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

The Biggest Privacy Developments Of 2021

By **Allison Grande**

Law360 (December 21, 2021, 5:35 PM EST) -- The consumer privacy law landscape continued to expand in 2021, with two more U.S. states and China notably joining the fray, while the U.S. Supreme Court significantly narrowed the path for bringing robocall and other statutory privacy claims to federal court.

Here, Law360 looks at some of the top privacy developments from the past year.

Virginia, Colorado Join State Privacy Law Patchwork

After California passed its landmark consumer privacy law in 2018, attention turned to which states would be first to follow. Virginia and Colorado answered that call in 2021, putting new laws on the books that will require businesses to give consumers more access to and control over their personal information beginning in 2023.

"Although they are not slated to go fully into effect until 2023, the passing of these two state regulations have required certain companies to rethink their privacy policies and take proactive steps to ensure compliance when these laws go into effect," said Jeffrey Mann, special counsel at Stroock & Stroock & Lavan LLP.

The new laws share several similarities with the California Privacy Rights Act, a ballot initiative passed last year to strengthen the state's original 2018 privacy law. One of the biggest changes in the CPRA, which is also slated to go live in 2023, is the expansion of consumers' right to opt out of the sale of their data to also cover the sharing of this information, a feature that's also prominent in the Virginia and Colorado laws and will require companies to make some significant changes to their current operations, attorneys say.

"While a number of companies have systems in place for do-not-sell, that new opt-out for sharing is more pointed toward digital advertisers and cross-context behavioral advertising," said Sarah Bruno, a partner at Reed Smith LLP in San Francisco. "So there's more of an urgency there to develop systems for compliance."

In general, the three state laws share some key principles, including establishing similar rights of access, correction, deletion, data portability and special protections for sensitive data. But they also contain important nuances that are likely to make compliance more challenging.

The Colorado and Virginia laws depart from the California framework by adopting language and data

assessment requirements that are more on par with the European Union's General Data Protection Regulation. The statutes also leave it completely up to the state attorney general — rather than consumers — to enforce the law, while the California law contains a limited private right of action that allows consumers to sue for certain data breach-related claims.

California's attorney general in July pulled back the curtain on its enforcement activities under the 2018 privacy law, revealing that while it has issued dozens of notices of noncompliance, 75% of businesses that received a notice from his office acted to come into compliance within the 30-day period that the law allows for companies to cure alleged missteps.

However, the CPRA that takes effect in 2023 doesn't contain this cure period, removing a vital backstop for companies facing regulatory probes into suspected failings to meet their obligations to ensure that consumers are able to access, delete, correct and opt out of the sale and sharing of their personal information, attorneys say.

"Given all the other excitement that's been going on in the data privacy and security world, companies generally may have been less focused the past year on doing what they need to comply with these laws starting in 2023," said Cynthia Cole, a partner and deputy department chair of the corporate section at Baker Botts LLP. "So not having a cure period under the CPRA is going to be a problem, because a lot of companies are likely to be caught off-guard because they haven't taken a hard look internally at what changes they have to make, particularly when it comes to the new obligations surrounding the sharing of personal data."

The emergence of two laws in 2021 that track more closely to EU rules than the California framework also raises questions about whether other states that join the data privacy law club in the coming months are likely to take a similar approach, with Dickinson Wright PLLC member Fred Bellamy predicting that the coming year will be the "year of 'GDPR-ification' of data privacy law in the U.S. and around the world."

"The writing is on the wall that the world is rapidly shifting to GDPR's human rights-based approach, and this trend will accelerate in 2022," said Bellamy, who added that several U.S. states and many countries are likely to soon adopt new GDPR-style data privacy laws.

China Quickly Pushes Through Privacy Law

China made a big splash on the privacy law front this year with the enactment of its Personal Information Protection Law, which was passed in August and went into effect on Nov. 1.

Like other data privacy regulations around the world, the PIPL lays out rules for the collection, use and storage of personal data and establishes restrictions on the flow of data outside the country. The law includes provisions that mandate that international data transfers be submitted first to the Cyberspace Administration of China, the nation's cyber and data protection regulator, and makes violations punishable by fines ranging between $7.7 million or up to 5% of a company's previous year's business revenue.

"If you're doing business in China right now, it's important to get familiar with the new law," said Keily Blair, who heads the cyber, privacy and data innovation practice at Orrick Herrington & Sutcliffe LLP in London. "There are some nuances that set it apart from laws like the GDPR and CCPA, and we're seeing much greater scrutiny from authorities in China, particularly when it comes to companies who haven't

made required notifications to them."

The push for companies to keep their data within China is one significant differentiator between the PIPL and other data privacy laws around the world, attorneys noted.

"There's been a lot of comparison of the Chinese law to GDPR, but it isn't," said Cole, the Baker Botts partner. "The GDPR is about data transparency and data use, and the Chinese law is more about data localization and the government ultimately getting access to data when they need it."

Companies are still waiting on guidance from regulators on how to implement China's law and are now staring down an enforcement start date of Jan. 1 in an environment that could result in hefty statutory penalties, according to attorneys.

"Chinese enforcement can be extremely vigorous," said Edward McNicholas, co-leader of the data, privacy and cybersecurity practice at Ropes & Gray LLP, adding that the Chinese cybersecurity administration will "routinely go into companies and conduct unannounced insight inspections" in a way that's rarely seen from regulators in the U.S. or EU.

McNicholas noted that, when he gave a presentation on the prospects for a privacy law in China a few years ago, 15 people showed up. A similar talk he gave more recently attracted a few hundred participants, he said.

"People are waking up to the significance of China in the cybersecurity and privacy realm and to the fact that the PIPL is distinctly different from the GDPR," he said.

Big GDPR Fines Finally Emerge

Since the GDPR took effect in 2018, pressure has been building on national data protection authorities in the EU to aggressively wield their powers to impose fines of up to 4% of a company's global annual revenue on businesses that fail to properly handle citizens' data.

In a March 25 resolution, the European Parliament drew attention to what it called the slow pace of GDPR actions in two EU nations that have an outsize presence of tech giants: Ireland, which hosts Facebook, Google, Apple, Twitter and Microsoft; and Luxembourg, Amazon's home in the EU. The lawmakers stated that they were "particularly concerned … that cases referred to Ireland in 2018 have not even reached the stage of a draft decision," and called on the Irish and Luxembourg watchdogs to "speed up their ongoing investigations into major cases in order to show EU citizens that data protection is an enforceable right."

The regulators have responded during the past year with major fines against U.S. tech giants for skirting the GDPR.

Ireland's data protection kicked off these efforts with its first major sanction against a Big Tech company last December, hitting Twitter with a €450,000 ($547,000 at the time) penalty for alleged missteps related to the company's reporting of a 2019 data breach.

In the past year, the agency has also fined WhatsApp Ireland Ltd. €225 million for failing to be transparent with users about how it discloses their information and has separately proposed that WhatsApp's parent company Facebook pay a fine of between $32 million and $42 million for not clearly

communicating to its users that it was not asking for their consent as a legal basis for collecting their personal data under the GDPR.

Luxembourg's data protection authority in July issued the biggest GDPR penalty of 2021, fining Amazon a record €746 million for its use of consumer data for behavioral analysis and targeted advertising purposes. The e-commerce giant is appealing that decision.

"GDPR enforcement started super slow, but then it kind of took flight in 2021," said Alja Poler de Zwart, a Brussels-based partner in the privacy and data security group at Morrison & Foerster LLP. "Now we're starting to see more and more regulators issuing fines, and the fines are getting bigger."

Attorneys said they expect national data protection authorities to continue to launch investigations into companies of all sizes and to dole out big fines in the coming year, with a particular focus on whether companies have a lawful basis for processing consumers' data, how businesses are responding to consumer requests to exercise their data access and control rights, and the security posture and disclosure procedures of companies that are hit by data breaches.

"You don't have to be in the eye of the storm or a high-profile player to become the target of a regulator," Poler de Zwart added. "If you have a breach or if people complain about the organization, that's usually enough to draw the regulatory interest.

High Court Chips Away at Robocall, Statutory Privacy Litigation

The U.S. Supreme Court in April provided some much-needed clarity on what type of dialing equipment is covered by the Telephone Consumer Protection Act. In a unanimous opinion, the high court sided with the argument advanced by Facebook, the federal government and more than a dozen amicus supporters that the statute narrowly applies only to random-fired calls and texts to cellphones.

Since that decision, overall TCPA filings have plummeted, with plaintiffs struggling or no longer bothering to make the case that modern dialing equipment used by many companies to contact preexisting lists of numbers that they've gathered from consumers that aren't randomly or sequentially generated fall within the TCPA's prohibitions on autodialing cellphones without consent.

"The biggest effect of the Facebook decision is that overall TCPA filings are down and plaintiffs lawyers are largely looking elsewhere, such as the national Do Not Call list and more hyper-technical Federal Communications Commission regulations, as they're seeing that autodialer claims are not a good use of their time and money," said Mark Eisen, partner and co-chair of the class action practice at Benesch Friedlander Coplan & Aronoff.

Still, the issue isn't completely settled, as the Supreme Court's ruling left open several questions, including whether a plaintiff may nevertheless survive the pleadings stage on the autodialer question or whether it's enough for the device used to place the call to merely have the "capacity" to use a random and sequential number generator, according to David Anthony, a partner at Troutman Pepper.

"Courts have already begun to weigh in on these questions, and many more are sure to do so in 2022," Anthony said.

Lower courts will also be busy in the new year dealing with the fallout from another major Supreme Court decision from 2021, which centered on what's required for consumers to maintain statutory

privacy claims on a classwide basis in federal court.

In TransUnion v. Ramirez, the high court in a 5-4 June decision found that only the members of a certified class who had alleged that TransUnion provided misleading credit reports on them to third parties had demonstrated the concrete reputational harm necessary to press forward with their claims and seek damages under the Fair Credit Reporting Act, while those who hadn't alleged such disclosures were barred from proceeding.

The ruling narrowed instances in which consumers can bring privacy claims under statutes like the Fair Credit Reporting Act in federal court, and will "likely result in an increase" in the coming months of these matters shifting to state court to avoid these issues, according to Kristin Bryan, a data privacy and cybersecurity litigator at Squire Patton Boggs.

Attorneys will also be watching to see what impact the TransUnion decision has on plaintiffs' ability to press data breach litigation, which hinges on the assertion that consumer data has been taken but not yet misused.

Some experts predicted that the number of data breach cases filed in federal court would decline following TransUnion, based on the Supreme Court's assertion that "the mere risk of future harm, standing alone, cannot qualify as a concrete harm," Bryan noted. However, that trend has yet to materialize, as "most courts so far have avoided directly applying the case in the cybersecurity context," Bryan said.

"It is anticipated going into 2022 that there will be more cases holding, consistent with TransUnion, that plaintiffs who allege only that they are at risk of future risk of identity theft or fraudulent charges on their accounts as a result of a data breach lack Article III standing," she added. "This area of the law will continue to develop going forward as the impact of TransUnion plays out in the lower courts."

The cases are Facebook Inc. v. Duguid, case number 19-511, and TransUnion LLC v. Sergio L. Ramirez, case number 20-297, in the Supreme Court of the United States.

--Editing by Alanna Weissman.
