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

Top Privacy Developments Of 2022: Year In Review

By **Allison Grande**

Law360 (December 21, 2022, 11:23 PM EST) -- The past year saw California and the Federal Trade Commission take major strides in regulating children's online safety issues and consumer privacy concerns, as well as the emergence of new consequences for companies and their executives in the wake of data handling missteps.

State attorneys general and European Union data protection authorities also turned up the heat in 2022 with eye-catching privacy settlements against major brands such as Google and Facebook.

"2022 brought numerous steps to mature the expectations for data privacy compliance," noted Aloke Chakravarty, a partner at Snell & Wilmer LLP.

Here, Law360 takes a look at some of the biggest privacy developments from the last 12 months.

Calif., FTC Turn Up Heat On Kids' Privacy

In September, Gov. Gavin Newsom signed the California Age-Appropriate Design Code Act. The law, which is modeled after the U.K.'s Age Appropriate Design Code and is the first of its kind in the U.S., requires companies that provide online services or products "likely to be accessed by children" to adhere to heightened privacy and data protection standards.

"This law is going to be an earthquake that rocks the privacy world," Tracy Shapiro, a partner at Wilson Sonsini Goodrich & Rosati PC, said.

Unlike the federal Children's Online Privacy Protection Act, or COPPA, which requires companies to obtain verifiable parental consent before collecting information from children under 13, and California's general consumer privacy law, which provides heightened privacy protections for users under 16, the new design code adds obligations for handling and processing data from those who are under 18.

Businesses will have until July 2024 to comply with the law, which the attorney general is allowed to enforce by seeking an injunction or civil penalties of up to $2,500 per affected child for negligent violations and up to $7,500 per affected child for intentional violations.

One major issue that's likely to be a cause for concern will be the "very broad scope of potentially who the law can apply to," Shapiro noted. The statute covers businesses that provide an online service, product or feature "likely to be accessed by children" under the age of 18, a phrase that those in charge of enforcing

the law "can really interpret broadly to cover any service," including those that 16- and 17-year-olds may access but a younger teen or child probably wouldn't, according to Shapiro.

The requirement for companies to complete data impact assessments and put a plan in place to mitigate or eliminate any risks to children that are identified in the evaluation, including their exposure to harmful content, is also likely to present issues as companies scramble to figure out which content could be considered detrimental to children and teens, attorneys say.

With California taking the lead on this front, as it did when it became the first state to pass a comprehensive data privacy law in 2018, industry watchers are anticipating that other states will soon enact their own protections.

A New York state senator introduced legislation in September modeled after the California Age-Appropriate Design Code, while a New Jersey assemblyman this month proposed legislation that would require companies to evaluate digital offerings that are "likely to be accessed by kids" for potential harm before their launch and would create a new data protection commission to develop best practices on the subject.

"Companies that know that children use their products or services or that target their products and services to 'children' — the relevant age varies across existing laws, from 'under 13' to 'under 18' — will need to keep a close eye on developments and consider whether it makes sense to adopt child-specific changes on a nationwide basis," said Julie O'Neill, a partner at Morrison & Foerster LLP.

There was also notable progress on these issues at the federal level in 2022, with the U.S. Senate Commerce Committee in July voting to advance a pair of measures to expand online privacy and safety protections for children.

While the Democratic chair of the Senate Commerce Committee and others made a strong push for the proposals to be enacted during the lame duck session, they ran into opposition from a broad coalition of advocacy groups and law professors, who argued that the measure would harm minors and violate the First Amendment by curtailing their access to vital information and threatening their privacy.

The ranking members of the Senate and House Commerce Committee also blocked efforts to include the measures in a must-pass government funding bill due to concerns with preemption and preference for a stalled comprehensive data privacy framework, which like the kids' measures has yet to be adopted.

"There's a recognition at the federal level that, while COPPA does have teeth, there needs to be more comprehensive laws," said Liz Harding, a shareholder and vice chair of technology transactions and data privacy at Polsinelli PC. "However, the issue remains, particularly coming into a new legislative session after the midterms [which led to split control of Congress], whether federal lawmakers are realistically going to get anything done here."

The Federal Trade Commission, which is currently limited to enforcing COPPA protections for children under 13, has also kept the pressure on companies in this space.

In the waning days of 2022, the commission announced a record $275 million penalty against Fortnite creator Epic Games for violating COPPA by allegedly collecting personal data from children under the age of 13 without notifying their parents or obtaining their consent. The company also agreed to pay an additional $245 million fine that will go toward refunding consumers for unauthorized in-game payments,

which the regulator said would be its largest refund amount ever issued in a gaming case.

The FTC is expected to not only build on this enforcement action, but also keep a close eye on related topics like children's advertising, especially in the wake of a proposed October amendment to its endorsement guides "that would effectively mean advertising practices directed towards children may be treated differently by the FTC compared to those directed towards adults," noted Kyle Dull, an attorney at Squire Patton Boggs LLP.

"These changes reflect traditional advertising principles to not use unfair or deceptive tactics, but recognize that children may react differently to advertising than adults," Dull added.

Sephora First To Land In Privacy Enforcement Crosshairs

While the California attorney general has had the power to enforce California's novel data privacy law since mid-2020, the agency made its first major strike in August, when it announced that it had hit retailer Sephora with a $1.2 million fine for allegedly failing to tell consumers it was selling their personal data or to honor all of their requests to stop these sales.

The action marked the first monetary penalty assessed by the attorney general for violations of the California Consumer Privacy Act, which established new obligations for companies to ensure that consumers are able to access, delete and opt out of the sale of their personal information.

The Sephora case "really broadened" the concept of what qualifies as a "sale" of personal information to include "not just a cash transaction" but any situation where a company derives an additional benefit from the sharing of this data, in addition to driving home the point that companies "better be sure that its vendors are toeing the line or they're going to be held liable for it," said Robert Braun, co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP.

In its enforcement action, the attorney general alleged that the relationship Sephora had with third parties that are used by many online retailers to track customers as they shop constituted a sale of consumer information under the CCPA that triggered "certain basic obligations, such as telling consumers that they are selling their information and allowing consumers to opt-out of the sale of their information."

The attorney general asserted that Sephora "did neither."

While the California privacy law requires companies to honor requests made directly to them to stop selling their personal information, the Sephora matter was notable because it made clear that the attorney general also expects websites to respond to requests made through the growing array of tools that allow consumers to signal their opt-out preference on a global basis instead of needing to go to each individual website, attorneys noted.

"The Sephora matter gave us a little preview of how regulators are going to interpret some of these obligations moving forward, although more guidance is needed since it didn't provide a lot of information about the underlying technology and trackers involved and how those precisely violated the law," said Nancy Libin, a Davis Wright Tremaine LLP partner.

Further insight is expected to start trickling out in the coming months, as regulators across the country gear up to enforce a slate of new privacy laws that are scheduled to roll out over the course of 2023.

These statutes include an update to the California Consumer Privacy Act that explicitly encompass the sharing of data and establishes a new dedicated privacy agency, among other enhancements, along with data privacy measures that have been enacted in Virginia and Colorado in 2021 and Utah and Connecticut this past year.

"California is not the only one anymore," Braun said. "Privacy is still very high on people's list of concerns, and we've been seeing legislatures and regulators responding to the desire for people to have more control over the collection and use of their personal data. Having more states jump on the bandwagon suggests this is going to be a continuing trend."

New Consequences For Cos., Boards

As the enforcement actions and settlements continued to roll in during the course of 2022, attorneys began noticing differences in the proposed remedies and consequences for data breaches and other privacy missteps, including an increased focus on individual accountability.

"There's certainly been a push to hold executives responsible for the privacy and data security practices of a company, and executives and boards certainly need to think hard about these issues," said Lisa Sotto, who chairs the privacy and cybersecurity practice at Hunton Andrews Kurth LLP.

Two of the most prominent examples from the past year came from the FTC's October data breach settlement with liquor delivery app Drizly and former Uber executive Joseph Sullivan's conviction the same month on charges of covering up a 2016 data breach.

In the Drizly matter, the FTC took the unusual step of not only requiring the company to take several steps to boost its cybersecurity but also forcing Drizly CEO James Cory Rellas to follow detailed data security rules going forward, even if he leaves the company.

The move marked a rare case in which the terms of an FTC settlement would follow a company CEO even if that person were to take another job. The commission's Democratic majority has defended the requirement by arguing that the risk of being held personally liable for cybersecurity issues will spur executives to devote more resources to safeguarding consumer data.

These remarks "emphasize the need for executive accountability, as the commission is going to continue its efforts to include individuals in FTC orders," noted John Villafranco, a partner at Kelley Drye & Warren LLP. He added that Consumer Financial Protection Bureau Director Rohit Chopra, who's a former FTC commissioner, has similarly "outlined his vision for increased individual accountability" in his agency's enforcement actions.

In Sullivan's case, a California federal judge convicted the former Uber security chief of criminal obstruction and concealment of a felony for hiding a massive 2016 data breach from authorities, crimes that could put him behind bars for years.

"This is an incredible development, because being convicted for hiding a data breach has never happened in U.S. history, and it won't be the last time this happens," said David A. Straite, a partner at plaintiffs' firm DiCello Levitt Gutzler LLC.

Straite said that he's also noticing more companies agreeing to injunctions that require the deletion of allegedly improperly collected data.

Such was the case in a provision that was part of a $90 million deal in California that U.S. District Judge Edward J. Davila approved in November to settle litigation accusing Facebook of unlawfully tracking logged-out users' browsing activity. The pact requires Facebook to not only establish a monetary fund to be distributed equally among eligible class members but also to delete certain "wrongfully collected" data.

The FTC also tucked the deletion requirement into a $1.5 million deal that it reached in a children's privacy case against WW International Inc. as well as in a January 2021 settlement with now-defunct photo storage app Ever that forced the company to permanently delete biometric data gleaned from its users.

This push to mandate data deletion "really hit the ground running, and we expect to see a lot more of that in years to come," Straite said, adding that, increasingly, "money alone won't work" for plaintiffs and regulators.

Mark Krotoski, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP, noted that he's also been seeing the FTC in their enforcement work "getting more and more detailed about what they want" from companies in the privacy and data security space.

He specifically pointed to the detailed data security requirements that it expects Drizly and its CEO to follow as part of the parties' settlement, which includes employing multifactor authentication, destroying unnecessary personal data, and limiting the collection and retention of data moving forward.

"The FTC is including a level of specificity of what they expect that we haven't seen before, and that's only likely to continue," Krotoski said.

State AGs, EU Regulators Dive Into Enforcement

While state attorneys general have long been interested in data handling and cybersecurity issues that widely impact consumers, "2022 was the year they really turned up the heat on privacy," according to Straite.

Most recently, more than three dozen state attorneys general in November reached a record $391.5 million settlement with Google to resolve allegations that the tech giant surreptitiously tracks users' locations even after they believe they've turned off that feature.

The deal came on the heels of Arizona's attorney general disclosing in October that his office had reached a separate $85 million deal to end its similar location tracking suit against Google. The tech giant is still facing separate suits over these practices from attorneys general in Texas, Indiana, Washington and the District of Columbia.

Also in November, 40 state attorneys general announced that Experian and T-Mobile had agreed to a combined $16 million in settlements to resolve investigations into data breaches in 2012 and 2015 that exposed the personal information of millions of consumers.

Theodore P. Augustinos, a Locke Lord LLP partner and member of the firm's privacy and cybersecurity group, said that he's recently observed that "more states are getting more involved more frequently when there are breach notifications."

"For example, I have seen deep conversations with representatives of AGs offices and insurance departments when there are data breaches or other issues," Augstinos said. "They know what they are looking at and expect to see, and are active about it."

Overall, all the various state and federal agencies responsible for enforcement "have really beefed up on the personnel they have minding the store on cybersecurity and privacy issues as it becomes an incredibly pertinent topic," Augustinos added.

This includes national data protection regulators in the EU, which were handed beefed up powers to impose fines on companies that mishandle consumers' data when the General Data Protection Regulation took effect in May 2018.

During the past year, investigations that have been launched in the wake of the GDPR's enactment have finally started to reach conclusions, particularly in Ireland.

The Irish authority has responded to "sustained pressure" from fellow national authorities "to pursue tougher enforcement action against many of the global technology companies" that fall within its jurisdiction by issuing a number of "eye-watering fines," noted Robert Grosvenor, managing director and co-head of the global privacy practice in Alvarez & Marsal's disputes and investigations practice in London.

Ireland's data protection commissioner announced in November that it had fined Meta Platforms $275 million for allowing the personal data of more than 500 million Facebook users to be scraped from its network and posted on a hacking forum. This followed a separate €405 million ($401 million) fine that the regulator said in September is set to be imposed on Meta's Instagram for allegedly mishandling children's data, which the company has said it's appealing, and a €17 million penalty disclosed in March against Meta's Facebook for allegedly flouting the law in connection with a series of data breach disclosures lodged in 2018.

Additionally, the data protection authorities in Austria, France, Italy and Denmark have all issued rulings during the past year finding that the way companies are currently using Google Analytics violates the GDPR, which requires heightened protections for personal data that is transferred outside the bloc.

"The data protection and privacy space is heading towards a more heavily regulated landscape, [and] arguably right now we are only at the tip of the iceberg," said Tom Cope, chief information security officer of cybersecurity firm Next DLP.

While the latest slate of enforcement actions against major platforms is threatening to lull smaller companies into a "false sense of security," that's likely to change "quite dramatically" in the coming years, according to Cope.

"Regulations such as GDPR put rights to data security and privacy in the customers' hands and provides them channels to report companies violating their rights," Cope said. "As consumers gain more awareness of this, I can see a second wave of fines hitting smaller companies and data privacy becoming a crucial part of the 'bottom line' for all companies big or small."

--Editing by Emily Kokoll and Michael Watanabe.