to the regulation, or maybe they're finding out they had a data incident that affected a few thousand people in various regions, including the EU," said BakerHostetler partner Eric Packel.

Many companies may have been relieved to find that after two years of lead-up time to the compliance deadline, "the sky didn't fall" when the regulation took effect, Schreiber said.

However, that doesn't mean GDPR work isn't an ongoing effort that will march on for years to come, attorneys said.

"If you asked one of the EU data protection authorities, they would probably say that the whole point of GDPR is for it to be an ongoing exercise," Berman said.

These compliance efforts are likely to include not only determining whether and to what extent the regulation applies to companies' current businesses models — a recent survey by IT Governance of 210

EU-based organizations found that only 29 percent of respondents reported having fully implemented the GDPR — but also making sure their compliance plans gel with any new initiatives, attorneys say.

"Things change, so companies might have new vendor relationships or new uses of data that require revisiting GDPR to make sure they remain compliant," Augustinos said.

Externally, the most intriguing development that companies will be watching carefully in the upcoming year is how regulators choose to wield their authority under GDPR to bring enforcement actions and levy fines of up to 4 percent of a company's global annual revenue, according to attorneys.

"The regulation left much to be interpreted, and many are waiting to get a sense of the regulators' priorities as well as how and against whom they will seek to enforce the law," Berman said.

Enforcement is likely to fall into at least two buckets, according to Liisa Thomas, leader of Sheppard Mullin Richter & Hampton LLP's privacy and cybersecurity practice. These include actions involving data breaches that trigger reporting under the regulation's tight 72-hour notification window and that the regulator feels were caused by inadequate security, and those that center on alleged failures to provide consumers with the various data access and redress rights enshrined in the statute.

"GDPR enforcement is going to be the big ticket item for 2019," said Morrison & Foerster LLP privacy & data security co-chair Alex van der Wolk, who is based in the EU. "Companies have had a year to get their houses in order, so this year is going to see the next step."

The newly formed collective of national regulators known as the European Data Protection Board is also expected to offer guidance on how to interpret key provisions of the GDPR in the coming months that companies will want to carefully track, attorneys say.

"Every company has got to be jumping on new guidance as it comes out from the EDPB," said McDermott partner Ashley Winton, who is based in London.

Companies should also keep an eye on separate efforts by policymakers to replace the bloc's current e-privacy directive with a more stringent regulation. Lawmakers had said they were hoping to finalize the new regulation — which would expose tech companies such as Facebook and Google that fall outside the traditional telecom space to tighter rules for handling electronic communications and carrying out digital marketing — sometime in 2018 or by early 2019. Delays and squabbles over the proposed regulation's scope have made it likely that the process won't be wrapped up until later this year.

"The uncertainty around timing is a huge issue for companies in both the EU and globally," van der Wolk said. "Companies put a lot of effort into complying with the GDPR and had momentum going that they wanted to use to pick up e-privacy, but they still can't because it hasn't been finalized."

Federal Regulators Not Slowing Down

The regulatory environment at the federal level in the U.S. is also expected to remain active in the privacy and data security arena in the upcoming year, according to attorneys.

The Federal Trade Commission has long been considered the top privacy watchdog in the U.S., but how the Republican-led commission — which was restocked with a full slate of five new commissioners in 2018 — will tackle these issues remains to be seen. The commission held a two-day hearing in

December as part of its ongoing series on competition and consumer protection in the 21st century to discuss a range of data security issues, and will convene another hearing in February to explore the commission's remedial authority to deter unfair and deceptive conduct in the privacy realm.

"I will be watching whether the FTC takes on any meaningful privacy case," Nahra said. "They have built a strong history of data security cases over time ... but they haven't done as much to establish real boundary lines on privacy, beyond deception cases. Is there something on privacy that the FTC will find to be 'unfair'?"

Attorneys hope the FTC will deliver more clarity on the issues of what constitutes "unfair" privacy practices and "reasonable" data security in 2019, and also anticipate that there will be a continued push for Congress to give the commission stronger and clearer authority to go after such violations and levy fines.

"When it comes to federal privacy legislation, the debate is not only about whether we are overregulating companies, but on the other hand, are we doing enough to protect consumers by giving agencies like the FTC enough ammunition to go after companies," said Andy Gandhi, a managing director with Alvarez & Marsal's disputes and investigations practice and data risk expert. "The FTC doesn't have that power yet, but there will at least be conversations about giving the agency powers to go in and help remediate those issues."

The U.S. Securities and Exchange Commission also made a splash in the privacy arena during the past year with enforcement actions such as its first-ever settlement under its identity theft red flags rule with broker-dealer Voya Financial Advisers Inc. and the October revelation of it plans to launch a new slate of enforcement actions against public companies that fail to enact sufficient accounting controls to guard against cyberattacks. Attorneys expect the securities regulator to continue to be active in 2019.

"Cybersecurity and privacy issues are not going away and seem to be getting worse, so the SEC is likely to continue to feel a need to step in and assert itself as one of the main regulators at least for public companies on these issues," Berman said.

The U.S. Department of Health and Human Services' Office for Civil Rights, which has slowed down its enforcement pace in recent years but is still raking in significant fines in health privacy enforcement actions, will also continue to be a contender in the regulatory space in the upcoming year, attorneys predicted.

"OCR did very little for almost two years, but seems to be heating up again somewhat," Nahra said, noting that the lull coincided with staff turnover and other factors that focused leadership attention's elsewhere. "I hope that they will continue to be as thoughtful in their enforcement as OCR historically has been."

TCPA To Get FCC Makeover

Litigation under the Telephone Consumer Protection Act has exploded in recent years, as class action plaintiffs seek to capitalize on unclear statutory language and the potential for uncapped penalties of between $500 and $1,500 per violation. However, relief may be in sight for companies as the Federal Communications Commission is expected to issue declarations in the coming year that could help narrow liability under the decades-old law.

"The TCPA is in an unprecedented state of flux. And that is saying something, given that the regulatory approach to the TCPA has never been marked by consistency or clarity," said Drinker Biddle & Reath LLP partner Michael P. Daly. "In 2019 the FCC will have an opportunity to provide predictability that is much needed and long overdue."

The FCC is likely to start by addressing issues that were upended by the D.C. Circuit's March ruling in ACA International v. FCC. In that case, the appellate court narrowed a 2015 FCC order that expanded the scope of the TCPA, finding the commission's broad definitions of "automatic telephone dialing system" and "called party" under the statute were unreasonable and arbitrary.

However, the decision left open the questions of what is required for a system to qualify as an autodialer and the scope of liability for calling reassigned numbers, leaving it squarely up to the commission — which has solicited public comment on these topics and separately voted in December to create a reassigned number database to help ease liability — to again take a shot at defining these terms.

Given that courts have issued widely differing opinions on the scope of the autodialer definition post-ACA — including a recent Ninth Circuit decision that reached the opposite conclusion from the D.C. Circuit on the validity of the FCC's broad take on that term — "it will be interesting to see how the FCC's rules are received in jurisdictions where judicial precedent conflicts with those rules," according to Jaszczuk PC partner Margaret Schuchardt.

Ultimately, the FCC's move to answer any of the crush of outstanding questions under the 1991 statute has the potential to "go a very long way toward reducing predatory litigation and focusing our attention on the scam artists that the statute was really meant to address," Daly said.

--Editing by Emily Kokoll and Marygrace Murphy.