LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th 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 2024

By **Allison Grande**

Law360 (January 1, 2024, 8:02 AM EST) -- The red-hot data privacy and security arena shows no signs of cooling off in 2024, with the enforcement of several new state privacy laws expected to heat up and artificial intelligence continuing to drive the creation of regulations at an unprecedented clip.

Practitioners are also expecting more state privacy laws to join the 13 that are already on the books and for regulatory bodies to continue to be active, especially when it comes to holding executives liable for cybersecurity-related disclosure deficiencies.

Here are some of the top policy developments that will bear tracking in 2024.

The Growth of State Privacy Laws, Enforcement

The state data privacy law landscape more than doubled in 2023, with Iowa, Indiana, Tennessee, Montana, Florida, Texas, Oregon and Delaware joining the five other states that had previously enacted comprehensive laws, and attorneys are expecting this trend to continue in the new year.

"I certainly expect there to be more [comprehensive data privacy] laws in 2024," Kirk Nahra, co-chair of the cybersecurity and privacy practice at WilmerHale, said. "The key issue in my mind is whether any of these laws will push the envelope in a way that creates new challenges for corporate America."

While the new laws contain variations in the scope of coverage and how to inform consumers of their new rights, they are largely consistent in requiring companies to ensure that consumers are able to access, delete, correct and opt out of the sale and sharing of their personal information.

However, if states begin enacting laws that take novel steps like requiring blanket opt-in consent for the collection and use of all personal information or allowing consumers to sue for alleged violations, that could not only lead to compliance challenges for companies but also a stalemate in Congress, which made no significant progress during the past year on long-running efforts to put in place a nationwide data privacy framework.

"I had previously thought that having this many state laws would have led companies to push Congress for a national law, but that has not really happened, likely because these laws generally have not required new obligations," Nahra said. "One or two major states that pass 'different' or 'more aggressive' laws could easily change that dynamic."

As in previous years, there are no clear frontrunners for who will add to the privacy law patchwork in 2024, with laws aimed at protecting consumers' personal data expected to be introduced and move through state legislatures quickly.

However, lawmakers in New York, Massachusetts, Hawaii, Maine, Wisconsin and several other states have brought promising proposals to the table in recent years, including some with game-changing provisions like sweeping private rights of action not found in other bills, and attorneys say they'll be keeping especially close tabs on whether any of those measures gain traction in the upcoming year.

In addition to these potential new laws, the statutes already on the books will also keep companies on their toes in 2024, attorneys say.

"Now that we have all these privacy laws, it will be interesting to start to see how they're enforced," Patricia Carreiro, head of the cybersecurity and privacy practice at Carlton Fields, said.

Utah closed out 2023 with its privacy statute taking effect and, during the upcoming year, the Oregon and Texas laws will go live on July 1 and the Montana Consumer Data Privacy Act will be implemented on Oct. 1.

Enforcement of the privacy laws in California, Connecticut, Colorado and Virginia that all took effect during the course of 2023 is also expected to heat up significantly, as state attorneys general move closer to wrapping up investigations they likely began when the laws kicked in, attorneys say.

This will be especially true in California, which is the only state to have an agency dedicated to data privacy issues.

That regulator, the California Privacy Protection Agency, was dealt a temporary blow to its enforcement efforts in June, when a state court judge ruled that the agency couldn't enforce any regulations it had crafted until a year after they were finalized. The ruling has delayed enforcement of its initial batch of completed rules on topics such as privacy notice requirements and how to respond to consumer opt-out requests until March 29, 2024, but attorneys don't expect enforcement reprieve on these topics will last much longer than that.

"Companies should expect to see more enforcement activity in California once the regulations are enforceable," Reed Smith LLP tech and data partner Monique (Nikki) Bhargava said, adding that there should also start to be "enforcement in other states as well now that companies have had some time to comply with state laws and regulations."

Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP, agreed that the CPPA is "likely to make its presence felt in 2024" when the enforcement restriction lifts, noting that he wouldn't be surprised to see the agency bring an action that targets a California employer, given that the state's privacy law is the only one so far to extend to employee and human resources data.

The California privacy agency is also expected in the upcoming year to formally launch its highly-anticipated rulemaking on risk assessments, cybersecurity audits and regulating technologies fueled by artificial intelligence, another topic that practitioners will be closely monitoring.

This flurry of action at the state level will continue to fill in for the lack of action in Congress, which is likely to continue to face increasing calls for federal legislation that would address these issues in a more

uniform way.

While expectations remain low that federal lawmakers will be able to agree on comprehensive data privacy legislation, particularly in a presidential election year, chances are slightly better that Congress could agree on a narrower proposal to address a topic like children's privacy.

Lawmakers made some progress on that front in 2023, with the Senate Commerce Committee **in July** advancing an online safety bill that would require social media companies to do more to prevent harm to minors and a privacy proposal that would expand existing protections to cover 13- to 16-year-olds, ban targeted advertising to this demographic and set additional limits on the personal information companies can collect and retain.

However, there hasn't been movement on either bill since that vote, and so-far successful challenges to attempts to boost kids' online safety and privacy at the state level — including a September district court ruling that temporarily halted on constitutional grounds California's groundbreaking law requiring social media platforms to bolster their privacy protections for children — may further complicate these efforts.

In the case involving California's Age-Appropriate Design Code Act, as well as in a similar dispute over an Arkansas law aimed at limiting kids' social media access, the courts doubted the constitutionality of age verification and age estimation requirements that underpin laws that require companies to protect children online, teeing up questions for the upcoming year about how to craft such safeguards in a way that will survive judicial review, according to Lindsey Tonsager, who co-chairs the global data privacy and cybersecurity practice at Covington & Burling LLP.

"That's something to watch in 2022, because these efforts to regulate children's privacy aren't going away," Tonsager said.

Regulators Stepping Up Cybersecurity Game

Federal and state regulators have been paying increased attention to companies' ability to protect and secure the personal information they hold, a focus that was sharpened by the Biden administration's release in March of a national cybersecurity strategy calling for a more aggressive regulatory approach to dealing with hacking threats.

Since then, several major developments have transpired, including the U.S. Securities and Exchange Commission voting to finalize a rule requiring public companies to make certain public disclosures regarding material cybersecurity incidents within four business days and the Federal Trade Commission amending its rules to create additional cyber governance and reporting obligations for financial institutions.

"Overall, 2023 met if not exceeded our expectations for the evolution of the cybersecurity regulatory space," Caleb Skeath, a data privacy and cybersecurity partner at Covington & Burling LLP, said. "Agencies continued to exercise their authority on cybersecurity issues, and we're anticipating a continued drive along the same lines in 2024."

The SEC is expected to move forward in the coming months on a pair of proposed rulemakings that would require broker-dealers, clearing agencies, and other security market participants as well as registered investment advisers and investment companies to adhere to beefed-up cybersecurity

standards similar to those recently imposed on publicly traded companies, including adopting written policies and procedures reasonably designed to address cybersecurity risks and reporting significant cybersecurity incidents to the commission.

The Cybersecurity and Infrastructure Agency is also slated to soon release proposed regulations to require vital infrastructure operators to report cyber incidents and ransom payments to the agency. Congress charged CISA with crafting these rules when it passed the Cyber Incident Reporting for Critical Infrastructure Act in 2022 and gave the agency until March 2024 to publish its notice of proposed rulemaking.

Additionally, the FTC will likely continue its "creative aggressiveness" that has led to the agency "pushing the envelope" on its privacy and data security activities and "creating new obligations in the absence of actual new law," WilmerHale's Nahra said.

These recent efforts include the commission moving in February to bring its first enforcement action under its long-standing but little-used Health Breach Notification Rule. The FTC then proposed changes to the rule in May that included clarifying that the rule applies to health apps and other similar technologies that collect or use consumers' health information. Attorneys are expecting more action from the FTC on this front in the coming year.

"In the absence of activity in Congress on a federal cybersecurity law, we're seeing the executive branch come out and take a whole-of-government approach to regulation, with multiple agencies moving forward with cybersecurity initiatives in their own sectors," Micaela McMurrough, co-chair of the global and multidiscplinary technology group at Covington, said.

As these efforts continue into 2024, they will create an "increasingly complicated regulatory environment" where companies that operate in multiple sectors are likely to face overlapping and conflicting requirements from various regulators, McMurrough added.

On top of the requirements springing up in the U.S., companies will additionally need to pay attention to what's happening across the Atlantic, where the European Union is moving toward putting in place beefed up cybersecurity preparedness and breach reporting rules for critical infrastructure providers and connected device makers as the bloc inches toward the implementation of the NIS 2 directive and the EU Cyber Resilience Act, according to Mark Young, the London-based vice-chair of Covington's data privacy and cybersecurity practice group.

European Union member states will be busy drafting regulations to implement the NIS 2 Directive that sets heightened rules for banks, energy suppliers, medical device makers, digital services and a wide range of other critical infrastructure providers to secure their systems and report cyberattacks, Young said.

"Cybersecurity laws in the EU have been developing slowly but surely," Young said. "It's becoming a complex web and companies will have to work out what laws they're subject to and, if they're ever impacted by a cyber incident, what rules apply to them and how long they have to respond."

Chief information security officers and other high-ranking executives are also likely to face increased legal risk, as regulators continue to scrutinize these individuals' role in their cybersecurity preparedness and data breach response efforts, attorneys say.

During the past year, several regulators put the focus on individual accountability, including the SEC, which in October announced a lawsuit accusing both software provider SolarWinds Corp. and its CISO, Timothy Brown, of underselling investors on its vulnerability to cyberattacks like the one that struck the company and its federal government clients in 2020.

The New York Department of Financial Services also turned up the heat on executives with the release of updated cybersecurity rules that introduced mandates such as that an organization's governing board must confirm that the business has "sufficient resources to implement and maintain an effective cybersecurity program," and that its highest-ranking executive and its chief information security officer must sign an annual certification of material compliance.

Moving into 2024, the SEC and other regulators "will continue pushing further into the field of personal liability for CISOs and company executives, further exploring the question of who or what is responsible for safeguarding an organization's information assets," Cynthia Cole, a partner at Baker McKenzie, said.

This increased regulatory activity comes as cyber threats continue to grow more frequent and complex, with hackers turning to emerging tools such as artificial intelligence to more easily manipulate content, avoid grammatical errors that often tip off fraudulent activity and engage in activities that allow them to orchestrate attacks that are more sophisticated and damaging, attorneys noted.

"2024 is promising to be a more dangerous and menacing cybersecurity environment than 2023," Michael Gold, chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP, said. "The fact that the federal government is getting more interested is a good sign, but what really needs to change is the way companies assess and operationalize their cybersecurity risks factors."

AI Continues To Wreak Legal Havoc

Policymakers in the U.S. and abroad have scrambled during the past year to create standards to reap the benefits while managing the potential data privacy and cybersecurity risks posed by AI technologies, such as the popular text generator ChatGPT that OpenAI released late last year.

"AI has been a game changer," David Saunders, a partner at McDermott Will & Emery LLP, said. "Companies are focused on not only what their own internal practices and policies are going to be around AI but also on understanding what regulators are going to do."

The European Union has so far set the pace by moving on Dec. 8 to finalize the EU AI Act, which is poised to become the world's first comprehensive law to tackle the potential risks posed by AI systems.

In the U.S., the White House has taken several significant steps in response to the rise of AI, including issuing a comprehensive executive order in October that requires federal agencies to establish new standards for AI safety, security, privacy and innovation across a range of industries.

The executive order built on a range of prior steps taken by the Biden administration in this arena, including its issuance of an AI Bill of Rights laying out a voluntary road map for the responsible use of the technology, and its July announcement that it had secured commitments from seven leading AI companies — Amazon, Anthropic, Google, Inflection, Meta Platforms, Microsoft and OpenAI — to support the safe and responsible deployment of AI, including by boosting their investment in cybersecurity and being more transparent about how the technology is being used.

"Heading into 2024, a big open question will be how legislatures are going to decide how companies can use AI," Saunders said. "It will also be interesting to watch how countries work together across the globe to develop rules of the road for the appropriate use of AI and whether an industry standard around reasonable AI governance develops."

In establishing rules for how companies are allowed to use and need to secure the datasets that fuel AI models, policymakers have moved at a much faster pace than they did when concerns first arose about how BigTech companies were using and safeguarding data they collected from internet users, attorneys noted.

"Regulators are not wanting to make the same mistake with AI that they did with cybersecurity and privacy by taking more of a hands-off approach and letting the market achieve results on its own," Jud Welle, a partner in Goodwin Procter LLP's data, privacy and cybersecurity practice, said. "There's a sobering recognition that left unchecked, AI can create some real problems, so it's important to put some standards in place now."

In addition to lawmakers, regulators are also expected to play a major role in the AI field in the upcoming year.

This includes California's new privacy board, which will soon launch formal rule making on AI, and the FTC, which during the past year took notable steps such as opening an investigation into OpenAI's use of personal data and moving last month to approve a new process that will streamline its staff's ability to use civil investigative demands in investigations over AI-related products and services.

The latter move serves "as a clear indicator that the FTC will be carefully watching AI-driven products, services, and companies for potentially illegal conduct or unfair methods of competition, which could include use of data and adherence to privacy principles and the impact of potentially deceptive or misleading practices on consumers," Reed Smith's Bhargava noted.

The FTC has also indicated that it won't hesitate to use its existing authority, including its mandate to police unfair and deceptive trade practices, to crack down on data misuse and discrimination in the AI context.

The agency drove home this point on Dec. 19, when it announced an enforcement action that will ban Rite Aid from using facial recognition technology for surveillance purposes for five years to resolve the FTC's claims that the retailer violated a prior commission order by failing to implement reasonable procedures and prevent harm to consumers in its use of the AI-fueled technology in hundreds of stores, and attorneys anticipate that these types of enforcement actions will continue to be pressed in the upcoming year.

"Especially in the U.S., given how we legislate here, regulators are going to continue to leverage existing law to assume power in the AI space until something more concrete is put in place, which is likely to take time," Kaylee Bankston, a partner in Goodwin's data, privacy and cybersecurity practice, said.

Companies will also likely continue to face liability risks in the courtroom, with plaintiffs' attorneys expected to ramp up their efforts to claim violations of existing privacy and consumer protection laws to go after alleged misuses of personal information to train AI, attorneys say.

"AI will likely dominate the conversation next year just as it dominated 2023," Luke Sosnicki, a litigator

and data privacy partner at Thompson Coburn LLP, said, "and the bounds of what information companies may or may not use to continue to develop it are just now beginning to be explored."

--Editing by Alyssa Miller.
