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

5 Cybersecurity And Privacy Cases To Watch

By **Allison Grande**

Law360, New York (July 3, 2017, 1:38 PM EDT) -- The coming months promise action on many long-running cybersecurity and privacy disputes, including a closely watched challenge to a federal regulator's reach in controlling data security, the continued unpacking of the U.S. Supreme Court's pivotal ruling on Article III standing, and a decision that has the potential to stem the tide of litigation under the Telephone Consumer Protection Act.

In interviews with Law360, privacy and cybersecurity attorneys discussed cases on their must-watch lists for the remainder of 2017.

LabMD Takes FTC to 11th Circ.

The Eleventh Circuit in June heard oral arguments in a long-running case pursued by medical testing laboratory LabMD that attorneys say is likely to dictate how far the Federal Trade Commission is allowed to go in policing privacy and data security issues.

The dispute began in 2013 when LabMD Inc. became the second company, after Wyndham Worldwide Corp., to challenge the commission's allegations that it violated the unfairness prong of Section 5 of the FTC Act by failing to institute reasonable data security practices.

LabMD took the dispute to the Eleventh Circuit last year after top FTC officials overturned their own administrative law judge in concluding that the company's failure to employ "basic" security precautions led to an unauthorized disclosure of sensitive medical data. That disclosure, the FTC asserted, caused "substantial" harm to consumers, in violation of the unfairness prong.

The appellate court granted the lab's bid to stay, determining that the now-defunct LabMD would be irreparably harmed without it and concluding that the dispute presented substantial legal questions. The Eleventh Circuit heard oral arguments in the dispute on June 21, and a decision on the case is expected in the coming months.

"I'm still watching the LabMD case, to see if the courts restrict — or support — the FTC's overall efforts on data security and standards under which it can act," said Kirk Nahra, Wiley Rein LLP privacy practice chair. "It's not clear whether the new [Trump] administration will take the same path, but the courts could define an answer on this."

"The case presents important questions about the nature and probability of injury that the FTC must demonstrate to prove that a company's data security practices are 'unfair,'" said Janis Kestenbaum, a partner at Perkins Coie LLP and onetime senior adviser to former FTC Chairwoman Edith Ramirez. "The Eleventh Circuit's stay of the FTC's opinion suggests that the FTC's position that it must only show a 'significant' risk of injury, not that such injury is likely or probable, may not prevail."

LabMD is represented by Doug Meal, David Cohen, Michelle Visser and Douglas Hallward-Driemeier of Ropes & Gray LLP.

The FTC is represented by staff attorneys Theodore Metzler and Michael Hoffman.

The case is LabMD Inc. v. Federal Trade Commission, case number 16-16270, in the U.S. Court of Appeals for the Eleventh Circuit.

Spokeo Still Going Strong

The U.S. Supreme Court's May 2016 decision in Spokeo v. Robins, which holds that plaintiffs must allege concrete harm and cannot rely on mere statutory violations to establish Article III standing, has been dividing courts across the nation.

"We're living in a post-Spokeo world, and at this point the meaning of Spokeo is still being litigated, but it's obviously a very significant case when it comes to Article III standing," said Stephen Lilley, a Mayer Brown LLP partner.

In the year since the court handed down the watershed privacy decision, lower courts have issued a wave of conflicting decisions in cases under the Fair Credit Reporting Act, the Telephone Consumer Protection Act and the Fair and Accurate Credit Transactions Act.

These disputes are beginning to work their way up to the appellate courts, where attorneys are keeping careful watch on whether a circuit split emerges on the issue of whether a statutory harm is enough to allow plaintiffs to forge ahead with their claims.

Of particular interest to attorneys is the Spokeo dispute itself, which the Supreme Court justices remanded to the Ninth Circuit after concluding that the lower court had conducted an incomplete injury analysis related to the plaintiffs' FCRA claims. Meanwhile, an Eleventh Circuit decision looms in Price v. Godiva Chocolatier, which deals with the applicability of Spokeo to FACTA lawsuits.

"As of now, district courts in the Eleventh Circuit are the only courts in the country — with minor exception — finding that violations of FACTA give rise to standing per se," said David Almeida, a partner with Benesch Friedlander Coplan & Aronoff LLP. "Should the Eleventh Circuit reverse here and find that there is no standing for bare violations of FACTA, FACTA cases may be entirely relegated to state court. If the Eleventh Circuit disagrees with the Seventh Circuit, we may be well on our way to a Supreme Court clarification of Spokeo."

The Spokeo case centered on statutory privacy violations, but attorneys say that they also will watch in coming months to see how the Supreme Court's standing determination is applied to disputes involving corporate data breaches.

A pair of data breach cases have already worked their way to the appellate courts — Alleruzzo

v. SuperValu in the Eighth Circuit and Attias v. CareFirst in the D.C. Circuit. Attorneys say it's only a matter of time before the Supreme Court will be asked to tackle the question of whether consumers who have had their data exposed, but not misused, have suffered enough of an injury to move forward.

"In 2012, the Supreme Court denied a petition for writ of certiorari to address the question of standing in data breach cases in Reilly v. Ceridian Corp., but I expect the issue to be before the Supreme Court again soon," said Kristin Ann Shepard, a shareholder with Carlton Fields Jorden Burt PA.

"A favorable ruling for businesses on the standing issue would greatly reduce their litigation exposure in the event of a large-scale breach," she continued, "as only a minority of those whose information is compromised will ultimately experience identity theft or unreimbursed fraudulent charges."

Supreme Court Takes On Location Privacy

The Supreme Court in early June agreed to review the Sixth Circuit's 2016 decision in Carpenter v. U.S., which held that a phone's cell-site location information counts as a routinely collected business record that the government can gather without a warrant as long as the data reveals nothing about the actual content of cellphone communications.

Attorneys are keeping close tabs on the case to see how the justices decide on the expectation of privacy that individuals have in the personal information that they hand over to third-party service providers, such as cellphone carriers.

"What will be significant is whether it's decided that we have a diminished expectation of privacy in information that we purportedly, theoretically voluntarily, turn over to third parties," said Scott Vernick, Fox Rothschild LLP privacy and data security practice leader. "It's pretty clear that when we're walking on the street we don't have much of an expectation of privacy, but the question becomes is that expectation the same on the virtual highways and byways."

Experts anticipate that the case will require the justices to revisit the third-party doctrine, which the Supreme Court established in its Smith v. Maryland decision of 1979. The court in that case ruled that individuals do not have a reasonable expectation of privacy concerning information they voluntarily provide to third parties, like phone companies.

Since that decision, the court has issued two decisions that supported the notion that digital evidence deserves heightened privacy protections: The 2012 decision in U.S. v. Jones that the installation and monitoring of a GPS device on a suspected drug dealer's vehicle constituted a "search" under the Fourth Amendment and its 2014 holding in Riley v. California that law enforcement personnel may not search detained suspects' cellphones without a warrant.

Attorneys say they are eager to see not only how the justices deal with the new digital privacy issues in view of their previous determinations, but also whether the ruling more broadly impacts the regulation of location data collection.

"The FTC has taken the position that geolocation data shouldn't be collected without explicit consent, and that's become a best practice," said Mary J. Hildebrand, chair of the privacy and information security practice at Lowenstein Sandler LLP. "While the Carpenter case arose from a criminal situation, I'm wondering what impact the decision might have on the FTC's position with respect to the collection of that data for commercial purposes, in addition to what this might mean for surveillance practices in the U.S."

Carpenter is represented by Nathan Freed Wessler of the ACLU Foundation.

The government is represented by acting Solicitor General Jeffrey Wall of the U.S. Department of Justice.

The case is Carpenter v. U.S., case number 16-402, in the Supreme Court of the United States.

TCPA Faces a Pivotal Ruling

Attorneys on both sides of the recent explosion in TCPA litigation eagerly anticipate the D.C. Circuit's looming decision in a challenge led by ACA International to a June 2015 Federal Communications Commission order that expands the scope of the TCPA in an effort to crack down on telemarketing robocalls.

The order broadened the definition of "autodialer," set strict conditions on calling reassigned numbers, and gave consumers wide latitude to revoke consent. Businesses have argued that it went too far, while the FCC has countered that its order was carefully considered and well-reasoned.

"The D.C. Circuit's ruling has the potential to radically reduce the effectiveness of the TCPA as a class action weapon by narrowing the definition of automatic telephone dialing system," said Michael Rhodes, chair of Cooley LLP's privacy and data protection practice group.

Both the autodialer issue as well as questions over the ability of companies to call reassigned numbers and individuals who have withdrawn their consent have fueled the flood of TCPA litigation. Additionally, many cases have been stayed in anticipation of the circuit court's decision in the wake of oral arguments held in October, Troutman Sanders LLP partner David Anthony noted.

Lawyers expect that the D.C. Circuit's decision will go a long way to determining whether companies will continue to face claims that subject them to uncapped statutory damages of $500 and $1,500 per violation, or whether they begin to feel some relief.

"If the FCC is forced to go back to the drawing board here on any aspect of the omnibus order, we can expect the current commission, in light of the new administration, to make many defense-oriented changes that will likely have a lasting impact on the viability of TCPA cases going forward," Almeida said.

Jaszczuk PC founder Martin Jaszczuk agreed that the current FCC, led by Commissioner Ajit Pai, "espouses a real-world view of the TCPA that would both protect consumers and keep regulations fair for the industry."

He said that the D.C. Circuit's recent ruling in Bais Yaakov of Spring Valley v. FCC, which struck down a rule that required opt-out notices to be placed on solicited faxes, gave a significant boost to the prospect that the appellate court "will bring rationality" to the TCPA definitions established by the Obama administration.

"There is significant cause for hope that the D.C. Circuit will once again deliver a sound ruling, grounded in principle, that brings fairness to the TCPA and its regulations," Jaszczuk said.

The case is ACA International v. Federal Communications Commission et al., case number 15-1211, in the U.S. Court of Appeals for the District of Columbia Circuit.

Biometrics, Connected Devices Continue to Heat Up in Court

With the growing prevalence of internet-connected devices and biometric identifiers for use in everything from fraud prevention to digital advertising, legal risks also are expanding, attorneys say.

"I'm watching for more privacy class action lawsuits to be filed that are based on how companies are using and sharing sensitive information; as opposed to cases that arise from data breaches," said Al Saikali, Shook Hardy & Bacon LLP data security and privacy group chair.

In March, the maker of an internet-enabled vibrator that can be controlled remotely by an app agreed to pay $3.75 million to settle a suit alleging it had secretly collected intimate information from users, such as when and on what settings the device was used. Attorneys expect a proliferation of claims challenging device makers' data collection and security practices as more connected products go online.

"It's a potential issue for manufacturers to think through on the back end because people are going to be looking at those products with an eye toward litigation," Lilley said.

Disputes surrounding the collection and use of biometric data such as fingerprints and face scans also still are in early stages. Illinois is the only state to enact a biometric privacy law, the Illinois Biometric Information Privacy Act, and attorneys say they'll be watching how that litigation develops.

Almeida cited two noteworthy disputes: In re: Facebook Biometric Information Privacy Litigation in the Northern District of California, and Rivera v. Google in the Northern District of Illinois.

Each case concerns the Illinois biometric privacy law and raises threshold issues such as Spokeo's impact, whether the state law can apply extraterritorially and whether the the biometric law applies to information derived from photographs through tagging features, Almeida said.

The Facebook case is stayed pending the Ninth Circuit's rehearing of Spokeo, he said, and Google is seeking to appeal to the Seventh Circuit an adverse decision on their motion to dismiss.

Almeida predicted that the cases will "significantly impact" the viability of the Illinois biometric privacy law.

--Editing by Rebecca Flanagan and Katherine Rautenberg.
