Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy Cases To Watch In 2016

By **Allison Grande**

Law360, New York (December 24, 2015, 8:37 PM ET) -- The U.S. Supreme Court is set to decide a pair of privacy disputes that are poised to have a lasting impact on the ebb and flow of consumer class action litigation, while lower courts will have their hands full with challenges to data security claims brought by the Federal Trade Commission and a warrant for data stored overseas by Microsoft.

Following a year that produced major decisions that helped to boost plaintiffs' prospects in data breach litigation and shed light on the contours of the FTC's data security authority, 2016 promises to be another marquee year in privacy law, with a duo of looming Supreme Court decisions dealing with standing and settlement offers poised to headline the show.

"The Supreme Court decisions have the potential to change the class action landscape in the United States forever," Locke Lord LLP partner Martin Jaszczuk told Law360. "While the Supreme Court could craft narrow decisions limited to the specific facts of each case, both controversies present the court with a platform to rewrite the way Rule 23 is applied to consumer class actions."

Here, privacy attorneys flag some of the major cases that they will be keeping their eye on in 2016.

Spokeo v. Robins

On the heels of a Nov. 2 oral argument session, the high court justices are expected to issue a decision in the first half of 2016 addressing the hotly debated question of whether consumers can sue companies such as Spokeo Inc. for technical violations of the Fair Credit Reporting Act and similar statutes without alleging an actual injury.

"The Spokeo decision may impact the overall injury standard for consumer class actions, which has been built through a strong wall of precedent holding that consumers need to assert an actual harm before a case can proceed," Wiley Rein LLP privacy practice chair Kirk Nahra said. "If this standard changes in any material way, it could open the floodgates for new privacy and security breach litigation."

The issue comes to the justices in the context of a dispute between Spokeo and Thomas Robins, a consumer who sued the self-proclaimed people search engine for allegedly violating the FCRA by falsely reporting that he was wealthy and had a graduate degree when in fact he was struggling to find work.

The Ninth Circuit in 2014 sided with Robins in reviving the suit on the grounds that Spokeo's alleged violation of the FCRA amounted to an injury. But while the instant dispute is limited to claims brought

under the credit-reporting statute, the justices' decision is poised to have an impact on future allegations under a slew of other privacy laws that provide for hefty automatic statutory penalties, including the Telephone Consumer Protection Act and the Video Privacy Protection Act, according to attorneys.

"Class action plaintiffs have largely been unable to satisfy a showing of damage or common injury, which has led to a lot of class actions not proceeding," White & Case LLP partner Daren Orzechowski said. "People are going to be watching the Spokeo case to figure out whether or not class actions lawsuits are now going to become a serious threat to Internet-based businesses."

Spokeo is represented by John Nadolenco, Andrew J. Pincus, Archis A. Parasharami, Stephen Lilley and Donald M. Falk of Mayer Brown LLP.

Robins is represented by Jay Edelson, Rafey S. Balabanian, Ryan Andrews and Roger Perlstadt of Edelson PC and Will Consovoy, J. Michael Connolly, Michael Park and Patrick Strawbridge of Consovoy McCarthy Park PLLC.

The case is Spokeo Inc. v. Thomas Robins et al., case number 13-1339, in the Supreme Court of the United States.

Campbell-Ewald v. Gomez

The Supreme Court will likely make another splash in the privacy pool when it releases its highly anticipated decision in early 2016 on the issue of whether defendants can strategically offer individual plaintiffs the relief necessary to make them whole at the outset of the litigation in order to avoid a long court battle or a potential multimillion-dollar class action settlement down the line.

The justices considered the settlement offer quandary during oral arguments in October in the context of the TCPA, which longtime government contractor Campbell-Ewald Co. is accused of violating by sending naval recruitment messages to about 100,000 people in 2006 through a subcontractor.

"A holding in favor of Campbell-Ewald could drastically limit the types of class actions plaintiffs can pursue in federal courts," said Jaszczuk, who heads Locke Lord's TCPA class action litigation section.

However, a ruling in favor of plaintiff Jose Gomez — who was offered $1,503 by Campbell-Ewald for each unsolicited text message he allegedly received, which represented more than three times the statutory amount of $500 per violation — would help to further swell already padded class action dockets, attorneys say.

"Given the unlimited liability that companies face under statutes such as the TCPA, it makes a big difference if businesses can pick off plaintiffs," said Scott Vernick, Fox Rothschild LLP's privacy and data security practice leader.

Campbell-Ewald is represented by Laura A. Wytsma and Meredith J. Siller of Loeb & Loeb LLP and Gregory G. Garre and Nicole Ries Fox of Latham & Watkins LLP.

Gomez is represented by Suzanne L. Havens Beckman and David C. Parisi of Parisi & Havens LLP, Michael J. McMorrow of McMorrow Law PC, Myles McGuire and Evan M. Meyers of McGuire Law PC and Scott L. Nelson, Allison M. Zieve and Adina H. Rosenbaum of Public Citizen's Litigation Group and Jonathan F.

Mitchell of Stanford University Law School.

The case is Campbell-Ewald Co. v. Gomez, case number 14-857, in the Supreme Court of the United States.

FTC v. LabMD

The FTC in November took the anticipated step of asking its own commissioners to review a surprising ruling by an administrative law judge that threw out the agency's data breach suit against medical testing company LabMD Inc., setting the stage for continued fireworks in 2016 over the scope of the agency's data security authority.

"What drove the decision was that the administrative law judge found that the commission had failed to show that there had been actual harm to consumers," Vernick said. "If that standard is upheld, that will likely influence and information what kind of actions the FTC bring in the future."

In stark contrast to the boost that the FTC received in August when the Third Circuit ruled that it had the authority to police private companies' data security under the unfairness prong of Section 5 of the FTC Act, the administrative law judge's ruling dealt a significant blow to the commission by endorsing a narrow view of the "harm" required by the statute.

Moving the commission's pleading burden closer to that required by private plaintiffs in class action litigation over data breaches and other alleged privacy violations, the administrative law judge in nixing the suit concluded that hypothetical or theoretical harm caused by the lab's conduct was insufficient to maintain the commission's allegations.

"This case was the first time a company successfully challenged an FTC complaint involving unreasonable information security under Section 5 unfairness authority," said Mauricio Paez, who heads Jones Day's privacy and cybersecurity practice. "If this reasoning holds up — and the FTC's argument that liability can be imposed based on solely on the risk of a data breach is ultimately rejected on appeal — the FTC's authority to bring data security actions in the future could be undercut."

The FTC filed its opening brief in the appeal on Dec. 23, and LabMD is expected to file its reply brief on Feb. 18.

LabMD is represented by Reed D. Rubinstein, William A. Sherman II and Sunni Harris of Dinsmore & Shohl LLP and Daniel Epstein and Patrick Massari of Cause of Action.

The FTC is represented by Alain Sheer, Laura Riposo VanDruff, Megan Cox, Ryan Mehm, John Krebs and Jarad Brown.

The case is In the Matter of LabMD Inc., docket number 9357, before the FTC's Office of the Administrative Law Judges.

Microsoft's Overseas Data Warrant Dispute

The Second Circuit is expected to soon hand down its ruling on whether the U.S. government can use warrants to access consumer data stored overseas by service providers such as Microsoft Corp., a decision that is likely to have sweeping international ramifications.

"This is a very big issue because U.S.-based service providers are facing questions from those both inside the U.S. and internationally about what whether the government will have access to data stored with it," Orzechowski said.

The parties' dispute centers on whether the government can use warrants issued under the Stored Communications Act to reach data stored outside the U.S.

Microsoft and its supporters — which include other major service providers such as Verizon Communications Inc., AT&T Inc. and Apple Inc. — have argued that U.S. statutes could not apply extraterritorially unless Congress explicitly said so, while the government has countered that search warrants issued under the SCA allow the government to access data stored anywhere.

A New York federal judge sided with the government in a July 2014 ruling that the location of the data mattered less than who controlled it, and Microsoft immediately appealed to the Second Circuit, which held oral arguments on Sept. 9.

While waiting for the ruling, Microsoft announced in November that it is setting up a new cloud service in Germany where user data is controlled by a "data trustee" operating under German law in order to skirt the control issue, a move that could spark another court fight in the coming months.

“This is a case to watch on two fronts: the issue that’s currently before the Second Circuit, as well as the one that has yet to come up yet as to whether the new Microsoft offering sufficiently removes possession, custody and control from U.S. companies,” Orzechowski said.

Microsoft is represented by E. Joshua Rosenkranz, Robert M. Loeb, Brian P. Goldman and Susannah Landes Weaver of Orrick Herrington & Sutcliffe LLP, James M. Garland and Alexander A. Berengaut of Covington & Burling LLP, Guy Petrillo of Petrillo Klein & Boxer LLP, and in-house attorneys Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer and Nathaniel Jones.

The government is represented by the U.S. Attorney for the Southern District of New York Preet Bharara and Assistant U.S. Attorneys Justin Anderson and Serrin Turner.

The case is 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 Order Challenge

A coalition of businesses and organizations including the U.S. Chamber of Commerce, collection company trade group ACA International, Sirius XM Radio Inc. and Rite Aid Corp in November took to the D.C. Circuit a contentious order issued by the FCC that expanded the scope of the TCPA.

In their brief, the groups urged the appellate court to overturn the June order, which has been widely panned by businesses because it backs a broad definition of automatic telephone dialing system, its slim liability shield for calling reassigned numbers and the wide latitude it gives consumers to revoke consent.

“The appeal of the FCC’s order could mark a sea change in TCPA litigation across the country,” Jaszczuk said. “If the appellate court were to call into question the FCC’ ultra-broad ATDS definition, or the FCC’s

unrealistic characterization of the term ‘called party,’ the TCPA class action litigation landscape could change overnight.”

Some of the nation's largest retail, technology, financial and utility industry groups threw their support behind the petitioners in a slew of amicus brief lodged with the circuit court in December, highlighting the sweeping nature of TCPA liability, which has exploded in recent years due to unclear statutory definitions and the lure of uncapped statutory damages of between $500 and $1,500 per violation.

"This is a very hotly contested space right now, and we should only expect more movement on this front in the new year,” BakerHostetler partner Tanya Forsheit said.

The FCC's reply brief is due Jan. 15 and final briefs are due Feb. 24, according to a court order. Oral arguments have not yet been scheduled.

The petitioners are represented by Dykema Gossett PLLC, Gibson Dunn, Wilson Sonsini Goodrich & Rosati PC, Jones Day, Squire Patton Boggs LLP, Covington & Burling LLP, and Sheppard Mullin Richter & Hampton LLP, among others.

The government is represented by Scott Matthew Noveck, Richard Kiser Welch and Jacob M. Lewis of the FTC, and Steven Jeffrey Mintz and Kristen Ceara Limarzi of the U.S. Department of Justice.

The lead 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.

Data Breach Fallout

Companies ranging from extramarital dating website Ashley Madison to electronic learning toymaker VTech became the latest to uncover major data breaches in 2015, adding to a crush of disclosures that has resulted in a wave of litigation filed by consumers, banks and shareholders.

Aside from the landmark decision by the Seventh Circuit to revive a data breach class action against Neiman Marcus in July, consumers had little luck in 2015 in demonstrating the harm necessary to overcome traditional standing hurdles, a trend that attorneys will continue to closely monitor in the new year.

"We'll be watching to see whether plaintiffs will be able to get past standing, and if a failure to secure data without consequences is enough for a suit to continue,” Crowell & Moring LLP privacy and cybersecurity group co-chair Robin Campbell said.

Financial institutions fared markedly better in the past year. In December, a class of banks reached a $39 million deal with Target Corp. that allowed them to recover more than if they had gone through programs run by Visa Inc. and MasterCard Inc., and attorneys will be watching similar suits — including contentious litigation over the Home Depot Inc. breach — to see whether financial institutions will continue to have success in recovering their breach-related losses.

"The Target settlement was noteworthy, and it will be interesting to see if it was just an anomaly or the start of a larger trend,” Paul Hastings LLP privacy and cybersecurity practice co-chair Behnam Dayanim said.

The shareholder derivative suits filed against Target and Home Depot will also bear keeping an eye on in 2016, especially in light of the October 2014 dismissal of a such a suit against Wyndham Worldwide Corp. on the grounds that there was no proof that the board's failure to investigate and remedy the hotel's security protocols was a sign of bad faith.

“These cases are anticipated to provide further guidance about what is required to show liability regarding the duty of a director to oversee risk, including cybersecurity risk, and shape the actions that directors take in fulfilling their oversight duty,” Dorsey & Whitney LLP partner Melissa Krasnow said.

--Editing by Katherine Rautenberg and Patricia K. Cole.