Privacy Cases To Watch In 2016: Midyear Report

Allison Grande
New York
Law360
07.22.2016

Law360, New York (July 22, 2016, 2:32 PM ET) -- The privacy legal landscape shows no signs of cooling off in the second half of the year, with the continued fallout from the U.S. Supreme Court's landmark Spokeo ruling, disputes concerning the Federal Trade Commission's data security authority and the validity of the new trans-Atlantic data transfer Privacy Shield likely to dominate the headlines.

Here, attorneys flag some of the top cases that they'll be keeping their eye on in the second half of 2016.

Spokeo Fallout

In handing down **its hotly-anticipated decision** in Spokeo v. Robins in May, a shorthanded Supreme Court not only produced what is widely considered to be the most significant privacy decision of the first half of the year, but also sparked a debate that is expected to generate many more notable privacy rulings in the coming months, attorneys say.

"The Supreme Court punted on Spokeo, meaning that there will be continuing fights both about its meaning and on the broader standing and injury issue in general," Wiley Rein LLP privacy practice chair Kirk Nahra said.

The high court justices in their 6-2 ruling held that in order to maintain Article III standing, a plaintiff must allege a tangible or intangible concrete injury and cannot rely solely on a mere statutory violation. However, the majority declined to apply this test to the specific dispute in front of it, electing instead to take the rare step of sending the dispute back to the Ninth Circuit to consider whether plaintiff Thomas Robins had pled harm that was particularized and concrete, which would allow him to continue with his suit accusing Spokeo of violating the Fair Credit Reporting Act.

The justices' refusal to opine on how the Article III standing test they laid out would work in practice has left the door open for both plaintiffs and defendants in a range of consumer protection and data breach disputes to seize on the analysis and attempt to use it in their favor. Since the high court's ruling, scores of litigants have raised Spokeo in a range of matters, including in actions over **a data breach** at Paytime and alleged violations of the Video Privacy Protection Act by media outlets such as CNN and USA Today.

"We should be tracking every case now arguing Spokeo to see whether there are more winners or losers," Fox Rothschild LLP privacy and data security practice leader Scott Vernick said. "That way, we would have some

empirical data about whether Spokeo is ultimately pro plaintiff or pro defendant."

In addition to the wide array of cases under the FCRA, VPPA, Telephone Consumer Protection Act and a range of other statutes whose disposition may hinge on Spokeo, attorneys say that they will also be keeping an eye on the dispute that started it all, which is back before the Ninth Circuit. Spokeo **fired its opening salvo** in that dispute earlier this month, when it filed a brief arguing that the presence of untrue information on a website by itself is not a material-enough harm as defined by the Supreme Court for a lawsuit to stand.

"This case [before the Ninth Circuit] should set something of a high-watermark for what constitutes a concrete injury under FCRA specifically, but will likely have much broader implications for similar no-harm statutes," Sheppard Mullin Richter & Hampton LLP partner David Almeida said.

The remanded case is Thomas Robins v. Spokeo Inc., case number 11-56843, in the U.S. Court of Appeals for the Ninth Circuit.

FTC v. LabMD

With its aggressive data security enforcement efforts, the Federal Trade Commission has positioned itself in recent years as the nation's top privacy cop. But that calculus may shift, depending on the outcome of a battle that LabMD has long been fighting with the regulator over its ability to go after companies for allegedly lax data security practices.

"We'll be watching the FTC's decision in LabMD, to see whether the FTC has authority to pursue security breach cases even without consumer harm," Nahra said.

The parties' long-running dispute dates back to 2013, when LabMD **became the second company**, after Wyndham Worldwide Corp., to push back on rather than settle the commission's data security allegations. The Wyndham dispute came to an end last year, after the Third Circuit in August **affirmed the agency's authority** to regulate data security.

But the LabMD dispute turned out differently, with one of the FTC's administrative law judges in November **dismissing the case** on the grounds that the agency had failed to meet its burden of proof under the unfairness prong of Section 5 of the FTC Act because there was no evidence that any consumers had suffered harm.

The FTC immediately appealed the ruling to the agency's acting commissioners, who **heard oral arguments** in the dispute in March. The commissioners were slated to announce their decision in June, but on the day of their deadline **issued an order** giving themselves until July 28 to reach a final determination.

"The Spokeo decision sort of fit together with what the FTC though it could do — the FTC could act whether or not there was identifiable consumer harm, meaning that the private litigation could be limited to 'harm' situations," Nahra said. "But, maybe not, depending on the outcome of LabMD."

Janis Kestenbaum, a partner at Perkins Coie LLP and former senior legal adviser to FTC Chairwoman Edith Ramirez, agreed that how the commissioners resolve the question of what harm is required to maintain an unfairness claim will have a "big impact" on not only the commission's data security enforcement efforts but also the approach taken by other federal and state regulators.

"But the commission's decision may not be the last word," Kestenbaum added. "LabMD has been a heated, acrimonious fight, and if the commission rules against LabMD, it is headed for the Eleventh Circuit or another court of appeals."

The case is In the Matter of LabMD Inc., docket number 9357, before the Federal Trade Commission.

Microsoft Fights The Feds, Part 2

In April, Microsoft **lodged a headline-grabbing suit** in Washington federal court challenging the government's ability to force service providers to keep customers in the dark about law enforcement demands to access user data.

With the Second Circuit earlier this month **having backed Microsoft's stance** in a separate case in ruling that the U.S. government cannot use search warrants to reach customer data stored overseas, attorneys' attention for the second half of the year will now turn to the latest legal drama to see if Microsoft can again prevail.

How the Microsoft case, which asserts that the government "gag orders" are unconstitutional, plays out will be particularly interesting in light of another development that rose to prominence during the first half of 2016: Apple's bicoastal fight with the government over the FBI's demand to help unlock iPhones, which ended rather benignly after the government found ways to break into the devices without the tech giant's help and dropped the disputes.

"The Apple fight certainly sensitized people to these issues and made people thing more about this whole area, and now Microsoft has sued the Department of Justice as a follow-on to further expand some of these issues," Hughes Hubbard & Reed LLP data privacy and cybersecurity group co-head Dennis Klein said.

The case is Microsoft Corp. v. the U.S. Department of Justice et al., case number 2:16-cv-00538, in the U.S. District Court for the Western District of Washington.

Privacy Shield Challenge

Outside of the U.S., one of the most closely-tracked developments in the first six months of this year has been the evolution of negotiators' efforts to replace the more than decade-old safe harbor deal, which allowed thousands of multinationals including Google and Facebook to seemingly transfer data between the U.S. and European Union but **was struck down by** the EU high court in October.

Officials from both sides of the Atlantic **announced in February** that they had reached a revamped pact, known as the Privacy Shield, which imposes stronger obligations on U.S. companies to protect the personal data of Europeans and requires more robust monitoring and enforcement by regulators, and the deal was formally approved on July 12.

But despite the deal gaining the backing of EU and U.S. officials, privacy advocates have vowed to mount a challenge to the deal similar to the one that led to the demise of the popular safe harbor mechanism. That case is widely expected to be filed in the coming weeks, as U.S. companies gear up to begin certifying their compliance starting on Aug. 1, and attorneys say they and their clients will be watching any dispute closely.

"We should watch for a new court challenge to the Privacy Shield and, starting August 1, 2016, we should see how many companies have filed for certification to take advantage of the new data transfer regime," Vernick said. "It may be that many U.S. companies decide that the new regulatory framework is too new and unstable to take the risk, opting instead to stick with the binding corporate rules and model contracts they negotiated in the intervening period."

Taking On TCPA

With litigation under the Telephone Consumer Protection Act continuing to hammer businesses in a range of sectors, a pair of cases currently being considered by the D.C. Circuit are likely to go a long way in dictating the future ebb and flow of such litigation, according to attorneys.

In one matter, petitioners led by ACA International are challenging an Federal Communications Commission order **from June 2015** that expands the scope of the TCPA in an effort to crack down on robocalls from telemarketers. Businesses have argued that the order will cause an uptick in TCPA litigation, while the FCC has countered that it had given adequate considerations to the objections the petitioners raised but exercised its discretion in handing down the June rule.

"This appeal has the potential to impact almost every TCPA call and text case pending right now where issues like the use of an [automatic telephone dialing systems], revocation of consent and/or recycled numbers are likely to play a role," Almeida said.

The second dispute, which was filed before the ACA International case, concerns the FCC's decisions to require opt-out notices on faxes, even if they are solicited, and to waive retroactive enforcement of that regulation. In a **final brief filed in March**, the commission countered businesses' challenge to its authority to regulate solicited faxes by arguing that the rule aligned with the goals of the TCPA and contended that consumers' contention that the regulator should not be allowed to waive enforcement were also unfounded.

"Should the D.C. Circuit invalidate the solicited fax rule, it would likely spell the end for TCPA fax class actions where consent could be an issue," Almeida said.

The cases are ACA International v. Federal Communications Commission et al., case number 15-1211, and Bais Yaakov of Spring Valley et al. v. Federal Communications Commission et al., case number 14-1234, in the U.S. Court of Appeals for the District of Columbia Circuit.

Practice Areas

Class Action Defense

Telephone Consumer Protection Act (TCPA)