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

Privacy Policy To Watch For The Rest Of 2022

By **Allison Grande**

Law360 (July 29, 2022, 10:13 PM EDT) -- Privacy legislation is set to be the focal point for both businesses and consumer advocates for the remainder of 2022, with Congress mounting its strongest push yet to enact a nationwide standard and five state laws ready to go live next year if those efforts fall short.

U.S. and European Union officials are also expected to soon finalize another replacement for a vital trans-Atlantic data transfer mechanism, and a fully staffed Federal Trade Commission is poised to step up pressure on companies to safeguard children's, health and other sensitive data.

"It's been a profoundly unsettled time" for those that have had to navigate a patchwork of privacy laws and increasing scrutiny around international data transfers, noted Andrew Baer, chair of the technology, privacy and data security practice at Cozen O'Connor.

But while the coming months have the potential to deliver both uniformity and clarity if policymakers can push tentative deals across the finish line, "it's anyone's guess what will happen," Baer added.

Here, privacy pros look ahead to what's shaping up to be a pivotal end to the year.

'Best Opportunity' for Federal Privacy Legislation

While Congress has been trying for years to set a national standard for how companies use and disclose consumers' data, the past two months have produced some of the most significant and promising developments on this front.

In June, shortly after Connecticut became the fifth state to enact a comprehensive law to give consumers more access to and control over their personal information, a trio of key congressional leaders floated a bipartisan proposal they called the "best opportunity" in decades to establish a long-elusive national data privacy framework.

The American Data Privacy and Protection Act would give consumers the right to access, correct, delete and stop the sharing of their personal information, while enhancing data protections for children and teens and helping to clamp down on algorithmic bias. The measure has so far fared well in the lower chamber, with the House Committee on Energy and Commerce voting 53-2 to **send the proposal** to the full House on July 20.

"There is more hope this time around," Baer said. "Something feels different from previous years, and that difference is the passage of the California Privacy Rights Act and the four other state privacy laws, which are similar to each other but not mutually consistent. So the growing threat of a completely fractured privacy landscape in the U.S. is causing industry groups to put more pressure on Congress."

The ADPPA has emerged as the leading contender largely due to its bipartisan nature — its sponsors include House commerce committee Chair Frank Pallone, D-N.J., and ranking member Cathy McMorris Rodgers, R-Wash., as well as Senate commerce committee ranking member Roger Wicker, R-Miss. — and the middle ground it seeks to strike on the hot-button issues of whether consumers should be allowed to sue and whether more stringent state laws should be preempted.

The version of the legislation that passed the House commerce committee would allow consumers to bring lawsuits after notifying certain state and federal regulators beginning two years after the law takes effect — down from the four-year wait period proposed in the initial draft. And the current patchwork of five state privacy laws would be preempted, although California's new privacy agency would be allowed to enforce the federal law.

"If the U.S. wants to be a leader on all things data and technology, they need to not only go up against cyber bad actors but also create a workable privacy playing field for companies," said Michael Bahar, a partner and co-lead of the global cybersecurity and data privacy practice at Eversheds Sutherland. "With each new state privacy law that's passing, the pressure is building, and the momentum is gaining, for Congress to act so that companies don't need to navigate both a global and a 50-state patchwork, which isn't workable or manageable."

However, despite the changed landscape, several obstacles loom, including the distraction of the upcoming midterm elections and the limited amount of time in the current congressional session.

The California delegation may also stand in the way, with the two votes cast in opposition to the bill in the commerce committee coming from a pair of California Democrats who supported a failed amendment that would have allowed states to set restrictions that went beyond what's in the federal proposal.

Additionally, the new California Privacy Protection Agency has voted to oppose the bill because it provides "substantially weaker protections" than the state's existing law while declining to allow states to enact more stringent standards. And, critically, the federal proposal still lacks support from a key lawmaker, Senate commerce committee Chair Maria Cantwell, D-Wash.

"The window for passage is likely between now and November, and while the proposal is getting traction and probably has a significantly greater chance of becoming law than anything we've seen before, that significantly greater chance may still only be 50/50," Baer said.

Gearing Up for State Privacy Law Onslaught in 2023

As Congress grapples with a federal privacy law, states continue to march forward with their own regulations.

The coming year promises to be a pivotal one, with California's revamped privacy law and the Virginia Consumer Data Protection Act set to go live on Jan. 1, Colorado and Connecticut's privacy laws

taking effect on July 1 and Utah's Consumer Privacy Act closing out the year with a Dec. 31 effective date.

"2023 is going to be the most interesting year in the history of privacy law," Baer said. "In some ways, it'll be like playing multidimensional chess, in that companies will need to prepare for these state privacy laws while keeping their eye on the federal law, which could theoretically bail them out."

However, "I wouldn't advise any company to wait for a federal privacy bill to preempt these state laws," Baer added.

Instead, businesses need to ensure that they have a handle on what consumer data they hold and what they're doing with it and that they have policies and procedures in place to ensure that consumers can utilize their new rights to access, delete, correct and opt out of the sale or sharing of their data, including for targeted advertising.

John deCraen, an associate managing director of Kroll's cyber risk practice, noted that while most companies are doing well with high-level tasks like data mapping, they're struggling with isolating individual data elements in order to be able to effectively respond to requests to delete or correct a specific consumer's information.

This is due in large part to a lack of technology that allows companies to keep track of where each customers' data resides and to search their vast databases for this specific information, according to deCraen, who predicted that there will soon be a major push to develop systems to fill that gap, especially as the state landscape continues to grow in complexity.

"These states are racing to outdo each other with their privacy laws and to be the most privacy-secured state in the union," deCraen added.

Companies that do business in California will need to additionally pay attention to rulemaking efforts that the state's privacy agency recently initiated, as well as the fate of a vital exemption that's set to evaporate when the California Privacy Rights Act takes effect in January.

Under the consumer privacy law that state lawmakers passed in 2018, information collected in the employment, human resources and business-to-business contexts largely falls outside the law's reach, with companies that handle this data needing only to provide notice of their data collection practices to employees and implement the necessary "reasonable" data security measures required by the law.

But the CPRA, which state voters approved in 2020 to strengthen and replace the existing privacy law, scraps this exemption and extends the law's beefed-up rights to access, delete, correct and opt out of the sale and sharing of personal information to cover data gathered from HR data subjects such as employees, job applicants and independent contractors and in certain B2B transactions and communications. This change would make the California law the only one of the five state privacy laws to sweep up this data.

While state lawmakers have floated legislation to extend or permanently enshrine these exemptions, the proposals have yet to gain traction, making it likely that the rules for those who handle this data will change on Jan. 1.

"Employers need to be thinking about what the [expiration of these exemptions] means for them,"

said Travis Brennan, a shareholder and chair of the privacy and data security practice at Stradling Yocca Carlson & Rauth PC. "If a company has employees that are California residents, these individuals are suddenly going to acquire all the privacy rights that consumers currently enjoy, and businesses need to decide how they're going to deal with things like requests from their own employees to delete their personal information."

That the "verbiage and intent" of the CPRA is aimed at consumer data, rather than information generated in the B2B or employment contexts, is likely to further complicate matters for businesses, noted Arsen Kourinian, a partner in the cybersecurity and data privacy practice at Mayer Brown LLP.

"It will be like trying to squeeze a square peg in a round hole," Kourinian added. "It adds another layer of complexity for companies, which are really struggling because they want to comply with the law, but they also have to wait on a lot of issues to resolve themselves."

Attorneys say they'll also be watching to see if any state legislative body takes up privacy measures during a special session in the coming months, and it's widely expected that at least one state will enact a privacy bill next year, possibly Florida, Washington or Indiana, which have all recently come close to passing such a measure.

"We are at an inflection point with respect to the introduction of individual state privacy laws," said Stuart Levi, co-head of the intellectual property and technology transactions group at Skadden Arps Slate Meagher & Flom LLP. "While companies can likely manage compliance with the five state privacy laws that will be in effect by next year, the introduction of a few more could create an untenable situation for companies."

Another Framework for EU-U.S. Data Transfers

Companies seeking to legally transfer personal information outside the EU currently find themselves on somewhat shaky ground.

Privacy Shield, a highly favored method that thousands of multinationals relied on to send data from the EU to the U.S., was struck down by the EU's high court in 2020, while the European Commission last year moved to revamp standard contractual clauses, which many businesses have adopted as their preferred data transfer method following Privacy Shield's demise.

Additionally, Ireland's data protection regulator on July 7 revealed that it's planning to block Facebook and Instagram from transferring personal data from the EU to the U.S. using standard contractual clauses due to the risk that transferred data could end up in the hands of U.S. intelligence authorities.

"This year has seen a continuous workflow from clients to assist with the re-papering and management of international data flows in light of the various regulatory developments on the safeguards of data transfers," said Eve-Christie Vermynck, London-based counsel in the intellectual property and technology group at Skadden.

However, some relief may soon be on the way, after U.S. and EU leaders revealed in March that they've reached a deal to replace Privacy Shield.

"The Trans-Atlantic Data Privacy Framework, sometimes referred to as Privacy Shield 2.0, could — if

implemented — once again provide EU and U.S. companies with an easier path towards transborder data flow compliance under the EU's General Data Protection Regulation," Levi said.

However, "what remains to be seen is whether companies will take advantage of this framework, or determine that it is not worth it given the rejection of the predecessors to the framework — the Safe Harbor and the Privacy Shield — by the European Court of Justice," Levi added.

In striking down both the Privacy Shield and its predecessor Safe Harbor, the Court of Justice pointed to concerns that the frameworks failed to provide Europeans with effective redress rights or to adequately protect them from having their data intercepted by U.S. intelligence authorities.

While the details of the tentative Privacy Shield replacement deal remain murky, it's expected to rely largely on executive orders issued by President Joe Biden, rather than the legislative fixes to U.S. surveillance policies that advocates argue is necessary, to address the court's criticisms.

"Pragmatically, under the new Trans-Atlantic Data Privacy Framework, the way that a treaty-based compromise may be achieved is by trusting the U.S. intelligence community to abide by their professed procedural protections for European data subjects' going forward," said Aloke Chakravarty, a partner at Snell & Wilmer LLP, adding that the institution of a new agreement would help lift companies out of "the purgatory" that many of them have been living through in the recent past.

However, the tentative framework has been met with warnings that policymakers haven't made the necessary changes to be able to withstand another round at the Court of Justice, where activist Max Schrems, who successfully challenged the prior two mechanisms, has already said he'll be making a challenge to any replacement that's implemented by EU and U.S. policymakers.

"It's a real mess," Kroll's deCraen said. "The White House is saying it's all settled and this one won't be invalidated. But companies have been burnt before and are likely to be hesitant to spend time and money trying to comply with the new framework, and they will probably be more inclined to wait and see what this [tentative deal] means."

Regulators Are Stepping Up Privacy Game

In both the U.S. and abroad, regulators in recent years have been ramping up their focus on how companies use, share and secure consumer data, and attorneys only expect that heat to grow as more laws are put on the books and as data privacy issues become even more prevalent in society.

"Companies need to steel themselves for heightened scrutiny as well as heightened enforcement actions," Eversheds Sutherland's Bahar said.

One sure source of regulation will be the FTC, which has long been the nation's leading data privacy and security watchdog.

The commission was restored to full strength in May, when Alvaro Bedoya was confirmed as the third Democratic commissioner on the five-member commission. With her party holding the majority, FTC Chair Lina Khan is expected to step up efforts to institute her ambitious agenda, which includes stretching its existing authorities to "take swift and bold action" against companies that misuse or fail to adequately secure consumers' personal information and initiating rulemaking to address issues such as commercial surveillance and lax data security practices.

"Now that they're at full strength, the FTC is likely going to flex their muscles and focus on expanding the boundaries of its authority governing data collection, use and sharing as much as possible through both increased enforcement and rulemaking," said Bradley S. Shear, a privacy attorney and managing partner of Shear Law LLC.

The use and protection of sensitive data such as health, location and children's information is likely to be of particular interest to both the FTC and other state and federal regulators, especially in light of heightened concerns about the detrimental impact of social media on young users and about the misuse of data about web searches and abortion clinic visits following the Supreme Court's decision to overturn Roe v. Wade.

"We're going to see a much stricter view taken by regulators, and a lot more enforcement in the U.S., on the use, disclosure and overcollection of sensitive health and location data in this post-Roe world we're living in," said Jami Vibbert, a partner at Arnold & Porter. "It was already going to be an issue, and the Supreme Court's decision just put it further into the spotlight."

State attorneys general are also expected to be more active on this front, especially in the wake of five state privacy laws going live in 2023 that hand enforcement authority to their offices and with the California Consumer Privacy Agency and Colorado's attorney general being entrusted with the additional responsibility of drafting regulations for their laws.

Outside the U.S., data protection authorities in the EU have been steadily ramping up their efforts to enforce the General Data Protection Regulation, which took effect in 2018, and attorneys are anticipating that these regulators will keep up the pressure on issues such as cross-border data transfers and the use of cookies to deliver services and targeted advertising to online users.

"Society is becoming more aware of these issues, and that's going to factor into the way regulators look at and enforce these topics," said Matthew Baker, a partner at Baker Botts LLP.

Additionally, companies will need to keep an eye on regulatory activity in China, which last year passed a law that lays out rules for the collection, use and storage of personal information. The Personal Information Protection Law also imposes strict requirements on international data transfers, including the mandate that they be submitted to the nation's cyber and data protection regulator for approval, and makes violations punishable by fines of $7.7 million or 5% of a company's previous year's business revenue, whichever is higher.

"If China starts flexing regulatory muscle, that is something American businesses will need to navigate," said Chakravarty, of Snell & Wilmer. "While it is notoriously difficult to predict technical compliance issues in China, the national security implications of data privacy along with political objectives may affect how Chinese governmental entities enforce the law, particularly against Western countries, who will likely have to play catch-up to enforcement patterns."

--Editing by Emily Kokoll.
