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 And Privacy Policy To Watch In 2021

By **Allison Grande**

*Law360 (January 3, 2021, 12:02 PM EST)* -- California's landmark privacy law and looming changes to strengthen those rules are poised to keep companies busy in 2021, while state legislatures and Congress are expected to jumpstart efforts derailed by the COVID-19 pandemic to rein in how businesses use and share personal information.

How the transition to a Democratic Biden administration impacts the Federal Trade Commission's privacy and data security enforcement efforts and the future health of transatlantic data flows will also bear watching, experts say.

"2021 promises to be the most eventful year for consumer privacy law this country has ever seen," said Alan Friel, a California-based privacy partner at BakerHostetler.

Here, attorneys flag some of the major policy issues they will be tracking in the new year.

**Calif. Privacy Enforcement to Ramp Up as New Regime Looms**

The California Consumer Privacy Act, which went live on Jan. 1, 2020, will continue to captivate in 2021. The first law in the nation to give consumers the ability to find out what data companies hold about them, the CCPA also allows consumers to have that data deleted and opt out of selling their data.

"While many companies have taken a first pass at compliance, because it's such a comprehensive law and it requires companies to implement entirely new processes, it's going to take some time for companies to work out the kinks and provide the best response," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

California's attorney general began enforcing the law in July over the objections of several business trade groups that pushed for a delay due to the impact of the pandemic and the unfinished nature of vital regulations for implementing the law.

While the attorney general kicked off enforcement by blasting out warning letters that focused on the obligation of companies to ensure there's a clear and visible way for website visitors to opt out of the sale of their data, the regulator has yet to publicly bring an enforcement action, although attorneys say such a move likely isn't far off.

"Once enforcement is in full swing, that's going to tell us a lot about what the attorney general's priorities are and what companies should really be paying attention to," said Cynthia Cole, special counsel at Baker Botts LLP.

Aside from ensuring their policies and procedures align with the enhanced notice, transparency and consumer choice requirements of the CCPA, attorneys say companies will also need to start preparing for Jan. 1, 2023, when the California Privacy Rights Act, a ballot initiative to beef up the law that voters passed in November, is slated to go into effect.

"Rather than saying they have to finish up with the CCPA and then turn to the CPRA, companies should try to start to leverage their existing CCPA compliance program and figure out what additional work they need to do to build on it in order to comply with the CPRA," said Amy de La Lama, leader of the global data privacy and cybersecurity team at Bryan Cave Leighton Paisner LLP.

The CPRA ratchets up the existing law's protections in several vital ways, including by creating a new agency dedicated to data privacy and handing consumers the right to limit the use and disclosure of a new category of "sensitive" personal information, which includes health, financial, racial and precise geolocation data.

The measure also empowers consumers to opt out of the sharing of their data and correct inaccurate data, and triples fines for the unlawful collection or sale of children's personal information.

Attorneys say they'll be paying close attention in 2021 to the establishment of the California Privacy Protection Agency, which the CPRA requires to replace the state's attorney general as the primary enforcer of the law. The independent watchdog will be governed by a five-member board that's expected to seated by the end of January and will be charged with both enforcing the law and crafting regulations to help companies comply with their new obligations.

"The agency will have the broadest authority in the country to issue regulations on topics like automated decision-making tools that aren't typically core privacy issues, and how they interpret and enforce the law is likely where we're going to see a lot of the changes from the CCPA moving forward," said Lindsey Tonsager, vice chair of the data privacy and cybersecurity practice at Covington & Burling LLP.

**Congress to Take Another Stab at National Privacy Law**

As the patchwork of privacy regulations grows in both the U.S. and abroad, pressure has been building on Congress to enact a uniform federal consumer data privacy standard. But despite both Democrats and Republicans agreeing that such a framework is needed, long-running disputes over whether the law should preempt more stringent state protections and whether consumers should be allowed to bring private lawsuits tripped up lawmakers in 2020.

"It will bear watching who controls the Senate and how much attention privacy gets on a crowded national agenda," said Jeremy Feigelson, co-chair of the data strategy and security practice at Debevoise & Plimpton LLP.

"There's a lot of bipartisan agreement on the issue," Feigelson added. "Everybody's for privacy generally, so there's a decent chance we might see movement on this front if people are finally ready to make a deal on important particulars like preemption and a private right of action."

Attorneys predict the Biden administration is likely to make consumer privacy a higher priority than it's been in recent years, especially given Vice President-elect Kamala Harris' reputation for being an aggressive privacy enforcer while serving as California attorney general. And if Democrats are able to seize control of the Senate by winning the two remaining open seats during the Georgia run-off election on Jan. 5, the prospects for a federal privacy law will grow even higher.

"We've been talking about a federal privacy law for over a decade, and while it's not clear if this will actually be the year, if Democrats are able to take the Senate, this might be the year," said Brenda Sharton, co-chair of the global privacy and cybersecurity practice at Dechert LLP.

Because this isn't a new issue, lawmakers have had ample opportunity to voice their opinions during numerous privacy hearings and in several draft proposals that have been floated in recent years, including dueling proposals released by the Republican chair and Democratic ranking member of the influential Senate Commerce Committee.

That maturation is likely to help move things along in 2021, according to Kurt Wimmer, co-chair of the data privacy and cybersecurity practice at Covington & Burling.

"The difference this year is that we've had past years, and what's happened in the past few years has been super helpful in flushing out what various members of Congress think is important in privacy legislation," Wimmer said. "So rather than letting a thousand flowers bloom, it's more likely that the [Commerce] Committee will focus on moving a proposal or set of proposals through."

Congress is also likely to feel increased pressure from the business community to act in light of the rapidly evolving nature of California's privacy rules and efforts by other states to put in place similar protections, attorneys say.

"The proliferation of state privacy laws, including not only the CCPA but also now the CPRA, has caused many companies to start wishing for a comprehensive federal U.S. data privacy law that would set uniform standards across all states, thus avoiding the need to monitor and operationalize differing privacy laws in each state," said Christine Lyon, a partner at Morrison & Foerster LLP.

However, a federal privacy law may not necessarily relieve companies' obligations to comply with laws like the CCPA, Lyon noted. Lawmakers have long struggled to agree on preemption, and the powerful contingent of California representatives in Congress is likely to push hard to block lawmakers from bypassing the state's protections, especially given that 56% of voters backed the CPRA in November.

"The CPRA has made that sticking point even stickier," said Laura Jehl, who heads the privacy and cybersecurity practice at McDermott Will & Emery LLP. "The California delegation in Congress is very proud of their state's reputation on privacy and are set on not having that be preempted."

Federal lawmakers during 2020 also floated narrower proposals to set restrictions on the collection, use and sharing of personal data such as biometrics and location information for specific purposes like COVID-19 contact tracing and identifying people in large crowds. Attorneys say they'll be watching to see if these more targeted efforts gain any traction in 2021, especially as the rollout of COVID-19 vaccines continue to fuel thorny data collection issues.

"If Congress takes one specific issue, like around how to use contact tracing apps or biometric identifiers, that seems like the sort of thing that's more likely to get bipartisan support than a

comprehensive privacy law and something that the federal government can tackle without stepping on too many states' toes," said Melinda McLellan, a partner at BakerHostetler.

**States' Privacy Proposals to Make a Comeback**

When 2020 began, many industry watchers believed at least one if not several states would join California in enacting consumer privacy protections. But after Washington state in mid-March **failed to push through** privacy legislation for the second year in a row due to disagreements over how the law should be enforced, the COVID-19 pandemic took hold and effectively ground to a halt state legislatures around the country.

"In my mind, the biggest privacy development in 2020 was the lack of developments on the legislative front," said Morrison & Foerster LLP partner Nathan Taylor.

Attorneys are expecting these proposals to reignite once state legislatures start coming back in early 2021. The sponsor of Washington state's privacy bill has already said he's reviving the measure, and experts say it's also likely that states like New York, New Jersey and Texas will again pick up privacy proposals that appeared to have momentum in previous sessions.

"The real question for the post-pandemic world is going to be whether the momentum we thought these measures had at the beginning of 2020 was real or just a perception," Taylor said, adding that if several states do act, that's likely to "increase the probability that we'll have conflicting privacy models" at the state level that will further complicate the compliance obligations of companies.

Congress is also likely to play a role in whether a rash of new privacy laws are enacted, according to Covington & Burling's Wimmer.

"If Congress can move forward quickly enough with federal privacy legislation before additional states pass laws, that may have the effect of encouraging busy state lawmakers to pause and say, 'Given all the other things we have to do right now, maybe we won't do privacy legislation,'" he said.

**FTC Privacy Enforcement to Heat Up**

The FTC has continued to vigorously pursue privacy and data security missteps during President Donald Trump's tenure. Last year alone, it notched a record $5 billion settlement against Facebook for a string of data misuse scandals and set a high water mark for children's privacy violations with a $136 million fine against Google's YouTube subsidiary.

Attorneys expect no slowdown in 2020, with current Republican Chairman Joe Simons likely to step aside as the agency's leader traditionally does when a new party enters the White House, and the commission poised to flip to a 3-2 Democratic majority.

"Chairman Simons has been an aggressive enforcer, and that's shifted the goal post for what people expect the agency to do," said Duane Pozza, partner at Wiley Rein LLP. "The FTC would be hard-pressed to go back to a less aggressive approach."

Democratic Commissioners Rohit Chopra and Rebecca Kelly Slaughter have provided a glimpse into what the commission's enforcement strategy might look like under their party's leadership through the dissents they've regularly penned in recent privacy and data security actions, including high-profile

settlements with Facebook and Zoom.

The commissioners have criticized their colleagues for not doing enough to punish companies or protect consumers and have pushed them to find more creative ways to fine companies, hold individual executives liable, set rules of the road, and merge privacy and cybersecurity issues using their existing authority.

Commissioner Chopra's dissent in the recent Zoom data security settlement, in particular, will likely provide an "important guide in terms of what we're going to see from U.S. agencies in terms of cybersecurity regulation during the next four years," noted Aaron Charfoos, a partner in the privacy and cybersecurity practice at Paul Hastings LLP.

The FTC's leadership on both sides of the aisle have also pushed Congress in recent years to enhance their currently limited ability to fine companies and engage in rulemaking, a proposal that lawmakers have seemed receptive to and one likely to appear in any federal legislation that may pass through Congress.

"It seems there's bipartisan consensus that the FTC is the right place at the federal level to focus on privacy enforcement and to provide it with additional authority and resources to continue to get that job done," said Alan Charles Raul, the leader of the privacy and cybersecurity practice at Sidley Austin LLP. "The FTC has been aggressive to date, and it's unlikely they'll become less aggressive."

The FTC isn't the only regulator that's expected to step up their privacy and data security enforcement efforts in 2021, with attorneys saying they're anticipating more action from federal agencies such as the Federal Communications Commission and U.S. Securities and Exchange Commission as well as already active state attorneys general.

The FCC will be particularly important to watch. During the Obama administration, a divided commission approved landmark broadband privacy rules that required providers to get permission from consumers to use and share web browsing data and other sensitive information, but Congress quickly axed the regulations at the beginning of the Trump administration.

"There's likely to be more interest in a more muscular approach to privacy and cybersecurity at the FCC, and it will be interesting to see whether the commission goes back to the broad internet privacy rules that were promulgated under the previous Democratic administration," said Wiley Rein LLP partner Megan Brown.

As cyberattacks targeting both private companies and the federal government continue to proliferate, regulators are also expected to up their oversight of data security and breach response efforts, attorneys say. This includes federal banking agencies, which last month proposed new rules that would require banks to alert their primary federal regulators within 36 hours after they believe they've experienced a "significant" cybersecurity incident.

"We're certainly going to see increased attention to this area in the new year, as regulators take stock of what's happened in 2020 in terms of rising cybersecurity incidents and redouble their efforts to increase scrutiny of companies' cybersecurity programs in general," said Hogan Lovells partner Peter Marta.

**EU, US Will Look to Shore Up Transatlantic Data Flows**

The European Court of Justice rattled the digital trade ecosystem in July when it invalidated the popular Privacy Shield mechanism that more than 5,300 companies relied on to transfer personal data from the European Union to the U.S.

The court cut down the agreement on the grounds that it failed to provide Europeans with effective redress rights or adequately protect them from having their data intercepted by U.S. intelligence authorities.

It also directed companies and national data protection authorities to more carefully scrutinize data transfers to anywhere outside the EU using standard contractual clauses, another widely used mechanism that the European Commission is expected to update in 2021, and to shut down these exchanges when the laws of the country where the data is being sent don't provide adequate protection for this information.

"There's going to be a lot of activity out of Europe with regards to understanding how companies will apply the [Privacy Shield] decision and how supervisory authorities will start to enforce and apply it as well," said Bryan Cave partner de La Lama.

Companies will also be closely watching to see how data protection authorities across the EU respond to the Court of Justice's directive to more closely scrutinize international data transfers, attorneys say.

"The age of enforcement is upon us, and while there's pressure on member states to not be so hard on businesses that they leave, the overall trajectory is going to be toward greater enforcement," said Michael Bahar, who co-leads the global cybersecurity and data privacy practice at Eversheds Sutherland and is currently based in London.

U.S. and European authorities previously worked together to establish Privacy Shield in 2016, after the Court of Justice axed its predecessor safe harbor framework due to similar government surveillance concerns.

The European Commission and Commerce Department have already confirmed they're in talks to replace the scrapped deal, and the leaders of the Senate Commerce Committee expressed support at a December hearing for taking steps such as enacting federal privacy legislation and revising the government's surveillance regime to build confidence with Europeans.

Additionally, the incoming Biden administration is expected to take a more diplomatic approach than the current administration to lowering tensions on digital trade, and as a result is likely to "set a more encouraging tone for the probability that we'll see a third scheme put in place between the EU and the U.S.," according to Gabriel Voisin, a Bird & Bird LLP partner based in London.

"But at the same time, both sides are likely to be very careful and prudent about getting a third deal in place, because who wants to see a third scheme get demolished again by the European court," Voisin added.

--Editing by Cole Hill and Philip Shea.