Privacy Cases To Watch In 2017

By **Allison Grande**

Law360, New York (January 2, 2017, 1:03 PM EST) -- Privacy attorneys are expecting the upcoming year to bring payoffs involving a host of long-simmering legal questions, including what exactly plaintiffs need to allege to prop up statutory privacy claims, how far the Federal Trade Commission can go in policing data security and whether the newly inked trans-Atlantic Privacy Shield data transfer mechanism is indeed a stronger mechanism than its predecessor. Fueled by the movement of many established disputes to appellate courts, the privacy litigation landscape promises to be anything but boring in the coming months, with the ongoing and consuming task of tracking how courts continue to interpret the U.S. Supreme Court's landmark Spokeo ruling on the top of most attorneys' lists of cases to watch. "On privacy litigation generally, we should be watching whether class action cases continue to grow, and become a replacement of sorts for the possibility of less government enforcement" under the incoming Trump administration, said Wiley Rein LLP privacy practice chair Kirk Nahra. Here are some of the top cases that privacy attorneys will be keeping on their radar in 2017. **Spokeo Fallout** The biggest decision of 2016 is certain to continue to loom large in 2017, with attorneys saying that the importance of how both district and appellate courts apply the Supreme Court's landmark May decision in Spokeo v. Robins — which held that plaintiffs must allege a concrete injury and cannot rely on mere statutory violations to establish Article III standing — will only keep increasing as the months tick by. "We expect the Supreme Court's decision in Spokeo to remain a popular subject of intense litigation in 2017 across all Consumer Protection Act class actions, with major consequences across the landscape of these types of claims," Troutman Sanders LLP partner David Anthony said. In the months since the high court handed down its decision, lower courts have **already begun to issue** conflicting decisions in cases with similar fact patterns under statutes such as the Fair Credit Reporting Act, the Telephone Consumer Protection Act and the Fair and Accurate Credit Transactions Act, and attorneys expect this trend to only grow stronger in 2017. "With Spokeo, the jury's still out as far as where things are going to go because both sides have declared victory in that case and there's been some conflicting results in different circuits about whether there was really harm," said Bradley S. Shear, managing partner of Shear Law LLC. "It's likely going to take another year or two to figure out what the ruling really means." One dispute that will be of particular interest — and could help feed into a split at the appellate level in the coming year — 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. The Ninth Circuit **heard oral arguments** in the remanded case on Dec. 13, and is expected to decide in the coming months whether to uphold its prior decision finding that Robins had alleged a sufficient injury to continue with his claims under the FCRA. While the Spokeo dispute involves a statutory privacy violation, attorneys say they will also be keeping close tabs on how courts apply the concrete injury requirement

established by the high court to cases involving data breaches, which often involve situations where personal data is compromised but not necessarily misused. "The brick wall of defense wins in class action cases involving breaches is still pretty strong, but there are increasing cracks in the wall," Nahra noted. "At some point, the wall may collapse." Spokeo is represented by Andrew J. Pincus, Donald M. Falk, John Nadolenco, Archis A. Parasharami, Stephen C.N. Lilley and Daniel E. Jones of Mayer Brown LLP. Robins is represented by Jay Edelson, Rafey S. Balabanian, Ryan Andrews, Roger Perlstadt and J. Aaron Lawson of Edelson PC, and William Consovoy and Patrick Strawbridge of Consovoy McCarthy Park PLLC. The case is Thomas Robins v. Spokeo Inc., case number 11-56843, in the U.S. Court of Appeals for the Ninth Circuit. **LabMD, FTC Go to Eleventh Circuit** The yearslong data security battle between the FTC and LabMD finally reached the Eleventh Circuit in 2016, and attorneys say that how that dispute ultimately plays out could have widespread ramifications for how the commission wields its unfairness authority under Section 5 of the FTC Act going forward. "The LabMD case is going to be one of the most important things happening in the next year," Foley Hoag LLP attorney Christopher Hart said. "If the appellate court rules against the FTC, its power would be curtailed in such a way that's going to have pretty lasting effects and could give the FTC some heartburn." The medical testing laboratory lodged its appeal shortly after the three acting FTC commissioners released **an opinion in July** that overturned their own administrative law judge in concluding that the lab's failure to employ "basic" security precautions led to an unauthorized disclosure of sensitive medical data that caused "substantial" harm to consumers in violation of the unfairness prong of Section 5. The appellate court offered a glimpse into its take on the ruling in November, when it **granted the lab's bid** to stay enforcement of the order after concluding that the dispute presented substantial legal questions and that now-defunct LabMD would be irreparably harmed absent a stay. "The Eleventh Circuit dealt the FTC a blow in holding in its ruling on the motion to stay that the commission had to demonstrate a higher level of harm in order to bring an unfairness case," Hogan Lovells senior associate Bret S. Cohen said. "The case is now back before the parties to argue whether or not the FTC has met the relevant standard of harm, but it's now a much higher bar for the FTC to meet." If LabMD is successful in making its argument that the FTC has fallen short of meeting its burden of proving that consumers were harmed by the purported data leak, that could significantly upend the regulator's increasingly aggressive privacy enforcement agenda, attorneys say. "The FTC is trying to use LabMD as a vehicle for dramatically expanding its enforcement authority, not just in the data security context but in the broader consumer protection context, so depending on how the Eleventh Circuit approaches the case, it could determine whether or not the FTC is successful in accomplishing that expansion of its authority based on an ill interpretation of Section 5 that had never been announced before the commissioner's decision that came out earlier this year," Ropes & Gray LLP privacy and data security group co-chair Doug Meal, who is representing LabMD in the appeal pro bono, said in a recent interview. A LabMD victory would also "set up a split with the Third Circuit, which decided in August 2015 that Section 5 provided the FTC with jurisdiction in data security suits in FTC v. Wyndham Worldwide Corp.," Hughes Hubbard & Reed LLP data privacy

and cybersecurity group co-heads Dennis Klein and Seth Rothman said in a joint email. 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. **EU-U.S. Privacy Shield Under Fire** When EU and U.S. officials got together in February to announce that they had hammered out a deal, dubbed the Privacy Shield, that would allow multinationals to legally transfer personal data across the Atlantic, experts predicted that the pact would soon be the subject of court challenges similar to the one that led to the demise of the longstanding safe harbor mechanism that Privacy Shield replaced. That forecast quickly panned out, with Digital Rights Ireland and French civil liberties campaign group La Quadrature du Net lodging separate complaints in the European Court of Justice this past fall challenging the adequacy of the new data transfer mechanism. "The privacy shield is an important and constructive tool for the transfer of data across borders and will be depended on by a lot of businesses, so the business community is likely to be hoping that it will be upheld," Sheppard Mullin Richter & Hampton LLP partner David Almeida said. In weighing in on Privacy Shield's predecessor, the EU high court ruled in October 2015 that the safe harbor deal hurt EU citizens' privacy rights because it gave U.S. intelligence officials unfettered access to their personal data. With uncertainty swirling how the incoming Trump administration will address national security issues, attorneys say that a similar holding on Privacy Shield is not out of the question. "The Privacy Shield is premised on having certain protections in place, so depending on what the future administration does with regards to bulk data collection and other intelligence-gathering issues, that may affect the legality of Privacy Shield because if the EU court sees a drastic change in current policy, it might say that maybe this transfer mechanism should be invalidated again," Shear said. Attorneys noted that they will also be watching a **separate challenge** pending before the Irish high court over the legality of standard contractual clauses, which is another popular trans-Atlantic data transfer mechanism. "With Privacy Shield itself under fire from European regulators, the ... challenge to the sufficiency of model contractual clauses is cause for concern among many businesses who rely on international data transfers," Sheppard Mullin privacy and security practice co-chair Laura Jehl said. **Microsoft Warrant Fights** Microsoft spent the past year pressing a pair of challenges to government data requests, and attorneys predict that both will continue to warrant attention in 2017. In one of the fights, the U.S. Department of Justice **has asked the Second Circuit** to rehear a July ruling that the government can't use search warrants to access consumer data stored overseas by service providers such as Microsoft. "The Second Circuit's decision in July was not widely expected in that the court ruled against the government's arguments about the scope of its investigatory powers abroad, so it will be interesting to watch next year what happens with that appeal, what the government's strategy will be and ultimately whether the Supreme Court gets involved," Cohen said, adding that the dispute will also be closely watched by outside the U.S. given that "the ability of the U.S. government to access data that is merely accessible to a cloud-based service provider is a key sticking point in trans-

Atlantic data flows." The other pending matter, which Microsoft just **lodged in April** and has already received a swell of amicus support, challenges the legality of gag orders issued under the Electronic Communications Privacy Act that force service providers to keep their customers in the dark about law enforcement demands to access user data. "It's very important that the U.S. show the world that it can properly balance privacy and lawful access," Shear said. "ECPA is 30 years old and being used in ways that were not anticipated when the law was put in place, so it's important to ensure that that proper balance is struck both by courts and through potential legislative updates." The cases are 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 and In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., case number 14-2985, in the U.S. Court of Appeals for the Second Circuit. **TCPA Challenges** The D.C. Circuit is poised to issue a pair of rulings in 2017 that attorneys say could have a dramatic impact on the ebb and flow of Telephone Consumer Protection Act litigation that has been hitting companies hard in recent years. In one dispute, on which the appellate court **held oral arguments** in October, petitioners led by ACA International are challenging a 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 — which broadened the definition of "autodialer" and set strict conditions on calling reassigned numbers, among other things — went too far, while the FCC has countered that its order was carefully considered and well-reasoned. "Based on the panel's questioning at oral argument, there is a genuine possibility that the D.C. Circuit may limit the scope of the FCC's order, which could fundamentally alter the viability of plaintiffs' TCPA claims throughout the country, or at least certain fundamental issues in TCPA cases," Anthony said, adding that numerous courts around the country have already granted stays pending the appellate court's ruling. The other case before the D.C. Circuit 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 oral arguments held in November, a majority of the appellate panel appeared sympathetic to those opposing the decision in characterizing the agency's attempt to regulate solicited faxes as a "power grab." "Almost every fax case we see today involves an allegation concerning the opt-out language, and that allegation really turns on whether it's required on solicited faxes or not," Almeida said. "That's what's created an uptick in fax litigation in recent years, so if the D.C. Circuit revises the solicited fax rule as it seems poised to do, that could drastically limit the number of TCPA fax cases that are filed moving forward." 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. **Biometric Privacy Litigation** In recent years, prominent social media companies including Facebook, Google and Snapchat have been swept up in the rising stream of litigation under the Illinois Biometric Information Privacy Act, which makes it unlawful for a company to collect, capture or otherwise obtain a person's biometric identifiers or information unless it informs the

subject and receives consent in writing. "Companies are using biometrics — including fingerprints, iris scans, voiceprints and facial geometry data — for a growing list of purposes, from authenticating consumer identities prior to online purchases to tracking employees' time on the job," Cooley LLP privacy and data protection practice group chairman Michael Rhodes said. "These cases may provide guidance on plaintiffs' ability to maintain BIPA class actions and the extent to which nationwide online businesses face exposure for BIPA noncompliance." A tanning salon chain recently became **the first company to settle claims** brought under the law, and with pivotal dismissal motions pending in cases involving Facebook and others, 2017 could prove to be a significant year for not only the health of this emerging line of privacy claims, but also the success of efforts to expand the unique restrictions on biometric data use to other states, attorneys say. "The outcome of these cases and how the Illinois law is interpreted by the courts really have the potential to shape the landscape not just from a legal perspective but also a public policy perspective," Shear said.