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 2020

By **Allison Grande**

Law360 (January 1, 2020, 7:03 AM EST) -- California's landmark new privacy law is expected to occupy much of businesses' attention in 2020, while momentum will continue to build for other states and Congress to craft their own rules for how companies use and share personal data.

Businesses will also be keeping close tabs on what U.S. regulators such as the Federal Trade Commission and state attorneys general do to keep pressure on companies to adhere to their privacy promises and secure their networks, and are anticipating big fines out of the European Union as the bloc's General Data Protection Regulation enters its third year, according to cybersecurity and privacy attorneys.

"The laissez faire days of data privacy and security may be over," said Michelle Hon Donovan, a partner at Duane Morris LLP. "In 2020, expect to see a paradigm shift in how consumers and regulators view and enforce privacy and security requirements."

Here's a look at major legislative and regulatory developments to watch this year.

California Privacy Law Goes Live

The new year kicked off with a bang in California, where the first-of-its-kind Consumer Privacy Act officially took effect at the stroke of midnight on Jan. 1.

Companies have spent the past year scrambling to comply with the law, which was put on the books in June 2018 and gives consumers the right to find out what data online businesses such as Google and Facebook hold about them, request that the data be deleted and opt out of the sale of the information.

"Top of mind for everyone going into 2020 is going to be CCPA and how that's going to be interpreted and enforced," said Behnam Dayanim, the co-chair of the privacy and cybersecurity practice at Paul Hastings LLP.

Several vital questions surrounding the CCPA continue to remain unresolved, including what the final regulations from the state's attorney general — which are expected in the first half of the year — will look like and whether further legislative amendments or a new ballot initiative will supersede much of the work that companies have already done to prepare for the law.

"The law is still a moving target, and everyone will be watching and waiting to see once this comes to rest a little bit more whether the final form of the law and regulations will require even more compliance work," said Jeremy Feigelson, co-chair of Debevoise & Plimpton LLP's cybersecurity and data privacy practice.

The attorney general's office in early October issued its long-awaited draft regulations offering guidance on several vital aspects of the law, including how to respond to consumer data requests and how to avoid discriminating against consumers. The regulations have drawn criticism from the business community for purportedly going beyond what's required by the statute and from consumer advocates who are pushing to narrow or eliminate provisions that they say will allow companies to skirt the law.

"Hopefully the attorney general will provide a lot more specificity in terms of not just what the law says but how it needs to be implemented by businesses at an operational level," said Bradley Arant Boult Cummings LLP partner Erin Illman.

Although the law is now live, the attorney general is restrained from bringing enforcement actions until July 1. Attorneys expect the regulator to issue at least one major enforcement action before the end of the year and will be keeping a close eye on what his office chooses to focus on.

"Often, initial enforcement actions are a way of sending a message to the business community about what sort of compliance issues a regulator views as priorities, and there will be a lot of interest in seeing what sort of message the attorney general's office sends about the CCPA," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

While companies have a brief reprieve from regulatory enforcement, consumers can immediately begin seizing on the statute's narrow private right of action for data breach claims, and attorneys on both sides of the bar expect the area to be fertile ground for a flood of new litigation.

The new year may also bring changes to the statutory text of the CCPA that companies will need to follow closely, attorneys say.

California lawmakers pushed through several narrow amendments to the law in September, and stakeholders such as the American Civil Liberties Union of Northern California have said that they plan to continue to push for further changes to the law in the upcoming year.

One issue that will almost certainly be tackled by the Legislature is how employee data fits into the statutory scheme. As part of the September amendments, employers were given a one-year reprieve from complying with most of the law's obligations to give lawmakers a chance to come up with a more tailored statutory regime.

"Employers need to be watching around midsummer what's going on in the Legislature to get a better feel for whether or not they're going to have to deal with full CCPA compliance with respect to human resources data come Jan. 1, 2021," said Philip Gordon, co-chair of the privacy and background checks practice group at Littler Mendelson PC.

Additionally, Alastair Mactaggart, the real estate magnate who spearheaded the drive that led to the enactment of the CCPA, introduced a ballot initiative in September that would amend the law to, among other things, allow consumers to expressly opt out of the sale of certain categories of sensitive information and establish an agency that would replace the state's attorney general as the primary

enforcer of the law. If Mactaggart is able to gather enough signatures, the initiative would be presented to voters across California in November.

"Complying with the CCPA requires a lot of technical changes as well as legal ones that are difficult to implement and take time, and from a business perspective, this new ballot initiative adds extra cost and uncertainty to those efforts," said Mary Stone Ross, who co-authored the original ballot initiative that led to the CCPA's enactment and now runs her own consulting firm, MSR Strategies.

States Poised to Follow California's Lead

California is far from the only state looking to establish more formal protections for consumer data. New York, New Jersey, Texas and Washington were among the states that seriously considered privacy proposals in 2019 that both borrowed from aspects of the CCPA and sought to create brand new restrictions. State legislatures are expected to continue to be on top of these issues this year.

"In 2020, a primary battleground will be over whether or not individual states are going to adopt all or part of the CCPA," said former Maryland Attorney General Douglas Gansler, who heads Cadwalader Wickersham & Taft LLP's state attorneys general practice. "The California law really sent shockwaves throughout the tech community, and if other states adopt laws similar to that, that's going to have a dramatic impact."

In Washington state, lawmakers are poised to resurrect a consumer privacy bill that the state Senate overwhelmingly approved last year before it died in the House, and Texas Gov. Jim Abbott recently filled a five-member board that lawmakers created in 2019 to study privacy laws and make recommendations to the Legislature about how it should proceed on this front.

New York state senators also recently signaled their impatience with waiting for Congress to act during a hearing that dug into options for regulating consumer privacy in the Empire State. Possibilities include pushing through the New York Privacy Act, a proposal that would set an even higher bar than California by allowing consumers to sue for any violations of the law and requiring businesses to act as "data fiduciaries" that are barred from using personal information in a way that benefits them to the detriment of their users.

"Everybody's already tearing their hair out trying to comply with the CCPA, and if states keep going with more and different privacy laws, everyone will just keep tearing out what little hair they have left trying to engineer new compliance programs every time a state acts," Feigelson said.

Attorneys expect to see this patchwork begin to emerge in full force sooner rather than later, as states that were likely waiting to see how the California law panned out begin moving aggressively to ensure that their residents aren't left behind.

"If the privacy law in California doesn't break the internet, that will give other states political cover to pass their own versions," said MSR Strategies' Ross.

Congress Grapples with National Privacy Standard

The growing privacy momentum at the state level has spurred both the business community and consumer advocates to put increased pressure on Congress during the past year to craft a national standard for dealing with and protecting consumer data.

A bipartisan group of senators' effort to come up with such a proposal ultimately fizzled, but the heads of the Senate Commerce Committee released dueling partisan proposals in November. Members from both sides of the aisle broadly agreed at a December hearing convened to discuss the drafts that a federal privacy law is long overdue.

"We're seeing a very serious effort in the Senate Commerce Committee and a lot of bipartisan energy around federal privacy legislation, but there are still some very important details that need to be worked out," said Maureen Ohlhausen, a Baker Botts LLP partner and former FTC acting chair who testified at the recent Senate hearing.

Whether federal legislation should override state protections and whether private citizens should be able to sue — the primary issues that have long derailed legislative efforts in this space — remain the biggest stumbling blocks.

The divide is clear in the competing drafts issued by the Republican chair and Democratic ranking member of the Commerce Committee. The Democrat-backed proposal would allow both states and individuals to bring federal lawsuits and supersede only "directly conflicting" state laws, while the Republican version would completely preempt state privacy laws and does not include a private right of action.

"Data privacy has become somewhat of a populist movement, and states and consumer groups are not likely to roll over all that easily to total federal preemption," Baker Botts special counsel Cynthia Cole said.

With major elections coming up in November and the current difficulties with reaching a consensus regarding practically any issue on Capitol Hill, the prospects for an agreement on federal privacy rules remain slim. But attorneys say lawmakers are closer than ever to finding common ground and that uniform rules could be on the horizon once the dust settles from the elections, particularly if states continue to act independently.

"The big wildcard is if three to five states pass their own law," said Kirk Nahra, co-chair of the cybersecurity and privacy practice at WilmerHale. "I think that puts a lot of pressure on companies to get something done, but it is still a long shot in 2020. After that, all bets are off, regardless of the administration."

US, EU Regulators Could Surpass Record Privacy Fines

The FTC cemented its place as the nation's top privacy enforcer with several notable enforcement actions in 2019, including a record $5 billion fine against Facebook in July for a string of data misuse scandals and a historic $136 million penalty against Google and its YouTube subsidiary that set a new high-water mark for alleged violations of the federal Children's Online Privacy Protection Act.

Attorneys are bracing for more of the same from the FTC in 2020, with the commission expected to continue its aggressive pursuit of companies of all sizes for privacy and data security missteps and to undertake a highly anticipated review of its COPPA rules that is likely to result in significant changes to the framework.

"The commission has sent a very clear message that the days of the 'slap on the wrist' financial penalties are over and from here on out, the numbers are going to hurt," said Feigelson.

These enforcement efforts may get a boost this year from Congress, which is weighing privacy proposals that would give the commission more power to write rules and hand out fines for first-time violations.

“There’s a growing perception that the FTC is beginning to reach the limits of its tools,” Ohlhausen said. “It’s like the little agency that could — it’s done a great job with what it’s been given, but there’s pretty widespread agreement that it needs more statutory and monetary resources.”

Europe’s data protection regulators recently saw their enforcement powers expand significantly with the May 2018 launch of the bloc's General Data Protection Regulation, and 2020 promises to be the year that the full potential of these new tools are realized.

Some national authorities have already begun to capitalize on the significantly beefed up fining powers that they were granted under the GDPR, with the U.K. regulator’s proposed £183 million ($244 million) data breach penalty against British Airways and the French authority’s nearly $57 million fine against Google being among the most significant from the past 12 months.

But attorneys are expecting to see data protection regulators ramp up both the size and frequency of GDPR enforcement actions in the coming year and will be particularly focused on Ireland’s data protection commissioner, who has disclosed several major investigations into tech giants such as Facebook, Twitter and Apple that are nearing completion.

“It’s wrong to think that because we haven’t seen many high-ticket fines that regulators aren’t going to be able to enforce the law,” said Eduardo Ustaran, who is based in the U.K. and serves as global co-head of the privacy and cybersecurity practice at Hogan Lovells. “Enforcement is still a work in progress, and regulators are learning as much about what to do with the law on a daily basis as companies are.”

Businesses that operate in the EU are also likely to face enhanced liability risks in the new year when it comes to their handling of electronic communications, attorneys said.

A proposed update to a separate EU law, the e-privacy directive, has been swirling around since early 2017. The more uniform and stringent regulation would expose tech companies that fall outside the traditional telecom space to tighter rules for handling electronic communications and carrying out digital marketing, but member states have failed to reach the consensus necessary to move the proposal forward.

Work is expected to continue into 2020 to push through the proposed regulation, with the process likely requiring serious changes to be made to win member states' buy-in. Hogan Lovells’ privacy and cybersecurity team recommended in a study released in November that policymakers consider pivoting away from restricting data processing activities that aren't harmful to individuals in order to better align the e-privacy regulation with the GDPR and to push the proposal across the finish line.

“What has become obvious is that we are trying to pass a law that is meant to regulate the use of data in the digital economy, but it’s being drafted with sort of a 1990s mindset that’s much different from the risk-based approach taken by GDPR,” Ustaran told Law360.

TCPA Clarity Could Be on the Horizon

Both businesses and consumers have been clamoring for the Federal Communications Commission to provide certainty to the widely disputed statutory interpretation questions that have helped fuel an

explosion in litigation under the Telephone Consumer Protection Act.

Following a March 2018 D.C. Circuit decision that invalidated key components of a 2015 FCC order that expanded the scope of the TCPA, the commission was widely expected to quickly offer fresh guidance on the pivotal issues of what constitutes an autodialer and the requirements for calling reassigned numbers.

Instead, nearly two years have gone by without further insight from the FCC, during which time the Ninth Circuit further complicated matters by embracing a broad definition of autodialer. Attorneys are hoping the long wait for FCC guidance will finally come to an end in 2020.

"We're getting to the point where we have to see bigger regulations coming out of the FCC sooner rather than later," said Robins Kaplan LLP principal Michael Reif.

The FCC has made more progress in addressing the reassigned numbers issue, with the commission publishing a final rule in March that paved the way for the creation of a database of reassigned numbers that callers would be responsible for checking. But efforts to launch the database before the end of 2019 fell short, leaving businesses looking toward the new year.

"The FCC has put out some broad strokes on the reassigned number database, but they need to put the finishing touches on it and let businesses know what's available and what are the rules surrounding it," said Winston & Strawn LLP partner Sean Wieber, adding that the long-term viability of many current TCPA disputes hinges on what action the FCC elects to take.

--Editing by Aaron Pelc and Alyssa Miller.