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

Top Privacy Developments Of 2021: Midyear Report

By **Allison Grande**

Law360 (July 2, 2021, 9:09 PM EDT) -- State legislatures and the U.S. Supreme Court left their marks on the privacy landscape in the first half of 2021, with Virginia and Colorado adding to the growing state privacy law patchwork and the nation's high court delivering a pair of rulings that are expected to limit statutory privacy claims.

Outside the U.S., European Union leaders acted to modernize a key international data transfer tool and ensure that personal data could continue to move freely to the U.K. post-Brexit.

"The headline for me is privacy is in vogue, with a lot of people now talking about and focusing on privacy around the world," said Tim Shields, a partner at Kelley Kronenberg.

Here, Law360 looks at some of the top privacy developments from a busy past six months.

Virginia, Colorado Cross Privacy Law Finish Line

After California enacted its landmark Consumer Privacy Act in 2018, experts predicted that it was only a matter of time before other states followed suit. While the COVID-19 pandemic and disputes over whether consumers should be allowed to sue derailed several promising efforts on this front, Virginia and Colorado finally broke through this year, passing laws that will require businesses to give consumers more access to and control over their personal information beginning in 2023.

"What we're seeing in the U.S. is a move away from sectoral privacy laws, which have been the traditional approach in the U.S., and a movement toward a more holistic approach similar to what they've done in Europe, where every company across the board has a role and responsibility to protect personal information," said Jacqueline Cooney, lead director of the data privacy and cybersecurity practice group at Paul Hastings LLP.

The passage of the Virginia and Colorado laws builds on this trend and highlights the increased focus of states on privacy rights and the protection of consumers' personal data, Cooney added.

The Virginia Consumer Data Protection Act, which was signed into law in March and takes effect on Jan. 1, 2023, gives consumers the right to access, correct and delete their personal information and to opt out of the processing of this data for targeted advertising purposes, while also giving the state attorney general exclusive authority to enforce the law.

Similarly, the new Colorado Privacy Act, which the legislature passed last month and is expected to either be signed by the governor or enter into law without his signature by July 8, requires businesses to give consumers the right to access, correct, delete and opt out of the sale of their personal information or processing of this data for targeted advertising and profiling purposes, while putting both the state attorney general and district attorneys in charge of enforcement.

These new laws — along with the California Privacy Rights Act, a ballot initiative that will overtake the CCPA and also go live in the beginning of 2023 — "will require most U.S. businesses to make material changes to their privacy compliance and information governance programs" in the next year and a half, said Alan Friel, the deputy chair of the global data privacy and cybersecurity practice at Squire Patton Boggs LLP.

"Although similar, the rights provided by the Virginia Act and Colorado Act, and the corresponding obligations and limitations, are not identical to what is provided by the CCPA/CPRA, and separate legal analysis will be required to identify the correct legal scope under the laws of each jurisdiction or to create the highest level of harmonization," Friel said.

The passage of both the Virginia and Colorado laws was somewhat unexpected, with neither state being widely viewed as a front-runner to enact such legislation when the year began. But with these protections now on the books, both statutes are likely to be major catalysts for other states and possibly the federal government to put in place similar protections in the coming months and years, attorneys say.

"It clearly has been harder for states to pass these laws than many people thought when CCPA passed," said Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale. "Yet we did have two new laws this year, from somewhat unexpected places. I think these laws will play a meaningful role in motivating even more states next year."

Supreme Court Takes Narrow View of Standing, Autodialers

During its recently completed term, the U.S. Supreme Court was asked to tackle the hot-button issues of what harm is required to press statutory privacy claims in federal court and what qualifies as an autodialer under the litigation-fueling Telephone Consumer Protection Act. The justices responded with a pair of rulings that are poised to significantly limit consumer class actions alleging procedural privacy violations or the use of equipment that dials from preexisting lists of numbers.

In a 5-4 ruling issued June 25 in TransUnion v. Ramirez, the high court 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 strengthened the Article III standing bar that the Supreme Court had established in its 2016 Spokeo v. Robins decision by declaring that every class member must be concretely harmed by an alleged statutory violation in order to press forward with claims, and provided more detail on what real-world injuries meet this standard.

"Over the long run, Ramirez will likely prove the most important privacy decision of the year," said Eric

Troutman, a Squire Patton partner. "By squarely holding that all unnamed class members must have Article III standing to recover damages at trial, the Supreme Court essentially did away with no-damage class actions. Since actual harm can often be difficult to demonstrate in privacy litigation, Ramirez will serve as a brake on litigation for years to come."

But plaintiffs attorney David Straite, a partner at DiCello Levitt Gutzler, said the majority's opinion creates more of a "venue problem" than an impediment to plaintiffs' ability to sue over statutory violations at all.

"The ruling will have very little impact on the traditional type privacy harms, such as invading on someone's privacy or wiretapping, where the spying has already happened and the harm has already occurred," said Straite. "If there's only a procedural violation, like a failure to delete or encrypt information, that hasn't resulted in harm, that may not be able to stay in federal court but rather will end up in state court."

The TransUnion ruling came less than three months after the Supreme Court's April 1 unanimous ruling in Facebook v. Duguid, which narrowly defined the types of dialing equipment covered by the TCPA.

"The Facebook decision was a game changer in the TCPA world," said Jaszczuk PC founder Martin Jaszczuk. "After years of litigation, hundreds of diverging district court opinions, countless gallons of printer ink spilled, and an emphatic circuit split, the Supreme Court finally clarified that the [automatic telephone dialing system] definition must be applied as the words are written on the page."

The impact of the high court's ruling that the statute covers only randomly fired calls and texts to cellphones "appears to have been immediate, with ATDS-based cases dropping off dramatically," Jaszczuk said.

However, despite the high court's clear declaration, "the last chapter of this story is likely still to be written," given that both Congress and state legislatures are "unlikely to leave this issue alone," according to Jaszczuk.

Sen. Ed Markey, a Massachusetts Democrat who helped write the TCPA when he was a member of the U.S. House of Representatives in 1991, and other lawmakers have vowed to "fix the court's error" and push through legislation to broaden the autodialer definition to cover systems that place robocalls and texts to telephone numbers stored in a list or database.

And Florida's Legislature recently approved legislation, which took effect July 1, to strengthen the state's telemarketing laws by requiring companies to obtain prior express written consent before placing sales calls using an "automated system for the selection or dialing of telephone numbers" and adding a mechanism for consumers to sue for alleged violations.

"The Supreme Court's decision gave companies a little more clarity, but then Florida took almost the opposite step, bringing it back to where it's a difficult landscape for companies to navigate," said Shields of Kelley Kronenberg.

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

Data Transfers Grab Spotlight in EU

The European Commission and the bloc's national data protection regulators took significant steps last month to respond to the considerable uncertainty created by the European Court of Justice's declaration last July that companies using standard contractual clauses to send personal data anywhere outside the EU must carefully scrutinize these transfers and shut them down if the laws of the country where the data is being sent don't provide adequate protections for the information.

For the first time in more than a decade, the commission on June 4 took the long-awaited step of formally updating standard contractual clauses to establish a "modular" structure that will allow companies to better tailor their contracts to their data processing activities while requiring them to warrant that they've taken reasonable steps to assess these transfers and that the exchanges don't raise any data protection concerns. Businesses will have 18 months to implement the revamped clauses.

The European Data Protection Board, made up of data protection authorities from each member state, on June 18 followed this move by adopting guidance on the Court of Justice's data transfer ruling, commonly referred to as Schrems II, to help companies "with the complex task" of assessing the data protection laws and policies of the country where data is being sent and to identify "appropriate supplementary measures" that companies may find necessary to undertake to transfer data. The regulators offered several recommendations, including having a firm grasp on where data is being sent and reevaluating "at appropriate intervals" whether the transfers are still valid.

"These are significant events that step up the responsibilities as well as the liabilities that senders and recipients of personal data now have to face," said Morrison & Foerster LLP privacy and data security group global co-chair Alex van der Wolk, who works in Brussels and London.

The EU's approval of the updated standard contractual clauses will require companies to revisit their contractual agreements for each data transfer they make in order to fulfill their obligation to attest that the exchanges meet the EU's high data protection standards on an individual basis — a task that is likely to be immense for companies that engage in hundreds or thousands of these transfers, attorneys noted.

"Because the standard contractual clauses are increasingly relied upon for lawful authority to export data in a post-Schrems II landscape, this process could become resource-intensive for affected U.S. companies," said Aloke Chakravarty, a partner at Snell & Wilmer LLP.

Even with the new clauses and guidance, companies are still likely to face uncertainties about how to properly evaluate such international data transfers.

"Since we're dealing with different countries that have different types of privacy and data security laws, which are layered on top of laws governing national security and government access, the problem lies with companies basically having to do their own due diligence to give a reasonable assurance that the data being transferred is not being intercepted by other parties or government bodies," said Robert Grosvenor, a managing director with Alvarez & Marsal's disputes and investigations practice in London.

In the wake of Brexit, the European Commission did help ease another area of concern in the data transfer landscape last month when it adopted a decision recognizing the U.K. as having adequate data protection rules on par with those across the bloc. The decision allows personal data to freely pass from the bloc to Britain for the next four years, when the deal is slated to expire under a sunset clause that's

unique to the U.K. deal.

"What this means in practice is that it helps take away that uncertainty that many companies had about whether they'd need to put in place additional transfer mechanisms in case the U.K. was not going to be deemed adequate," Grosvenor said. "Effectively, it will now be business as usual with respect to data transfers between European and U.K. companies."

--Editing by Alanna Weissman and Jill Coffey.
