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 2022

By **Allison Grande**

Law360 (January 3, 2022, 12:03 PM EST) -- States are expected to continue adding onto the emerging consumer privacy law patchwork in 2022, while regulators in the U.S. and Europe will keep pressure on companies to protect users' data and to boost their cybersecurity to combat a growing scourge of ransomware attacks.

Another attempt by Congress to enact long-elusive federal privacy legislation that would set a national standard for how companies handle and share personal data, along with whether the Biden administration can broker a deal with its European Union counterpart to allow personal data to flow freely between the regions, will also bear watching this year, cybersecurity and privacy attorneys say.

New Patches for the State Privacy Law Quilt

In 2021, Virginia and Colorado somewhat surprisingly became the first states to follow in California's footsteps and enact privacy legislation that requires companies to give consumers more access to and control over their personal information. But attorneys don't expect these three states to stand alone for much longer.

"Colorado and Virginia have broken the dam somewhat, and now that we've got those laws, it's quite reasonable to think that we'll see at least a couple other states join in soon," said David Saunders, a partner at McDermott Will & Emery LLP. "The only question is, what states will get to the finish line in 2022."

Contenders for the next state privacy law include Pennsylvania, Ohio, New Jersey and Minnesota, where legislatures are seriously considering such proposals. Repeat entrants like Washington state and Florida both fell one chamber short of enacting their own privacy proposals in 2021, after squabbles over whether consumers should be allowed to sue derailed these efforts.

Both Massachusetts and New York are pressing legislative proposals that include a private right of action that would enable consumers to sue companies that fail to adhere to their new privacy obligations, including responding to consumer requests to access, correct, delete and opt out of the sale or sharing of their personal information. Proposals such as these with broad lawsuit mechanisms are likely to get the most attention from businesses as they move through state legislatures, said Bill Ridgway, a partner at Skadden Arps Slate Meagher & Flom LLP.

"The proposed bills that establish a private right of action provide a much more significant hammer for

the plaintiffs' bar to use statutory damages against companies that allegedly have issues without having to show particular harm to an individual, and that's a big eye-opener for businesses," Ridgway said.

The Massachusetts Information Privacy Act, which was brought to the Legislature in March, will be especially important to watch, because it not only contains a sweeping private right of action but also applies to a broader range of information and individuals and contains "far fewer exemptions" than current laws, according to Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale.

"It is a more aggressive proposal than we have seen enacted so far," Nahra said. "If this one moves, it could have a meaningful effect both on setting a new state law standard and putting pressure on a federal law."

Ezra Church, a partner at Morgan Lewis & Bockius LLP, added that companies would also be gearing up in the coming year to fall into step with the new Virginia and Colorado privacy laws as well as a revamped version of California's landmark measure, which are all slated to take effect in 2023.

"We're definitely expecting to spend a lot of time helping clients tackle those new state privacy laws," Church said. "In particular, I think we'll be spending a lot of time working with clients on the application of [the California privacy law] to employees. Assuming it happens, this will be one of the biggest developments in U.S. privacy law in decades."

Congress to Take Another Shot at National Privacy Framework

As more states enact their own nuanced privacy laws, pressure continues to build on Congress to codify a national standard for the collection, use and sharing of consumer information.

Experts were optimistic at the beginning of 2021 that Congress would finally break through long-running disagreements about who should be allowed to enforce the law and whether more stringent state laws should be preempted. But as the year drew to a close, the same roadblocks to a long-elusive federal privacy law remained.

"On the national level, it feels like déjà vu all over again," Ridgway said. "Interest in having a national data privacy law seems to be a hot topic, but it never seems to get fully accomplished or passed, and it's hard to predict if next year will be the year something happens."

Last year marked one of Congress' best shots at passing a national framework, given that Democrats held control of both chambers of Congress and the presidency. In 2022, a midterm election year, enacting a federal privacy law is going to be an even tougher task, attorneys say.

"Congress is going to slow down even further, with Republicans hoping to flip back one chamber," said Edward McNicholas, co-leader of Ropes & Gray LLP's data, privacy and cybersecurity practice. "If that happens and there's a divided House, Senate and White House, it will be exceptionally unlikely we'll see movement on a federal privacy bill."

Still, the issue won't slink away quietly, especially if several states move in the coming year to establish privacy laws with requirements that depart significantly from what companies are already doing to comply with existing laws.

"We've never been closer to having a national privacy law, and state laws are what's driving that," said

Mark McCreary, co-chair of the privacy and data security practice at Fox Rothschild LLP, adding that a federal framework may have a better chance of passing once the dust from the midterm elections clears in 2023.

Members on both sides of the aisle have floated dozens of privacy-related proposals in Congress in recent years. These include dueling proposals by the top Democrat and Republican on the influential Senate Commerce Committee. The plans share several similarities when it comes to the expectations for how companies will handle and share consumer information, but differ on the hot-button issues of preemption and a private right of action.

"The preemption issue is going to be a big challenge, because on the one hand, the argument for preemption gets stronger as we get more of a patchwork of state laws that seem to conflict with each other, but at the same time, there are members of Congress, particularly those from California, that take this issue seriously and argue strongly against preemption," said Ben Rossen, special counsel at Baker Botts LLP. "It's going to be difficult to overcome that, but it can happen if Congress can get together a strong bipartisan bill with a lot of support."

Federal lawmakers are also pressing more narrow privacy proposals that would set limits on the collection and use of certain types of information, such as children's and biometric data, or would regulate emerging areas of technology, such as artificial intelligence. These measures, which may have an easier time breaking through congressional gridlock, include proposed reforms to the Children's Online Privacy Protection Act to cover teenagers, as well as legislation that would set standards for the operation of fitness apps and consumer devices that collect medical information but aren't covered by existing health privacy law.

"There's always a chance something smaller will get done," said Saunders of McDermott.

Regulators and Insurers' Response to Ransomware

Several major cyber events grabbed headlines in 2021, including ransomware attacks that impacted the critical operations of Colonial Pipeline Co., meatpacking giant JBS and software vendor Kaseya. These incidents have led to a robust response by the federal government, including moves to sanction cryptocurrency exchanges used by cybercriminals and to require banks, health care apps and government contractors to report data security episodes, and attorneys are expecting even more activity in the coming year.

"There's been an uptick across the board in terms of the attention cybersecurity has gotten at all levels of society, from Washington, D.C., prosecutors' office, companies, and the courts, so its prominence in the legal field has grown basically exponentially," said Brian Klein, a partner at Waymaker LLP who handles cybercrime matters around the country. "Next year, we should expect to see cybersecurity only grow in importance and to see regulators, prosecutors, and everyone else paying more attention than ever to cyberthreats."

The proliferation of ransomware attacks that use malicious software to lock companies out of their systems until a ransom is paid has also led to a spike in the premiums and standards for obtaining cyberinsurance, attorneys say.

"Cyberinsurance is going to be difficult and harder to get, with more exclusions and limited coverage for ransomware," said Robert Braun, co-chair of the cybersecurity and privacy group at Jeffer Mangels

Butler & Mitchell LLP. "Companies that are well positioned to show that they have a decent level security are going to be able to get better and more comprehensive insurance coverage."

As insurers adjust their business model for cyberinsurance to better price the risks of increasingly costly ransomware attacks, companies should expect to see "a lot more questions and followup questions" at the underwriting stage to ascertain what security protections they currently have and how high their risk is of being swept up by an attack, according to Avi Gesser, a partner in Debevoise & Plimpton LLP's data strategy and security practice.

"Everyone who's redone their cyberinsurance this past year has said it's a much more extensive and expensive process and insurers have become much more sophisticated in assessing and pricing the risk," Gesser said, adding that this growing scrutiny is "incentivizing companies to invest in better protections to obtain more robust coverage."

Martin Tully, a partner with the eDiscovery and information law firm Redgrave LLP, added that these enhanced insurability factors will in the coming year "continue to be a catalyst for organizations to more rapidly and robustly implement industry-standard data security programs to comply with insurance requirements and qualify for lower premiums."

These security upgrades are likely to include boosting the protections for personal data entrusted to third-party vendors, attorneys say. Several major incidents from the past year have targeted vendors that hold the key to critical data sets, including an attack on SolarWinds Corp. that compromised the networks of at least nine federal government agencies and hundreds of companies that used the hacked IT software provider's products.

"2022 will be the year of cybersecurity clauses in contracts ... [that require all parties to] certify their compliance with reasonable cybersecurity practices," said Fred Bellamy, a member of Dickinson Wright PLLC. "Even the smallest businesses will be under pressure to upgrade their cybersecurity and data privacy protection practices or risk getting shut out of deals. Simply put, businesses will no longer have any choice, with decent cybersecurity practices becoming table stakes to participate in the B2B world well beyond tech."

Governments in the U.S. and abroad will also continue to put pressure on companies to boost their cybersecurity practices in the face of mounting cyberthreats, attorneys say.

"It is imperative that governments continue and augment their efforts to prevent and mitigate these types of attacks, as well as to identify and prosecute those responsible, be they domestic or foreign actors," said Erik Weinick, a partner at Otterbourg PC.

The Biden administration has taken aggressive steps to attempt to combat supply chain issues and make it more difficult for bad actors to profit off these attacks. These moves include the president's May executive order that imposed heightened cybersecurity requirements on the federal government and its contractors and sanctioned Russian actors for their cyber activities. The administration also developed new rules that will force pipeline owners and high-risk railway operators to appoint a cybersecurity point person and quickly report security breaches to federal officials.

More of the same is expected for 2022, with attorneys saying they'll be watching whether the federal government is able to put more pressure on bad actors operating in nation states like China and Russia by seizing funds and imposing other consequences on them, as well as whether Congress will be able

to pass proposals to require more widespread reporting of cyber incidents and ransomware payments.

"We need to be clear eyed that the benefits and compensation that ransomware actors are able to get far outpace the cost to them," said Alex Iftimie, co-chair of the global risk and crisis management group at Morrison & Foerster LLP. "The government is starting to do more to chip away at and diminish the threat, and we're expecting to see a lot more action both in terms of the government using all of its tools to raise the costs on the criminals and nation state actors who are perpetuating these cyberattacks and regulators imposing new requirements on the private sector to make sure they're not the low-hanging fruit that threat actors go after."

Increased enforcement is also expected from banking regulators, who are increasingly focused on this issue and have been ramping up pressure on companies to have a proactive and tested cybersecurity plan in place, according to Skadden financial institutions regulation and enforcement partner Bao Nguyen.

"For bank regulators, cybersecurity is one of the top issues that keep them up at night," Nguyen said. "We're going to see an uptick in enforcement activities in 2022 from a broad range of banking regulators."

U.S., EU Privacy Enforcers to Get More Active

Regulatory scrutiny of how companies handle and protect personal information ramped up in 2021, with the Federal Trade Commission transitioning to Democratic leadership that has more aggressively wielded its existing authority to police this conduct, and data protection authorities in the European Union kicking off its highly anticipated sanctioning of businesses under the bloc's General Data Protection Regulation.

"Overall, we're seeing significantly more sophisticated regulators in this space, and they're asking tough questions and are equipped to enforce privacy and data security laws in ways that they haven't been in the past," said Skadden partner Ridgway. "And we're expecting even more aggressive enforcement in 2022."

The FTC is expected to continue to lead the way in the U.S. The agency underwent a significant shakeup in June, when President Joe Biden made the surprising move of elevating progressive academic and Big Tech adversary Lina Khan to helm the agency just hours after she was confirmed by the Senate.

The move handed Democrats a 3-2 majority that held until Commissioner Rohit Chopra left the FTC in October to lead the Consumer Financial Protection Bureau. It also set off a flurry of activity that largely centered on the commission taking steps to seize on existing but seldom-used powers to write new privacy and data security rules. This included a December notice signaling the agency's intent to initiate rulemakings to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination" and to press ahead with ongoing reviews of regulations such as its children's privacy rule.

"We're likely to see in 2022 an FTC that's interested in testing its boundaries in terms of enforcement and investigations," said McDermott partner Saunders. "The FTC has been the federal sheriff on the privacy beat for many years, and it's expected that the agency will be more active in this space and take a closer look at the privacy practices of companies."

Rossen, who joined Baker Botts as special counsel in November after a more than six-year stint at the FTC, noted that 2021 was somewhat of a "transitional year" at the agency, with the new Democratic leadership "eager to accomplish" what it could before Chopra's departure.

"It will be interesting to see what the FTC does in 2022 and how it builds on the momentum to reinvigorate its rulemaking authority in the absence of federal privacy legislation," he said.

Congress has also floated a proposal to set aside $1 billion for the FTC to create a new division that would police privacy violations, cybersecurity incidents and other online abuses, which would be huge for the agency, if enacted, Rossen said.

"People are always quoting the size of the privacy division at the FTC and how it's dwarfed by foreign data protection authorities that have so many more resources," he said. "A significant budget increase would allow for more full-time employees to address these issues and, as Chairwoman Khan has called for, more technologists and economic analysts to help bring tech to the forefront at the agency."

In the EU, national data protection authorities after a couple of years of relative quiet have begun aggressively enforcing the GDPR, which took effect in 2018 and allows regulators to fine companies up to 4% of their global annual revenue.

The past year has brought hefty fines against U.S. tech giants such as Facebook, Amazon and Twitter, and attorneys are expecting more of the same in the coming year.

"Everyone's getting more comfortable with the GDPR, and regulators are getting more on top of enforcement," said Alja Poler de Zwart, a Brussels-based partner in Morrison & Foerster's privacy and data security group. "What we usually tell clients is that it might be better to invest in compliance now than to invest in compliance after you've triggered a regulator and are under investigation, because the second option is going to cost you more."

3rd Round for Transatlantic Data Transfer Mechanism

After the European Court of Justice in July 2020 struck down for the second time a mechanism that thousands of multinationals relied on to legally transfer data from the EU to the U.S., talks began almost immediately between the European Commission and U.S. Department of Commerce to come up with a replacement.

While the past year has failed to yield an agreement, officials on both sides of the Atlantic have signaled that they are still motivated to come up with a new lawful data transfer mechanism to replace the invalidated Privacy Shield, and attorneys say another revamped version of this deal could be on the horizon.

"The hope for 2022 is that the U.S. and EU figure out a replacement for Privacy Shield," Saunders said. "A new Privacy Shield would be welcomed by companies, given the necessity of finding a way to make data transfers between the U.S. and the EU less burdensome for companies on both sides of the Atlantic."

Any revamped deal would most likely have to be strong enough to survive another round at the European Court of Justice, where privacy activist Max Schrems — who successfully challenged the first two mechanisms — has already said he'll fight any new agreement.

"Hopefully, the U.S. and EU and governments will take their time and prepare something that sticks," said Poler de Zwart.

A Privacy Shield replacement would also provide companies with a more efficient way to lawfully transfer data than standard contractual clauses and binding corporate rules, the current alternatives for transferring data outside the EU.

Both mechanisms require more legwork to implement than certifying compliance to Privacy Shield, with binding corporate rules only being able to be used for transferring data within a corporate unit and standard contractual clauses requiring the sender and receiver of data to enter into an agreement over how transferred data will be handled.

Standard contractual clauses, or SCCs, have become even trickier to implement in recent months, after the European Commission in June took the long-awaited step of updating the rules to establish a "modular" structure that will allow companies to better tailor their contracts to their data processing activities while requiring them to guarantee that they've taken reasonable steps to assess these transfers and ensure that the exchanges don't raise any data protection concerns.

"International data transfers continue to be a mess," said Keily Blair, who heads the cyber, privacy and data innovation practice at Orrick Herrington & Sutcliffe LLP in London. "It's very hard for companies at the moment to prove that they have appropriate safeguards in place to transfer personal data outside the EU."

Under the revamped clauses, which businesses have until the end of 2022 to implement, companies must carefully scrutinize each international data transfer and shut them down if the laws of the country where the data is being sent don't provide adequate protections for the information. Especially for companies that engage in thousands of data transfers, the process is likely to be costly and time-consuming, while additionally opening companies up to scrutiny from regulators that may not agree with their assessment of why a particular data transfer was lawful, attorneys say.

"The issuance of new standard contractual clauses was a major development that has and will continue to impact businesses through 2022," said Jeffrey Mann, special counsel at Stroock & Stroock & Lavan LLP. "Understanding the revisions to the SCCs and incorporating the different modules into existing and new vendor agreements is important for all companies that process and/or transfer data outside the European Union."

--Editing by Nicole Bleier and Alyssa Miller.
