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 Legislation And Regulation To Watch In 2023

By **Allison Grande**

Law360 (January 2, 2023, 12:02 PM EST) -- The new year kicks off with California and Virginia's new privacy laws taking effect, and things will only ramp up from there, with privacy professionals keeping a close eye on long-standing efforts to enact a federal data privacy framework and the Federal Trade Commission's increasingly aggressive approach to regulating data-handling practices.

More states are also expected to jump on the privacy law bandwagon in 2023, and the anticipated finalization of a key deal allowing personal data to again flow freely between the European Union and U.S. is expected to bring some relief to companies, attorneys say.

"2023 is shaping up to be a huge year for both privacy enforcement and for continued privacy law development in the states, at the federal level and internationally," said Reed Freeman, partner and co-chair of the privacy and data security practice group at ArentFox Schiff LLP. "In particular, I think that when all is said and done, we may look back on 2023 as a watershed enforcement year for the FTC and [California's new privacy agency]."

Here, Law360 looks at some of the legislative and regulatory developments that will be at the top of practitioners' minds in 2023.

State Privacy Laws Go Live

Since California in 2018 became the first state to enact legislation giving consumers more access to and control over their personal information, four more states have added to the patchwork, and voters in the Golden State have moved to strengthen their landmark law by adding substantial new data control mechanisms and creating the first U.S. agency dedicated to data privacy.

All of these protections are slated to roll out over the course of 2023, with the Virginia Consumer Data Protection Act and the California Privacy Rights Act going live on Jan. 1, similar privacy laws in Colorado and Connecticut becoming effective on July 1 and Utah's privacy law entering into force on Dec. 31.

"The biggest issue for businesses has been how to develop a cohesive privacy program that's both implementable within the company and also achieves compliance with all five state laws, which is hard to do when you have five disparate laws," said Lisa Sotto, who chairs the privacy and cybersecurity practice at Hunton Andrews Kurth LLP.

The laws generally give consumers the right to access, correct, delete and opt out of the sale or

processing of their personal information for the purposes of targeted advertising and profiling. But they also contain important differences — including inconsistent requirements for dealing with consumer opt-out requests, how to handle sensitive information and which entities are covered — that companies will need to figure out how to account for in their compliance plans.

"Ultimately, there are more nuances in these state privacy laws than appear at first glance, and that's something everybody is starting to realize as they put in place and operationalize their programs," said Nancy Libin, partner and co-chair of the technology, communications, privacy and security practice at Davis Wright Tremaine LLP.

As companies work to build their compliance plans, regulators in California and Colorado continue to march toward finalizing the regulations that the state legislatures have charged them with drafting.

The new California Privacy Protection Agency and Colorado's attorney general can begin enforcing their respective laws on July 1. Both regulators have issued draft regulations on how they intend to interpret key requirements like privacy policy disclosures, consent and consumer opt-outs, and they're expected to finalize these rules in the coming months.

"This will be a big year as companies try to get everything in line to prepare for the inevitable enforcement actions that regulators will start to bring, and it's going to be interesting to get some clarification through those actions and hopefully through guidance from state regulators about the complicated issues that these laws present," Libin said.

One of the main issues that companies will have to grapple with is whether and how to implement a universal browser-based mechanism that consumers can use to opt out of the sale or use of their data for targeted advertising across the internet.

The California and Colorado regulators have made clear that they expect companies to honor these opt-out signals, which save consumers from having to go to each site they interact with to stop the sale and sharing of their data. But the business community has raised concerns about the difficulty of how to technologically recognize and respond to these signals.

"On the one hand, most consumers would probably say that they really like global privacy controls because those would give them a one-stop shop to stop or limit the use of their personal information," said Robert Braun, co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP. "But on the other hand, the way it is right now, every company would need to be able to identify every type of browser opt-out signal and be ready to recognize it, and that would be a pretty significant burden."

All five of the new laws going effective this year will also force companies to be more transparent in their dealings with consumers, including in their privacy policies, which consumer advocates have long criticized for being too long and unwieldy. Businesses will also have to undertake data protection assessments and revamp deals with vendors to ensure that they're adequately handling and protecting consumer data.

"Gone are the days when you can just throw out a quick privacy notice from a template and be done with it," said Liz Harding, a shareholder and vice chair of technology transactions and data privacy at Polsinelli PC. "The privacy landscape is becoming more and more complex and there's more and more that businesses have to cover."

The expansion of the privacy law landscape is also drawing in more types of companies. Colorado's law is the only one to cover nonprofits, and the revised California law will for the first time apply to employees, contractors and job candidates after the state legislature failed to extend or permanently enshrine an exemption in its current privacy law for employee and business-to-business data.

"This means that employers need to present robust privacy policies to their California employees and give them numerous rights, some of which will be challenging to honor in the context of employer-employee relationships, such as the right to have their personal information deleted or corrected by the employer, the right to receive a copy of their personal information that is held by their employer and the right to opt out of their employer using their personal information for certain purposes," said Kristen Mathews, a partner in the global privacy and data security group at Morrison & Foerster LLP.

In addition to keeping a close eye on the implementation and enforcement of the five new privacy laws, privacy practitioners will also be watching to see if "additional states pick up the mantle of comprehensive privacy legislation and, if so, if they continue to adopt a model more like Virginia and Colorado than California," which is considered more stringent than other states, noted Libbie Canter, a partner at Covington & Burling LLP.

Several states have made strong pushes but have fallen short of enacting their own protections in recent years, including Washington and Florida. These locales and others like Massachusetts, New York, Minnesota, Oregon and Maryland are expected to again mount serious efforts to add to the expanding patchwork, which Congress has thus far declined to preempt.

"If more states enact privacy laws as expected, that certainly adds risk, since the more divergent laws there are out there, the greater the risk that companies are going to miss something," said Christopher Wall, data protection officer and special counsel for global privacy and forensics at e-discovery company HaystackID.

Another Try for Federal Legislation

In 2022, Congress made the most progress to date on long-running efforts to enact federal privacy legislation, with the House Commerce Committee in July easily advancing the American Data Privacy and Protection Act. ADPPA would give consumers the right to access, correct, delete and stop the sharing of their personal information, enhance data protections for children and teens, and clamp down on algorithmic bias.

However, the bipartisan measure ran into opposition from key leaders, including House Speaker Nancy Pelosi, a California Democrat who objected to the federal bill overriding the more stringent privacy protections in her home state. With Democrats keeping control of the Senate and Republicans claiming a slim majority in the House, attention will turn to whether Congress can ride last year's wave to finally get federal privacy legislation across the finish line.

"Every year, the issues become clearer, the cost becomes clearer and the need for consistency becomes clearer," said Braun, of Jeffer Mangels. "In the new divided Congress, they're likely going to be looking for areas of consensus, and privacy is something where they could really find common ground."

As has been the case for nearly a decade, the latest push for federal privacy legislation was again derailed by disagreements over whether consumers should be allowed to sue companies for alleged

violations and whether more stringent state laws should be preempted.

Pelosi and her fellow California Democrats have been the main opponents of the federal law preempting the five state privacy statutes currently on the books, while Senate Commerce Committee Chair Maria Cantwell, D-Wash., has argued that the bill's enforcement mechanism — which would allow consumers to bring lawsuits after notifying certain state and federal regulators beginning two years after the law takes effect — is "too weak" to pass as currently drafted.

While Cantwell is likely to retain her position in the Senate, the House will look much different next term. Pelosi has announced that she's stepping down from her leadership roles, and Democrats have elected Rep. Hakeem Jeffries of New York to take over as head of the party in the next Congress, a shift that may give a boost to the drive to enact a uniform federal privacy framework, experts say.

"Speaker Pelosi has said she wouldn't allow the ADPPA to be considered by the House, but with a change in House leadership, there might be some movement on that front in 2023," said Wall, of HaystackID.

But in a divided Congress that has yet to fully solve the long-standing squabbles over preemption and enforcement, enactment of a federal privacy standard is still far from certain, attorneys noted.

"While privacy may be an issue that's bipartisan enough where the parties can get together and get something done, on the other hand, if Congress couldn't get it done when one party was in control, are they really going to get it done when there's one party in the House and another in the Senate?" asked Tracy Shapiro, a partner at Wilson Sonsini Goodrich & Rosati PC. "That creates an even bigger hurdle, and if history is an indicator of the future, it seems like we're not getting a federal privacy law anytime soon."

FTC Enforcement Continues to Heat Up

Under the leadership of Lina Khan, a Democrat who assumed the helm in June 2021, the Federal Trade Commission has been steadily turning up the heat on how companies handle, share and secure personal data, and the coming year looks to be no different.

"Statements from FTC Chair Lina Khan and other regulators make clear that we can expect to see continued robust enforcement of data protection requirements," said Martin Tully, a partner at Redgrave LLP.

In the past year, the FTC has pushed the envelope in enforcement actions, including forcing CafePress to take the unprecedented step of instituting multifactor authentication as part of a data breach settlement and suing mobile app analytics provider Kochava Inc. for allegedly selling geolocation information that can be used to track people to reproductive health care clinics and other sensitive places.

Instead of settling these claims as most companies do, Kochava has pushed back hard on the FTC's allegations, arguing that the commission has provided "no facts" to show how the disclosure of consumers' whereabouts causes harm to them and filing its own suit arguing that the agency lacks the authority to press its claims.

Covington & Burling's Canter said she'll not only be watching the Kochava matter, but also monitoring

"to see if other defendants challenge the FTC's authority over the next year."

To go after companies for alleged consumer privacy and data security violations, the commission has long relied on its authority to police deceptive practices under Section 5 of the FTC Act. But the agency under Khan has shown a greater willingness to use its authority under Section 5 to assert that a specific practice is likely to cause substantial and unavoidable injury to consumers.

The FTC leaned heavily on this authority in August when it launched an ambitious effort to craft sweeping data privacy and security rules. The commission called for input on 95 questions that are intended to guide the agency as it seeks to set limits on the business of collecting, analyzing and profiting from consumers' data — a practice the agency has termed "commercial surveillance" — and to crack down on lax data security practices.

While the rulemaking is expected to last several years and will likely span presidential administrations, attorneys will be watching how the commission responds to the more than 11,000 comments it received by the close of the public feedback period in November and which of the topics in its broad inquiry — which touches on targeted advertising, artificial intelligence, algorithmic bias, biometrics, data minimization and protections for children and teens online — the agency chooses to focus on moving forward.

"We're waiting to see what the FTC does with its rulemaking, which is going to have a big impact on companies, and of course the big question will be whether the FTC will stay within the four corners of its statutory authority or if it exceeds that authority," said Libin of Davis Wright Tremaine.

The FTC has already faced backlash to the breadth of its rulemaking efforts, including from three Republican senators who have argued that the commission needs to "leave the task of creating data privacy and security rules to the elected officials in Congress."

However, "while the political environment and rulemaking landscape remain somewhat unsettled, organizations would be wise to proactively seek to comply with evolving data privacy and cybersecurity requirements they may be subject to," said Redgrave's Tully. "Otherwise, they risk being made an example of by fired-up regulators."

EU-US Data Transfer Pact Revived, but Challenges Loom

Since the European Court of Justice in 2020 struck down the popular Privacy Shield mechanism used by thousands of multinational companies to move personal information from the European Union to the U.S., such businesses have had to rely on the more complex standard contractual clauses that require them to assess whether there are sufficient privacy protections in place for each data transfer, as well as binding corporate rules that need to be approved by national data protection authorities.

"The issue of international data transfers has remained a thorn in the side of most privacy managers dealing with the aftermath of the [Court of Justice's] decision," said Robert Grosvenor, managing director and co-head of the global privacy practice in Alvarez & Marsal's disputes and investigations practice in London.

However, "on a brighter note," U.S. and EU leaders revealed in March that they'd reached a deal to replace Privacy Shield, and President Joe Biden in October signed off on enhanced protections for how the U.S. intelligence community handles EU residents' personal data and fields government

surveillance complaints, Grosvenor said.

The bolstered safeguards, which are meant to address the concerns that led the Court of Justice to strike down Privacy Shield, are currently under review by the European Commission, which must issue a declaration finding the new protections to be adequate before the Trans-Atlantic Data Privacy Framework can take effect. The commission released a draft adequacy decision on Dec. 13, and it's expected to finalize the deal within the next six months.

"The new framework would offer to companies that are transferring EU data to the U.S. a much more streamlined approach that is certainly more economically effective and efficient," said Sotto, of Hunton Andrews Kurth.

But while the framework will almost certainly be approved by the European Commission, its staying power remains uncertain.

Max Schrems, the Austrian privacy advocate who launched the legal challenges that led to the demise of Privacy Shield and its predecessor, Safe Harbor, has already vowed to fight the new deal. He's argued that the Biden administration's commitments to put tighter restrictions on how U.S. officials conduct signal intelligence activities involving transferred data and to create an independent Data Protection Review Court to handle EU residents' grievances don't go far enough in providing EU citizens safeguards and redress from use of their data by U.S. intelligence authorities.

The looming legal challenge again leaves companies in a position to decide whether to adopt a data transfer mechanism that may soon be invalidated, or wait to see how the review process plays out. Attorneys anticipate that most companies that transfer personal data from the EU to the U.S. for data breach investigations, human resources purposes and a host of other reasons are likely to certify their compliance to the new framework, although they'll have to keep a close eye on how legal process plays out.

"Companies should take advantage of this framework with the understanding that the data transfer regime is always subject to change," Sotto said. "At the least, the implementation of the framework will buy a few years of peace, and hopefully the Biden administration's executive order and new agreements reached between the U.S. and EU will go a long way toward quelling the fears expressed by the European Court of Justice."

--Editing by Alanna Weissman and Rich Mills.
