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 And Cybersecurity Cases To Watch In 2nd Half Of 2019

By **Allison Grande**

Law360 (July 12, 2019, 9:20 PM EDT) -- The fallout from U.S. Supreme Court rulings about how much weight to give regulatory decisions and what harm plaintiffs need to allege in privacy litigation will continue to inspire conflicting results in the second half of 2019 in the U.S., while Europe's top court is poised to determine the fate of vital transatlantic data transfer mechanisms, experts told Law360.

Here are the cases that privacy and cybersecurity attorneys said they will be watching in the next six months.

No End in Sight for TCPA Confusion

The wave of litigation under the Telephone Consumer Protection Act shows no signs of abating after the Supreme Court last month passed up an opportunity to deliver clarity on who has the final say on how the law is interpreted.

In a unanimous decision with two notable concurrences, the high court sidestepped the question of whether district courts are required under the Hobbs Act to defer to the Federal Communications Commission's numerous interpretations of the TCPA. The ruling is expected to fuel continued uncertainty by giving judges significant leeway to come down on either side of the debate, attorneys say.

"The Supreme Court left a lot of unanswered questions, which unfortunately means there’s going to be judges who are in the same courthouses across the hall from one another reaching different conclusions about what the Supreme Court decision means for any particular FCC order or pronouncement," attorney Mark Eisen of Benesch Friedlander Coplan & Aronoff LLP told Law360.

The dispute over an allegedly offending fax that chiropractic group PDR Network sent to chiropractic group Carlton & Harris now heads back to the Fourth Circuit, which had found that the lower court was required to accept the FCC's statutory interpretation wholesale.

The Supreme Court ruling vacates this decision and leaves it up to the Fourth Circuit to consider on remand whether the challenged FCC order was a legislative or interpretive rule and whether PDR Network had been afforded an adequate opportunity to challenge the order. The answer to these questions will inform whether the Hobbs Act, which gives appellate courts "exclusive jurisdiction" to determine the validity of agency orders, applies to the disputed FCC order in this case.

Attorneys will be watching not only how the Fourth Circuit handles this directive, but also how it affects the hundreds of cases pending under the TCPA.

The high court's decision also likely paves the way for the FCC to finally take action on what constitutes an autodialer and how to avoid liability for calling reassigned numbers under the TCPA. The FCC was pushed to take another stab at interpreting these provisions in the wake of a successful Hobbs Act challenge mounted by ACA International and others that resulted in the D.C. Circuit striking down a consumer-friendly 2015 FCC order on these issues.

Judges will have leeway to scrutinize the new FCC order in light of the Supreme Court's latest ruling. But the agency's new interpretation could clear up confusion that has driven a circuit split over the weight of earlier FCC orders, and how these terms should be defined, attorneys say.

"In a lot of ways, the FCC was waiting for the Supreme Court to rule, and now it's the FCC's turn," Eisen said.

TCPA practitioners also will be keeping an eye on litigation in Oregon that has the potential to subject health supplement marketer ViSalus to $925 million in damages for blasting consumers with more than 1.8 million unsolicited robocalls.

Few TCPA disputes go to trial, and the case highlights the massive liability businesses face under the statute. The federal judge overseeing the case refused last month to triple or otherwise enhance the potential statutory damages. He is expected to rule in the coming weeks on ViSalus' motion to decertify the class, which could significantly alter or even negate the jury's verdict and the resulting damages award.

"We'll be watching to see if the verdict holds up," Edelson PC founder Jay Edelson, whose firm is representing plaintiff Lori Wakefield in the ViSalus case, told Law360.

The remanded Supreme Court case is Carlton & Harris Chiropractic v. PDR Network LLC, case number 16-2185, in the U.S. Court of Appeals for the Fourth Circuit.

The $925 million TCPA case is Wakefield v. ViSalus Inc., case number 3:15-cv-01857, in the U.S. District Court for the District of Oregon.

Standing Issues Persist

Federal courts continue to be divided over what types of harm are sufficient to meet the Article III standing bar established by the Supreme Court's landmark rulings in Clapper v. Amnesty International and Spokeo v. Robins. Attorneys hope for some of the fog to be lifted in the coming months.

"Despite the volume of cases in recent years, the field is not getting clearer," said Kirk Nahra, co-chair of the cybersecurity and privacy practice at WilmerHale.

The challenge over a massive 2015 data breach at the U.S. Office of Personnel Management could be particularly important to scaling back some of this confusion, attorneys say. The D.C. Circuit broke with several sister courts in ruling last month that the heightened risk of identity theft stemming from the breach was enough to establish standing.

"The Supreme Court could provide valuable guidance around the type of allegations that need to be included in complaints to establish standing after data breaches, because right now in different circuits the same allegations can lead to different results based on how courts perceive the risk of future harm from those allegations," said Mayer Brown LLP partner Stephen Lilley.

The high court in March refused to weigh similar standing issues in litigation over a data breach at online retailer Zappos.com, which like the OPM dispute turned on whether the alleged injuries were more than merely speculative, as required by the Clapper decision.

Attorneys are hopeful that the OPM case will be more enticing to the justices.

"Because of the particular facts and nature of information at issue in the OPM case, if the parties did decide to pursue an appeal to the Supreme Court, the case could present the standing question pretty squarely to the court," Lilley said.

The standing landscape in disputes that involve alleged statutory privacy violations also remains murky, attorneys say.

The Supreme Court held in its 2016 Spokeo decision that harm must be concrete and mere statutory violations do not suffice. But that ruling has only served to further divide courts considering disputes

under statutes such as the Fair Credit Reporting Act, which was at the heart of the Spokeo case, according to Troutman Sanders LLP partner David Anthony.

The Fair and Accurate Credit Transactions Act, an amendment to the FCRA, has also sown discord and could prompt high court review.

The D.C. Circuit earlier this month found standing for claims that concessionaire Centerplate unlawfully printed all 16 digits of a customer's credit card number on a receipt. The ruling jibed with the Eleventh Circuit's decision last year that a customer had suffered a "concrete injury" simply by receiving a faulty receipt from Godiva, but conflicted with rulings by four other appellate courts.

The credit transactions act provides a "unique opportunity" for the court to address the standing split, Eisen said. These disputes typically don't involve instances of identity theft, he said, leaving a clear path to the threshold question of how immediate the risk of harm must be to establish standing.

"If it’s accepted on appeal, the issue would really force the Supreme Court to evaluate what Spokeo meant in the most fundamental sense, because this is really a situation in which the courts will have to analyze whether Congress can simply create a cause of action and say that, by the nature of this law, individuals have standing," Eisen said.

The OPM case is In re: Office of Personnel Management Data Security Breach Litigation, case numbers 17-5217 and 17-5232, in the U.S. Court of Appeals for the District of Columbia Circuit.

The FACTA case is Jeffries et al. v. Volume Services America Inc. d/b/a Centerplate/NBSE et al., case number 18-7139, in the U.S. Court of Appeals for the District of Columbia Circuit.

Data Transfer Tools Under Fire

Less than five years after the European Court of Justice struck down the popular safe harbor mechanism that allowed data to flow freely between the U.S. and the European Union under companies' promise it would be protected, the high court again has the chance to upend the global data transfer landscape.

The EU high court’s 2015 ruling deeming safe harbor to be inadequate “wreaked havoc” on transatlantic data transfers and caused most businesses to turn to either standard contractual clauses, which are also known as model clauses, or the Privacy Shield, which was put in place to replace safe harbor, according to Lisa Sotto, who chairs Hunton Andrews Kurth LLP's privacy and cybersecurity practice.

Now, both of those popular mechanisms are under attack, with the Court of Justice hearing arguments on July 9 in a dispute over the legality of these tools that was initiated by Max Schrems, the same Austrian privacy activist who successfully challenged safe harbor.

"The vast majority of companies in Europe rely on model clauses or the Privacy Shield to transfer data, so if the EU Court of Justice chooses to invalidate either mechanism, then in theory at least, commerce should come to a grinding halt,” Sotto said. "Data won’t be able to move between the EU and nonadequate countries like the U.S., and it’ll be impossible to conduct business."

There was some initial trepidation with implementing Privacy Shield, since companies that had relied on safe harbor "had just been burned," Sotto noted. But comfort with the mechanism has grown as it has survived two annual reviews, and nearly 5,000 companies — including Google, Facebook and Microsoft — have signed up to take advantage of the tool, according to the U.S. Department of Commerce.

With Privacy Shield and standard contractual clauses under the microscope, these companies could face another shakeup in the near future. The court's advocate general is expected to release an influential advisory opinion in three to six months, and the Court of Justice will follow soon after with its final determination.

Sotto predicted that Privacy Shield was the more likely of the two to survive, given that it's “the

more modern mechanism and takes into account the criticisms that were leveled against safe harbor."

If the data transfer tools don't pass the high court's review, companies will only be left with binding corporate rules, which are significantly more complex and take over a year to put into place, Sotto added.

"The hope is that if the court strikes down these mechanisms, there will be some grace period declared so that companies can try to find other mechanisms," Sotto said.

Biometric Privacy and State AG Enforcement

The flood of class action litigation under Illinois' Biometric Information Privacy Act is beginning to produce rulings that clarify key elements of the unique statute, and attorneys expect further light to be shed on the contours of the law in the coming months.

Employers facing claims from unionized workers are likely to derive some relief from a recent Seventh Circuit ruling that sent claims over fingerprints collected for timekeeping purposes by Southwest Airlines Co. and United Airlines Inc. to arbitration. But suits over the commercial use of biometric data are going stronger than ever in the wake of the Illinois Supreme Court's declaration in Rosenbach v. Six Flags that plaintiffs don't need to allege actual harm to file a case.

"While the Six Flags decision was well-reasoned, it really opened the door to a very significant amount of litigation that we'll be watching," Sotto said.

A key dispute to track will be Facebook's appeal to the Ninth Circuit of a ruling that certified a class of Illinois users who allege the social media giant's face-scanning practices violate BIPA, according to Edelson, whose firm represents the plaintiffs in that suit.

The Ninth Circuit heard oral arguments in June, with Facebook asserting that the decision to certify the class should be overturned because the ruling could lead to an "enormous statutory damages award" even though users haven't been harmed.

Whether attorneys general in Texas and Washington begin enforcing the biometric privacy laws on the books in their states will also bear watching, Sotto said. While Illinois is the only state with a biometric privacy law that allows consumers to sue, the Texas and Washington statutes provide for attorney general enforcement, although no such actions have been publicly announced.

Outside the BIPA context, attorneys general have been increasingly aggressive in policing privacy missteps and data breaches, and how they continue to deal with these incidents will be notable as well, attorneys say.

Aside from launching multistate probes, attorneys general have begun bringing private litigation over significant data security and privacy breaches. These include suits filed by the attorneys general of Massachusetts, Indiana, West Virginia and Puerto Rico and by the cities of Chicago and San Francisco on behalf of their residents in the wake of Equifax's massive data breach.

Goodwin Procter LLP privacy and cybersecurity practice chair Brenda Sharton, who has been handling data breaches for over 20 years, flagged as particularly notable the Massachusetts attorney general's litigation against Equifax. The suit was the first of its kind to be filed and received a boost last year when a state court judge issued a ruling that allowed it to move forward.

"Companies will be watching it closely as it represents a shift in a more aggressive direction, though the facts may have contributed to the AG's decision to file," Sharton said.

The Facebook case is Patel et al. v. Facebook Inc., case number 18-15982, in the U.S. Court of Appeal for the Ninth Circuit.

The Massachusetts AG's suit is Commonwealth of Massachusetts v. Equifax Inc., case number 1784-cv-3009, in Suffolk County Superior Court.

Growing Liability Risks for Health Data Use, Connected Devices

As companies embrace new technologies and consumers' understanding of how their data is being used continues to grow, litigation will keep popping up that has the potential to raise new liability risks for a range of companies.

A case that fits this mold is a recent lawsuit filed by attorneys at Edelson PC against the University of Chicago Medical Center and Google LLC. The suit claims that the university broke its privacy promise with the plaintiff and hundreds of thousands of fellow patients when it shared their medical information, but not their names or other identifying information, with the search giant.

The dispute "challenges a lot of the existing approaches to how de-identification works in the health care industry and would create some real concerns in the industry and for health care policymakers generally if this resulted in a reduced ability to use and disclose de-identified health care data," Nahra said.

Those who make connected devices and products that are part of the growing "internet of things" will also be keeping a careful eye on how consumers respond to security flaws that researchers may uncover, according to Lilley, the Mayer Brown partner.

"As security researchers focus more on these devices, a pattern could develop where security researchers look for these vulnerabilities and find them, and then plaintiffs bring lawsuits claiming that they paid a certain amount for the product and, due to these vulnerabilities, the product wasn't worth what they paid," Lilley said.

These cases have already started to emerge, and more are expected to be filed in the near future.

Some notable pending cases to monitor include a certified class action against Fiat Chrysler claiming Jeep Cherokees are vulnerable to hacking, which the Supreme Court declined to consider in January, and litigation against a Chinese sex toy maker that allegedly illegally harvested data from its users, according to Troutman Sanders partner Mark Mao.

A California federal judge in May allowed most of the sex toy case to stand after finding for the first time that vibration intensity settings are "content" under wiretapping law. Mao said it will be interesting to watch "how wiretap and interception claims evolve as a result" of this ruling.

The health information dispute is Dinerstein v. Google LLC et al., case number 1:19-cv-04311, in the U.S. District Court for the Northern District of Illinois.

The Jeep case is Flynn et al. v. FCA US LLC et al., case number 3:15-cv-00855, in the U.S. District Court for the Southern District of Illinois. The sex toy case is S.D. v. Hytto Ltd., d/b/a/ Lovense, case number 4:18-cv-00688, in the U.S. District Court for the Northern District of California.

--Additional reporting by Ryan Boysen, Dorothy Atkins, Dave Simpson and Ben Kochman. Editing by Jill Coffey and Alanna Weissman.
