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 & Cybersecurity Policy To Watch For Rest Of 2018

By **Allison Grande**

Law360 (July 27, 2018, 4:41 PM EDT) -- A vital trans-Atlantic data transfer mechanism will face its most serious test to date and the newly restocked Federal Trade Commission will begin to chart its own path on privacy and data security issues in the second half of 2018, while landmark privacy laws in the U.S. and European Union will continue to mature and offer new challenges for those swept up by them.

Here, attorneys talk about the privacy legislation and regulation they will be tracking closely for the rest of the year.

Privacy Shield's Uncertain Future

The European Parliament at the beginning of July took the long-anticipated step of calling for the suspension of the EU-U.S. Privacy Shield, a trans-Atlantic data transfer mechanism that EU lawmakers and others have been skeptical of since its enactment in July 2016 to replace a safe harbor tool that was invalidated by Europe's highest court.

"Privacy Shield is a significant method by which companies transfer data outside Europe into the U.S. and is used by a large number of companies, so its disappearance would be a greatly significant headache," said Behnam Dayanim, co-chairman of the privacy and cybersecurity practice at Paul Hastings LLP.

More than 3,300 multinationals, including Google LLC, Facebook Inc. and Microsoft Corp., have pledged to adhere to the principles of Privacy Shield when transferring personal data between the U.S. and the EU. But the European Parliament has repeatedly expressed concerns that the pact does not protect EU citizens from surveillance by U.S. intelligence agencies, and on July 4 it passed a nonbinding resolution proposing that the deal be scrapped if the U.S. doesn't take steps to fix these shortcomings by Sept. 1.

"The Privacy Shield is a big deal for businesses that have to take data from the EU; they were the ones really pushing for this framework after safe harbor was invalidated," said Debbie Reynolds, data privacy officer and director of e-discovery at Eimer Stahl LLP. "If the Privacy Shield is invalidated, that's likely to create a trade issue because companies would have to find ways around that, including avoiding transferring their data to the U.S. in the first place and instead doing businesses in other countries that have protections that the EU has deemed adequate."

Because the European Parliament only has the power to suggest that Privacy Shield be scrapped but can't actually suspend it, attorneys in the coming months will be closely tracking the outcome of the annual joint review slated for this fall by the European Commission and U.S. Department of Commerce of how the deal has been operating — the commission gave the Privacy Shield high marks in last year's review — as well as a looming battle in the European Court of Justice over the legality of the mechanism.

"If I were reading a crystal ball, what we could be looking at is a reworking of what self-certification under the Privacy Shield means for companies and more scrutiny of companies who have self-certified," Baker Botts LLP special counsel Cynthia Cole said.

Attorneys will also be watching how the fate of Privacy Shield will affect binding corporate rules and model contract clauses, the other two widely used mechanisms for transferring data across the Atlantic that have also fallen under fire in recent years due to questions about their strength and adequacy.

"The rationale being used to attack Privacy Shield could also be used to attack and reverberate to model contracts," Dayanim said. "All of that is likely to be raised in the commission's annual review this fall and in the pending court challenge in the Court of Justice, so we'll just have to wait and see."

New-Look FTC's Take on Privacy, Data Security

The FTC is finally operating at full strength for the first time in nearly three years, following the April confirmation of Chairman Joseph Simons and filling of three open commissioner posts, and what direction the newly minted leadership decides to take the commission on privacy and data security issues in the coming months will be a point of interest for many onlookers.

"The FTC will loom large in the latter half of 2018," said Jo-Ellyn Sakowitz Klein, co-leader of Akin Gump Strauss Hauer & Feld LLP's interdisciplinary cybersecurity, privacy and data protection initiative.

While the FTC has already brought more than 60 cases alleging that companies failed to implement "reasonable" data security safeguards, Simons told a House Energy and Commerce Subcommittee earlier this month that the commission planned to continue "to prioritize, examine and address privacy and data security with a fresh perspective," Klein said.

The approach the FTC will take on privacy and data security issues, particularly what level of harm is necessary to support an unfairness claim under Section 5 of the FTC, is likely to be determined in large part by what the commissioners take away from a series of public hearings that the agency will hold beginning in September to address whether changes in the economy, technological advances or other developments have created a need for adjustments to the agency's enforcement approach or priorities, attorneys say.

"The biggest thing to watch during this hearings will be the attitude of the new commissioners," said Mayer Brown LLP partner Stephen Lilley. "So far, all of the signals indicate that they'll still inclined to be very active on data security issues, but it will be interesting to see what industries they focus on and which way they are leaning when it comes to over what conduct they believe the commission can bring an enforcement action."

The hearings will come on the heels of a recent Eleventh Circuit ruling that struck down data security changes that the commission had ordered LabMD Inc. to undertake, which is expected to change and potentially limit how the FTC seeks remedies in these types of disputes, attorneys said.

"The FTC is at a bit of a crossroads right now because of the setback it had with the Eleventh Circuit decision in the LabMD case challenging their ability to impose mandates that generally require reasonable security without more detailed framework around what that means, coupled with the interest that incoming Chairman Simons has expressed in announcing the upcoming series of hearings in expanding the FTC's authority in order to regulate some of these large tech platform's data-handling practices," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

The FTC is also expected in the coming months to make progress on a probe that it confirmed in March into millions of Facebook users' personal data being swept up by Cambridge Analytica, to build on efforts to show Europeans that the commission is tough on those that don't adhere to Privacy Shield, and to continue to press Congress to give it the power to issue data security rules and impose fines, as the commissioners did during the recent House hearing, according to attorneys.

"Having four commissioners joining the FTC at the exact same time is unprecedented," said Drinker Biddle & Reath LLP counsel Katherine Armstrong, who spent more than 30 years at the FTC. "All have indicated an interest in technology and to some extent privacy and data security, but the FTC has limited authority because it can't do rulemaking. The hearings beginning this fall will be an opportunity to raise some of these issues against the backdrop of changing privacy norms and consumer expectations."

California Privacy Law Matures

California lawmakers hastily enacted a sweeping privacy bill last month to avoid a more stringent measure being presented to voters in November. But while the measure, which for the first time will require businesses to be more upfront with customers about the personal data they collect and give consumers broad latitude to control how companies use and share their personal information and to request its deletion, won't take effect until January 2020, the bill's passage has sparked plenty of questions and anxiety that will carry through the rest of the year, attorneys say.

"The passage of the California Consumer Privacy Act feels like kind of a watershed moment in U.S privacy regulation because for the first time principles like those in the EU's general data protection regulation are being implemented in the U.S. and changing the states' approach to privacy and cybersecurity regulation," Hirsch said.

Over the next year and a half, attorneys are expecting not only to see guidance from the California attorney general to clear up questions over how to comply with notice and deletion obligations, but also for the Legislature to address widespread concerns among business leaders about the scope of the law, who's allowed to bring suit under it and the breadth of companies' obligations to consumers, according to attorneys.

Because changes to the law within the next year are highly likely, attorneys are recommending that companies hold off on overhauling their notice and consent procedures until they know more about their exact requirements. However, businesses that will be swept up by the law can use the next six months to continue the process many had started when getting ready for the GDPR in Europe of taking stock of their data and where it's located.

"While it's uncertain how much the breadth of the law will change, the fundamental data access rights that consumers have seem to be the hallmark of the law and will require business to understand what data they have and what they're doing with it in order to be able to satisfy consumers' requests," Armstrong said.

While these type of data mapping exercises aren't "particularly sexy," they are crucial for compliance, Klein said.

Attorneys will also be watching whether other states or cities follow California's lead, as they did with data breach notification statutes, which started in the Golden State in 2002 and have since spread to all 50 U.S. states.

"Once one or two states jump out with standards, it doesn't take long for other states to follow and create their own standards," said Mark Krotoski, a partner and co-leader of Morgan Lewis' privacy and cybersecurity practice. "California has always been considered a bellwether state, and if other states consider enacting these types of standards, we cold see similar issues as we did with breach notification where companies are facing different rules at the state level."

GDPR Enforcement Actions Loom

While one of the main events from the first half of 2018 was the EU's stringent General Data Protection Regulation officially taking effect on May 25, the regulation will continue to loom large in the second half of the year, as companies anxiously await further guidance and the first enforcement actions under the law, which carries the potential for eye-popping fines of up to 4 percent of a company's annual global revenue.

"Everybody is looking for guidance from regulators on exactly how these GDPR standards should be applied in practice, and the hope is that regulators are thinking about the instructive value of these enforcement actions as a general matter," Lilley said, adding that the first enforcement action under the GDPR is likely to be followed "extremely closely by every company" to get a better sense of how regulators are interpreting key provisions of the regulation.

The lessons gleaned from enforcement actions are likely to help companies that have spent the past several years getting ready for the regulation to take effect to address nuances and further refine their compliance efforts, which like the California privacy law included taking stock of their data so that they could be responsive to consumer demands.

“Speaking from a technical perspective, companies are starting to understand that at the end of the day, proactive data governance and controls are the way to respond to all regulation,” said Andy Gandhi, a managing director with Alvarez & Marsal's disputes and investigations practice.

Experts will also be "anxiously watching" to see whether the implementation of GDPR will spark new laws in other countries, according to Mayer Brown partner Lei Shen, who specifically pointed to examples such as Brazil's recent passage of its own version of the GDPR and the approval of the California Consumer Privacy Act, "which also has GDPR-like protections and requirements."

Gandhi noted that given the global nature of the GDPR, which impacts not just EU companies but global multinationals that have any kind of personal data that touches the EU, it's unlikely that other countries will be quick to act until they have a better sense of the benefits of GDPR enforcement.

"Other countries such as India or Singapore might not care about laws like this until they see how the GDPR generates fines for regulators to protect consumers and change companies' behavior," Gandhi said.

ECPA Update May Finally Be in the Cards

While the upcoming midterm elections are likely to stymie most efforts at the federal level to enact sweeping privacy changes, attorneys are hopeful that one long-standing proposal might finally slip through: an overhaul of the decades-old Electronic Communications Privacy Act that would create a blanket warrant requirement for the contents of all electronic communications.

Unlike in previous years, where proposals have overwhelmingly passed in the U.S. House of Representatives only to be shut down in the Senate, lawmakers have tucked these privacy provisions into the must-pass defense spending bill for the 2019 fiscal year, the National Defense Authorization Act. That version was approved by the House in June and faces reconciliation with a Senate-passed measure that didn't include the ECPA overhaul.

"There might be a better chance for the Email Privacy Act this year than in past years, because right now it's in the NDAA that has to pass," Dayanim said. "Of course, those provisions could still be striped out of the bill that was passed in the House, but it seems like there's a really good chance that they'll stay in."

Both tech and privacy leaders support the legislative changes, with stakeholders including Google, Amazon.com Inc., Facebook, the American Civil Liberties Union and the U.S. Chamber of Commerce recently joining forces**,** as they have in past congressional terms, to urge Congress to pass a version of the NDAA that preserves the ECPA changes.

"For individuals, the proposed changes grant additional protections to emails from governmental acquisition by requiring a warrant no matter how long an email has been sitting in an inbox, and for companies the main implication is knowing that a warrant is required before they can provide the government with access to that email, and being able to show that they are protective of users' privacy," Dayanim said.

Reynolds added that efforts to update statutes such as ECPA, which currently allows law enforcement to obtain emails that are more than 180 days old without a warrant, and similar outdated rules for government access to user data could be further boosted by the U.S. Supreme Court's recent ruling in Carpenter v. U.S. that law enforcement generally needs a warrant to access historical cellphone location records.

"The really interesting thing the Carpenter ruling said was that cellphone location data is different than other information that law enforcement looks at," Reynolds said. "That sort of opens up a Pandora's box of people interpreting what this means for other types of electronic data and thinking about enhancing existing laws or enacting different laws to reflect that ruling at both the state and federal level."

--Editing by Brian Baresch and Katherine Rautenberg.
