LAW360

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 For Rest Of 2021

By **Allison Grande**

Law360 (July 30, 2021, 10:17 PM EDT) -- More states are expected to add their own consumer privacy protections to the books in the coming months, while federal regulators are likely to spend the remainder of 2021 stepping up their scrutiny of Big Tech and pushing to clamp down on a recent scourge of ransomware attacks.

Several major cybersecurity and privacy developments defined the first half of the year, including the addition of two states to an emerging consumer privacy law patchwork, a shakeup in leadership at the Federal Trade Commission and sprawling cyberattacks that impacted the nation's largest pipeline, a pair of major software providers and a global meat supplier.

This landscape is likely to prompt lawmakers and regulators to place even more focus through 2021 on how companies are handling consumers' data and defending against increasingly prevalent cyberattacks, industry experts say.

"It's definitely been an exciting and challenging time for privacy, even on top of everything going on with the global pandemic and the world in general," said Robert Grosvenor, a managing director with Alvarez & Marsal's disputes and investigations practice in London.

Privacy Law Quilt Could Get More Patches

Virginia and Colorado surprised many earlier this year when they became the second and third states, respectively, behind California to enact comprehensive consumer privacy laws that will require businesses to give consumers more access to and control over their personal information beginning in 2023.

The first half of the year also saw several other states — including Washington, Florida and Oklahoma — fall short of enacting their own promising privacy proposals, after squabbles over whether consumers should be allowed to sue derailed these efforts. But attorneys say that, despite these hiccups, more states will continue to push this year and into early 2022 to find ways to enact consumer privacy protections, especially in the absence of Congressional action.

"We're seeing a lot more states focus on privacy rights and the protection of people's personal information as more of a priority than we've seen it be before, and we definitely can't rule out any kind of state privacy laws being enacted in the next six months to a year," said Jacqueline Cooney, lead director of the data privacy and cybersecurity practice group at Paul Hastings LLP.

Given the swift and unexpected passage of the new privacy laws in Virginia and Colorado, it's "anybody's guess at this point" which state will be the next to cross the finish line, noted Andrew Baer, the chair of the technology, privacy and data security practice at Cozen O'Connor. Some potential front-runners include New York, Pennsylvania and the handful of states that came close to enacting laws earlier this year.

However, increased public attention to the vast quantities of consumer data that companies are amassing and how vulnerable this information has become to hacking threats are likely to "cause a snowball effect in states when it comes to privacy and security statutes," according to Baer.

"It wouldn't be surprising in the next six to nine months to see at least one new state privacy law enacted," Baer said.

The success of these efforts hinges significantly on whether state legislatures can agree on whether consumers should be allowed to bring lawsuits, as they are in a limited capacity in California, or whether they should adopt the approach embraced by Virginia and Colorado, which leaves enforcement up to state regulators.

"The private right of action issue is likely where the log jam is going to be, but I think someone is going to figure out a compromise, such as allowing consumers to sue but only for actual damages and not for statutory damages plus attorneys' fees," said Tim Shields, a partner at Kelley Kronenberg.

The question of who should be allowed to enforce the law has also long held up efforts to enact federal legislation that would set a nationwide privacy framework.

Several such proposals are pending in Congress. Legislation introduced Wednesday by Republican Sens. Roger Wicker of Mississippi and Marsha Blackburn of Tennessee would require companies to be more transparent and accountable for their data practices while enhancing the FTC's authority in this space. A bill floated by Democratic Sen. Kirsten Gillibrand of New York in June would create an independent federal privacy regulator to clamp down on questionable uses of consumer data and concerning Big Tech mergers.

Experts aren't optimistic that Congress will break through the impasse before the end of the year, which would also require them to resolve disagreements over the extent to which a federal framework would preempt more stringent state protections. But the proliferation of new state privacy laws is beginning to cause compliance challenges for companies that may spur federal lawmakers to act sooner rather than later.

"I will be surprised if Congress does much on federal privacy law this year," said Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale. "My bet is that they move more actively in 2023, when a couple more states pass laws next year."

Big Tech To Land In Regulators' Crosshairs

After four years of Republican leadership, the FTC flipped back to Democratic control earlier this year, leading experts to predict that the regulator would tap into creative and underused approaches for seeking remedies and crafting rules in the privacy and data security space.

While Democratic Commissioner Rebecca Kelly Slaughter has served as acting chair since January, 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 in June, further raising the prospects that the agency would focus on how large tech companies and other businesses gather and handle consumer data.

"With a new administration comes new priorities in data protection and security, [and] the recent appointment of FTC Chair Lina Khan and what it symbolizes with respect to antitrust implications for Big Tech, may be the biggest practical shift," said Aloke Chakravarty, a partner at Snell & Wilmer LLP.

The FTC took several major steps under the prior administration to crack down on major companies' allegedly unlawful data uses, including notching landmark privacy settlements with Facebook and YouTube using its general unfairness authority and children's privacy powers, respectively, and launching an antitrust suit challenging Facebook's acquisition of Instagram and WhatsApp that notably focused on how the social media giant's allegedly anti-competitive conduct has harmed privacy rather than price.

While the FTC suffered a setback in June when a district court dismissed the parallel antitrust enforcement action against Facebook that it had filed with state enforcers, the regulator is expected to continue to keep a close eye on the "Wild West" of social media and Big Tech in the coming months, Shields of Kelley Kronenberg said.

"The FTC is going to take a strong stance on what these companies are doing with people's private information, and we're likely to see more enforcement actions and more of the FTC interpreting the rules that they already have in place to be more aggressive in this space," Shields said.

The growing scrutiny and criticism of Big Tech's power from both sides of the political aisle, coupled with the FTC's loss earlier this year of a key enforcement tool that the agency used to collect restitution or disgorgement of ill-gotten gains from lawbreakers, could also spur action from Congress that would answer the commission's long-running call for more authority in this area, attorneys noted.

"There appears to be bipartisan agreement when it comes to tech companies maybe needing to be reined in, so that may be where federal lawmakers end up focusing their attempts to put privacy legislation into effect," said Jason Johnson, a partner at Moses & Singer LLP.

Regulators in the European Union are expected to further step up pressure on Big Tech in the coming months.

National data protection authorities — especially those in Ireland and Luxembourg, where Facebook, Google, Amazon and other Big Tech companies are headquartered — have faced mounting pressure to move more quickly to aggressively wield their enhanced enforcement and fining powers under the bloc's General Data Protection Regulation, which took effect in 2018, to crack down on data misuses.

Luxembourg's data protection regulator has answered by fining Amazon a record €746 million ($884.9 million) for allegedly violating the GDPR, a penalty that was disclosed by the e-commerce giant on Friday.

Additionally, the Irish regulator announced its first major sanction against a Big Tech company in

December, when it hit Twitter with a €450,000 penalty for alleged missteps related to the company's reporting of a 2019 data breach, and more significant actions are expected, experts say.

"One criticism of the EU is that it can be very good at bringing out new laws, but is less effective in actually enforcing them," Alvarez & Marsal's London-based managing director Grosvenor said. "There's definitely an incentive and strategy now with respect to most European data protection authorities to be more effective in terms of investigation and enforcement, especially when it comes to cross-border data flows and international data transfers, cases related to digital marketing and ad tech, and issues stemming from the global pandemic."

And in the U.S., attorneys will also be keeping an eye on enforcement at the U.S. Department of Health and Human Services. Xavier Becerra — who in his most recent role as California's attorney general took the lead in drafting regulations and enforcing violations of the state's landmark privacy law — was **confirmed in March** to helm the agency, and HHS' Office of Civil Rights has ramped up both the size and frequency of its health privacy and data security penalties in recent years.

"President Biden's cabinet is likely to be far more proactive on privacy than the past administration, and having Becerra, who's clearly viewed as a privacy hawk, being named as secretary of HHS, that will be something to watch," said Cooney of Paul Hastings.

Ransomware Attacks To Prompt Increased Federal Action

Following an uptick in major cyberattacks — including ransomware that temporarily took offline critical infrastructure provider Colonial Pipeline and incidents that impacted thousands of businesses and government agencies that relied on software provided by SolarWinds Corp. and Kaseya — the Biden administration issued an executive order that imposes heightened cybersecurity requirements on the federal government and its contractors and sanctioned Russian actors for their cyber activities.

Attorneys are expecting further action from the White House and government agencies on these issues in the coming months, as pressure is increasing for companies in both the public and private sectors to pay attention and ensure they have appropriate steps in place to tackle these threats.

"There is a lot of momentum now to put efforts toward trying to prevent these attacks, and now that it's on the Biden administration and other countries' radars, there's likely to be a more concerted effort to both prevent and go after the entities that appear to be behind this," said Johnson of Moses & Singer.

The enhanced pressure on the federal government to address systemic cybersecurity threats could result in a range of measures, including reporting requirements being imposed by legislation or increased regulation in key critical infrastructure sectors like energy, water and transportation, said John Dermody, data security and privacy counsel at O'Melveny & Myers LLP and a former legal adviser for the U.S. National Security Council and U.S. Department of Homeland Security.

"The administration can increase the collaborative resources it makes available to the private sector, can explore more prescriptive regulation of certain critical infrastructure sectors, and could potentially seek to regulate cryptocurrency as a means to cut off the supply line for ransomware actors," Dermody said. "But broad and comprehensive efforts will require Congressional action. There have been a number of recently proposed bills, and companies would do well to keep an eye on that space."

While these actions unfold, companies should look at these incidents as providing a catalyst for

implementing "formal, written data security programs that are strongly supported by management to establish 'tone at the top,'" said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

Since the disclosure of the Colonial Pipeline and other major hacks, companies that provide essential services have been increasingly seeking out counsel and guidance on developing systems so that they can be prepared in the event of an attack, according to Reed Smith LLP partner Sarah L. Bruno.

"Ransomware has been the topic of the day with respect to what clients are worried about," Bruno said.

The subject is likely to become even more urgent for companies as claims begin arising more frequently in private litigation that the influx of guidance and rules from federal agencies has created a new heightened industry standard for what constitutes reasonable security that companies can be held liable for failing to adhere to, said Baer of Cozen O'Connor.

"On the one hand these companies are victims, but on the other hand, no one can argue that this isn't foreseeable anymore," Baer said. "The real interplay to watch in cybersecurity will be between increased regulatory activity and the private right of action landscape, and we're only beginning to see the tip of the iceberg here."

--Editing by Emily Kokoll and Nicole Bleier.
