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 2022: Midyear Report

By **Allison Grande**

Law360 (July 22, 2022, 9:14 PM EDT) -- The first half of 2022 saw blockbuster U.S. Supreme Court decisions curtailing both abortion rights and environmental rulemaking that are poised to have a major impact on how location data is handled and regulated, while two more states joined the growing privacy law patchwork.

Additionally, California's new privacy regulator launched highly anticipated rulemaking on the state's beefed-up data privacy law, and Illinois' unique biometric privacy statute continued to generate landmark decisions and notable settlements.

Here, attorneys look back at some of the major privacy policy and case developments from a busy start to the year.

High Court Rulings Have Big Privacy Ramifications

Following the unprecedented leak of a draft majority opinion in May, the divided Supreme Court on June 24 issued its controversial decision to uphold a Mississippi abortion ban and overturn the constitutional right to abortion established nearly 50 years ago in Roe v. Wade.

The ruling in Dobbs v. Jackson Women's Health Organization immediately brought heightened attention to long-standing concerns over law enforcement's ability to access the troves of sensitive location and health information that tech companies like Apple and Google gather. It also ramped up pressure on such businesses to put protections in place to ensure that data related to web searches about reproductive health and visits to abortion clinics can't be used to prosecute individuals in states that have outlawed the procedure.

"Dobbs is really a watershed moment for privacy," said Eli Wade-Scott, a partner and leader of the class action practice group at plaintiffs firm Edelson PC.

"We've been saying for years that location tracking, along with biometrics, is the next big issue in privacy because that's how you track people," Wade-Scott said. "Dobbs is really going to allow people to understand why we've been on panels for so long saying, 'Don't track people without their consent because it's not good for you or them or society.'"

The Dobbs decision has already prompted lawmakers, regulators and consumers to look more deeply into how companies and data brokers gather and disclose personal information not covered by existing

privacy laws such as the federal Health Insurance Portability and Accountability Act, attorneys say.

"We have to figure out as a society how we want to protect privacy," said Bradley S. Shear, a privacy attorney and managing partner of Shear Law LLC. "The Dobbs decision raises a lot of questions as to exactly what kind of data is protected, how it's protected and where we're going moving forward."

On the same day the Supreme Court ruling was issued, several Democratic lawmakers asked the Federal Trade Commission to investigate how Apple and Google track mobile phone users' data, warning that prosecutors "will soon be able to obtain warrants for location information about anyone who has visited an abortion provider." A top Google executive subsequently said the company will delete user location data related to visits to abortion clinics and other health providers.

While many companies have yet to issue official statements on how their policies may change with regard to collecting sensitive consumer data and divulging that information to other businesses or law enforcement, "privacy lawyers will likely be monitoring the issue in the coming months and well into 2023," Troutman Pepper partners David Anthony and Ron Raether told Law360 in a joint email.

"As a precautionary measure, companies that do engage in the collection of location data should reassess and examine their privacy and data storage policies," they added.

Additionally, consumers may begin to find courts becoming more open to both pending and future claims that companies were tracking their digital footprint without consent, since the Dobbs decision "makes it easier to say that this is a concrete issue that impacts people's lives," said Wade-Scott, the Edelson attorney. Law firms that defend companies accused of unlawful tracking may start to rethink their representation, he added.

"Firms didn't think twice about representing these companies before, but it's going to be hard to not see this as a moral issue now," he said.

Regulators are also expected to step up their scrutiny of the data privacy issues highlighted by Dobbs, attorneys say. The FTC published a blog post July 11 pledging to crack down on the illegal sharing of sensitive medical and location data. The U.S. Department of Health and Human Services issued guidance June 29 that addressed the limitations on federal protections for medical information, and provided tips for safeguarding privacy when using mobile devices and apps.

"The FTC has come out pretty strongly in looking for more robust ways to regulate sensitive data," said Matthew Baker, a partner at Baker Botts LLP.

But the power to make and enforce such rules may end up being hindered by another landmark ruling the Supreme Court handed down at the end of its latest term.

In a 6-3 ruling June 30, the high court restricted the U.S. Environmental Protection Agency's power to regulate greenhouse gas emissions from power plants. The holding in Virginia v. EPA that the agency went too far in its rulemaking could end up scuttling efforts by federal agencies like the FTC to impose privacy and data security mandates moving forward, attorneys say.

"Read literally, the decision really calls into question the ability of regulators to implement rules that are essentially not very clearly delegated to them by congressional authority," said David Saunders, a partner at McDermott Will & Emery LLP. "So since data privacy and cybersecurity were things that

weren't thought about when these executive agencies were created decades ago, an interesting question will be whether federal agencies have the authority to set these rules."

"It opens up a whole can of worms, especially if someone decides to take a run at challenging these rules," Saunders added.

The cases are Dobbs et al. v. Jackson Women's Health Organization et al., case number 19-1392, and West Virginia et al. v. EPA et al., case number 20-1530, both in the Supreme Court of the United States.

Utah, Connecticut Join Privacy Law Fray

Following in the footsteps of California in 2018 and Virginia and Colorado in 2021, Utah in March became the fourth state to give consumers more access to and control over how companies handle their personal information. Connecticut expanded the patchwork to five in May, when the state's governor signed similar legislation.

The laws generally give consumers the right to access, correct, delete and opt out of the sale or processing of their personal information for targeted advertising and profiling purposes. But they also contain important nuances that companies will need to figure out how to plug into their compliance plans, including inconsistent requirements for dealing with consumer opt-out requests and how to handle sensitive information.

"While the requirements in the [new] laws are similar to those in other states, the passage of these two additional laws has indicated to companies that they shouldn't try to take a state-by-state approach and should instead take a holistic approach to dealing with data across the U.S.," said Jami Vibbert, a partner at Arnold & Porter.

Given this shift, the importance of companies and their counsel being able to identify the inconsistences in these laws has grown, said Michael Bahar, a partner and co-lead of the global cybersecurity and data privacy practice at Eversheds Sutherland.

"Companies should consider taking a forward-looking, future-proofing, high-water-mark approach to privacy compliance, and privacy lawyers have to up their game when it comes to their ability to discern trends and find areas of overlap while isolating the differences," Bahar said. "If companies continue to do the minimum, they risk playing Whac-A-Mole, and that's not efficient, sustainable or cost-effective."

Viewing their compliance activities through a wider lens will be especially vital as the nationwide privacy law patchwork continues to expand, attorneys say.

While Congress is strongly pushing the American Data Privacy and Protection Act, which easily passed the House Commerce Committee this month and would set a national privacy standard that would preempt similar state laws, the bill is missing the support of a key Democrat in the Senate, making its chances of passage this year slim.

In the absence of federal action, "we're going to see states continue to fill the vacuum and pass enhanced privacy legislation that could create even greater uncertainty for companies that do business in the U.S.," Bahar said.

While most state legislatures have adjourned for the year, attorneys say they will be watching to see if any legislative body takes up privacy measures during a special session in the coming months. They also expect at least one state to enact a privacy bill next year, possibly Florida, Washington or Indiana, which have all recently come close to passing such a measure.

"State laws are still going to be the focus and are going to be driving the evolution of U.S. privacy laws for the foreseeable future, unless Congress suddenly gets its act together," said Travis Brennan, a shareholder and chair of the privacy and data security practice at Stradling Yocca Carlson & Rauth PC.

Calif. Privacy Rulemaking Kicks Off

The California Privacy Protection Agency, the only dedicated privacy regulator in the U.S., took the major step July 8 of formally opening rulemaking on the California Privacy Rights Act, or CPRA, a strengthened version of the state's landmark Consumer Privacy Act that is set to take effect in January 2023.

"With the issuance of the CPRA draft regulations, the California Privacy Protection Agency announced its intention that California have the country's most consumer-oriented set of privacy laws," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

The agency set an Aug. 23 deadline for stakeholders to weigh in on its first effort to craft regulations to guide companies in implementing the CPRA's tighter restrictions on how they use and share consumers' personal information. It is also planning to gather additional input at public hearings Aug. 24 and 25.

"Now that the comment period for the regulations has commenced, we will see whether the agency is responsive to considerations raised by the business community," Hirsch said. "If the draft regulations are not modified, they will pose significant compliance challenges in 2023."

Experts are anticipating the agency will receive a flood of feedback on its voluminous proposal, which tackles topics like browser privacy signals and dark patterns that other regulators have yet to touch and has stoked concerns about a lack of harmonization between the California rules and other state privacy law regimes.

"The CPRA is already granular, and the regulations are even more granular and introduce some new elements that go beyond what's in the law," said Melissa Krasnow, a partner at VLP Law Group LLP. "That raises questions about how companies are going to comply."

Trade groups will likely focus on the workability of the technical requirements of the proposed regulations, including the difficulties that they'll argue businesses will have with honoring browser signals that allow consumers to opt out of sharing their data across the internet, while advocacy groups will push for the agency to resist efforts to weaken the regulations, attorneys say.

"It's going to be very interesting to see if the CPPA is going to listen to any of the public comments, or if it'll just jam through its proposed regulations," said Saunders, the McDermott partner.

Biometric Privacy Law Parameters Clarified

Illinois' unique biometric privacy law, which is the only statute of its kind that allows consumers to bring private lawsuits, has produced a wealth of influential rulings and resolutions during the past decade, and the start of 2022 has been no different.

"The Illinois Biometric Information Privacy Act, likely the most robust law governing biometric privacy in the U.S., has seen a [flurry] of cases this year that have resulted in hefty settlements and remedial measures put in place to lessen private companies' ability to collect and store consumer biometric data," said Anthony and Raether, the Troutman Pepper partners.

In May, the American Civil Liberties Union and other advocacy groups that accused Clearview AI of capturing more than 3 billion faceprints and selling access to them to various public and private entities without consent announced that the facial recognition technology company had agreed to a nationwide injunction blocking most private entities from accessing its database of faceprints.

The ACLU asserted that the deal demonstrated "strong privacy laws can provide real protections against abuse," while ensuring that the company can't use people's unique biometric identifiers "as an unrestricted source of profit."

"There is a battle being fought in courtrooms and statehouses across the country about who is going to control biometrics — Big Tech or the people being tracked by them — and this represents one of the biggest victories for consumers to date," Edelson's Wade-Scott, one of the attorneys representing the ACLU and several Chicago advocacy groups, said in a statement at the time.

Another notable BIPA development was handed down by the Illinois Supreme Court in February when it ruled in McDonald v. Symphony Bronzeville Park that the state Workers' Compensation Act doesn't preempt claims for statutory damages under BIPA.

The decision obliterated a defense routinely invoked by employers to stave off claims that they had unlawfully collected biometric data such as fingerprints for timekeeping purposes without obtaining written consent or providing required disclosures about the companies' data practices.

"The decision is yet another way of clarifying that this is a really important moment in the way that we treat data privacy and that Illinois is going strong on protecting that information, especially when it comes to information like biometric data that can't be changed," said Baker of Baker Botts.

Looking ahead to the rest of 2022, McDermott's Saunders predicted that an even bigger splash is likely to occur once the Illinois high court issues its anticipated ruling in Cothron v. White Castle System, which deals with whether damages accrue every time biometric data is captured without informed consent, or just the first time.

"The White Castle case is probably the most significant BIPA case we've had in years," Saunders said. "Whether each individual scan is in fact a new violation of BIPA and thus restarts the statute of limitations period and/or means incurring damages for each scan is a significant issue, and it will be interesting to see what the court does."

The cases are American Civil Liberties Union et al. v. Clearview AI Inc., case number 2020-CH-04353, in the Circuit Court of Cook County, and In re: Marquita McDonald v. Symphony Bronzeville Park LLC, case number 126511, and Latrina Cothron v. White Castle System Inc., case number 128004, both in the Supreme Court of the State of Illinois.

--Additional reporting by Celeste Bott, Lauraann Wood and Caleb Symons. Editing by Jill Coffey and Lakshna Mehta.