

Privacy Cases To Watch In 2015

By Allison Grande

Law360, New York (January 02, 2015, 3:26 PM ET) -- A pair of appellate challenges to the Federal Trade Commission's ability to regulate data security will captivate privacy attorneys in 2015, as will a dispute before the U.S. Supreme Court over the limits of standing in certain privacy cases and a heated Second Circuit fight over a search warrant for user data stored by Microsoft Corp. overseas.

The continued fallout from the massive data breach that hit Target Corp. at the end of 2013 as well as a case in Illinois that is likely to test the bounds of corporate liability for alleged telemarketing violations will also continue to grab headlines, according to attorneys.

Here are some of the cases that privacy attorneys will be watching closely in 2015.

FTC's Data Security Authority

The FTC has so far been able to brush back challenges from Wyndham Worldwide Corp. and LabMD Inc. over the scope of its authority to regulate data security under Section 5 of the FTC Act. But the Third and Eleventh circuits are poised to weigh in on the disputes in 2015, and their holdings are likely to have a significant impact on the future course of data security regulation in the U.S., attorneys say.

"This litigation has the potential to be a game changer for the FTC's enforcement authority," McDermott Will & Emery LLP partner Anthony Bongiorno said.

Both Wyndham and LabMD argue that the unfairness prong of Section 5 doesn't permit the FTC to regulate data security and that the agency has failed to provide fair notice of what constitutes reasonable data security standards.

A New Jersey federal judge snubbed those arguments in April, declining to dismiss the regulator's suit against Wyndham. The judge did grant the hotel chain's motion for interlocutory review in July, however. Wyndham filed its opening brief in the Third Circuit that month, and oral arguments are expected to be held in early 2015.

"If the court of appeals affirms the district court's order, it would not be a surprise for the FTC to bring enforcement actions against all types of 'unfair' data practices," said Kaufman Dolowich & Voluck technology practices group vice chair Hsiao (Mark) Mao.

But the appeals court could instead decide that the commission has a duty to publish regulations on what constitutes "reasonable" data security or that Congress hadn't intended for it to regulate data security at all. In that case, the commission's active data security enforcement — which has produced more than 50 cases in the past decade — will likely grind to a halt, attorneys say.

"A loss for the FTC would represent a seismic change in the data security landscape," Bongiorno said.

The LabMD case, which is pending before an administrative law judge as well as the Eleventh Circuit, could have an even greater impact. It casts doubt not only on the regulator's general data security authority but also on its ability to wield that authority against companies like LabMD that are already covered by established federal privacy regimes such as the Health Insurance Portability and Accountability Act.

"Companies like LabMD are already subject to the jurisdiction of the Office of Civil Rights under the HIPAA rules, so if the FTC wins, that means that companies in the health care field will have a second agency to worry about," Wiley Rein LLP privacy practice chair Kirk Nahra said.

After LabMD failed on two occasions to convince federal courts to hear its challenge while the administrative proceeding was still pending, the Eleventh Circuit in August agreed to take up the case, and it heard oral arguments Dec. 9.

Attorneys are also expecting an ALJ to issue a decision on the merits of the case in 2015. A trial in the administrative proceeding began in May but was quickly put on hold while a key witness sought immunity for his testimony, a process that is now close to completion.

Wyndham is represented by Michael W. McConnell of Stanford Law School; Eugene F. Assaf, Christopher Landau, Susan M. Davies and K. Winn Allen of Kirkland & Ellis LLP; Douglas H. Meal and David T. Cohen of Ropes & Gray LLP; and Jennifer A. Hradil and Justin T. Quinn of Gibbons PC.

LabMD is represented by William A. Sherman II, Reed Rubinstein and Sunni Harris of Dinsmore & Shohl LLP; Ronald L. Raider, Burleigh L. Singleton and William D. Meyer of Kilpatrick Townsend & Stockton LLP; and Hallee Morgan, Kent Huntington, Daniel Epstein, Patrick Massari and Prashant K. Khetan of Cause of Action.

The cases are *FTC v. Wyndham Worldwide Corp. et al.*, case number 14-3514, in the U.S. Court of Appeals for the Third Circuit; ; *LabMD Inc. v. Federal Trade Commission*, case number 14-12144, in the U.S. Court of Appeals for the Eleventh Circuit; and *In the Matter of LabMD Inc.*, docket number 9357, before the Federal Trade Commission Office of the Administrative Law Judges.

Spokeo v. Robins

The Supreme Court is weighing whether to take up Spokeo Inc.'s challenge to a Fair Credit Reporting Act suit accusing it of publishing false information about a Virginia man. If allowed to proceed, the case could have broad implications for data privacy class actions, attorneys say.

"If the Supreme Court decides to take the case, we may hear a more definitive word on the level of harm that someone has to suffer to be able to qualify for Article III standing," said Bradley Arant Boult Cummings LLP partner John Goodman.

In a February ruling, the Ninth Circuit revived plaintiff Thomas Robins' suit on the grounds that the alleged violations of his statutory rights under the FCRA sufficiently satisfied Article III's injury-in-fact requirement

for standing. But Spokeo has countered that there is a circuit split on the issue and that Robins must show actual harm rather than a mere fear that potential employers may rely on the allegedly inaccurate data.

Spokeo's challenge has drawn support from several high-profile backers, including Facebook Inc., eBay Inc., Google Inc. and Yahoo Inc., which filed an amicus curiae brief in June arguing that letting the Ninth Circuit's ruling stand would open the floodgates for a barrage of "no injury" class actions under the Telephone Consumer Protection Act, the Video Privacy Protection Act and similar statutes.

The Supreme Court — which in its landmark 2013 ruling in *Clapper v. Amnesty International* held that the plaintiffs need to prove they have suffered actual harm or a certainly impending injury to satisfy Article III — in October asked the solicitor general to weigh in on Spokeo's challenge, and a decision on whether the court will take up the case is expected in early 2015.

"There are a lot of instances where individuals claim that a statutory right to privacy has been violated without suffering any monetary damages, so this is a very important issue," JAMS neutral Judge James Ware said.

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 Deepak Gupta of Gupta Beck PLLC and Steven Woodrow, Jay Edelson and Rafey S. Balabanian of Edelson PC.

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

Microsoft's Overseas Data Warrant Dispute

The Second Circuit is poised to hear a first-of-its-kind fight over a search warrant issued by a New York magistrate judge that requires Microsoft to produce the contents of an email account stored on a Microsoft server located in Ireland.

"No matter how it's decided, this case will have earth-shaking consequences for both U.S. law enforcement and U.S. tech companies trying to compete overseas," Steptoe & Johnson LLP partner Jason Weinstein 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. A New York federal judge in July adopted the magistrate judge's holding that the SCA does not explicitly bar extraterritorial access to user data, and Microsoft immediately appealed to the Second Circuit.

In its Dec. 8 opening brief, Microsoft argued that Congress had never intended for the SCA to reach overseas and that allowing the lower court's ruling to stand would set a dangerous precedent that would open the door for other countries to try to circumvent U.S. privacy laws to obtain data stored in the country.

The company's position was backed by Verizon Communications Inc., the U.S. Chamber of Commerce and dozens of other technology companies, industry groups, privacy advocates and legal scholars in 10 separate amicus briefs filed with the Second Circuit on Dec. 15, as well as by the government of Ireland and a European Parliament member in separate briefs filed later in the month.

"If the U.S. loses, it will mean that the long arm of the law in the U.S. doesn't reach quite as far as the [government] thought, at least not without help from foreign partners," Weinstein said. "But if the U.S. wins, then it will make it even harder for U.S. companies in an increasingly global cloud computing market."

Microsoft is represented by E. Joshua Rosenkranz, Robert M. Loeb and Brian P. Goldman 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.

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.

In re: Target Corp. Customer Data Security Breach Litigation

While 2014 produced several high-profile data breaches that spurred a rash of class action litigation, the incident that marked the beginning of the data breach barrage — an intrusion announced by Target in December 2013 that compromised payment card and personal data for 110 million customers — has wound its way the furthest through the courts and promises to yield noteworthy results in 2015, attorneys say.

On Dec. 2, a Minnesota federal judge handed down the first significant decision in the litigation. The judge rejected most of Target's bid to dismiss sprawling litigation that has been brought on behalf of banks, credit unions and other financial institutions on the grounds that the retailer owed them a duty to protect customer credit and debit card information from hackers.

"The ramifications of the decision on the business community could be huge," Shook Hardy & Bacon LLP data security and privacy group co-chair Al Saikali said. "It could help pave the way for banks to pursue merchants in court for costs suffered as a result of a merchant's data breach."

The district court dealt another blow to Target on Dec. 18, when it left largely intact claims filed against the retailer by a putative class of consumers.

Moving into 2015, the litigation promises to continue to produce important determinations regarding what responsibility breached entities owe to consumers and other stakeholders who claim they have been damaged by a security failing.

"It will be interesting to see how this case proceeds at class certification, because it's difficult to imagine how plaintiffs are going to go about proving their injuries in a common way," Goodman said.

The financial institutions are represented by Zimmerman Reed PLLP, Lockridge Grindal Nauen PLLP, Chestnut Cambronne PA, Reinhardt Wendorf & Blanchfield, Barrett Law Group PA and others.

The consumer plaintiffs are represented by Vincent J. Esades and David Woodward of Heins Mills & Olson PLC, E. Michelle Drake of Nichols Kaster PLLP, John A. Yanchunis of Morgan & Morgan Complex Litigation Group PA, Ariana J. Tadler of Milberg LLP, Norman E. Siegel of Stueve Siegel Hanson LLP and Daniel C. Girard of Girard Gibbs LLP.

Target is represented by Wendy J. Wildung and Michael A. Ponto of Faegre Baker Daniels LLP and Harold J. McElhinny, Jack W. Londen, Michael J. Agoglia, Rebekah Kaufman and David F. McDowell of Morrison &

Foerster LLP.

The case is In re: Target Corp. Customer Data Security Breach Litigation, case number 0:14-md-02522, in the U.S. District Court for the District of Minnesota.

U.S. v. Dish

On Dec. 11, an Illinois federal judge found Dish Network LLC liable for having a hand in tens of millions of unwanted telemarketing sales calls, setting up a trial in which the federal government and several states could seek penalties exceeding \$1 billion for alleged violations of the Telephone Consumer Protection Act and related statutes.

"As plaintiffs often do in TCPA class actions, the plaintiff governmental entities had argued that Dish could be liable for many billions of dollars of damages," said Martin Jaszczuk, Locke Lord LLP's TCPA class action litigation section head. "The question now is where the runaway train will stop."

In recent years, litigation under the TCPA has exploded, in large part due to the allure of uncapped statutory damages of between \$500 and \$1,500 per violation. The risk of large damage awards has prompted a rash of settlements in recent months, including a \$32 million settlement doled out by Bank of America Corp. and a proposed \$75.5 million pact to resolve a class action against Capital One Financial Corp. and three collection agencies.

"There have been huge settlements this year in cases filed under the TCPA, which gives plaintiffs attorneys an incentive to continue to file these cases," Dorsey & Whitney LLP partner Melissa Krasnow said.

The case against Dish Network has the potential to add another lofty recovery to plaintiffs' recent fortunes. In his 238-page ruling last month, the judge found Dish liable for more than 57 million calls made by the company and its proxies, including more than 6 million calls to people who had placed their numbers on the national Do Not Call registry, which could theoretically put the company on the hook for more than \$700 billion in statutory damages.

"The Dish Network case should shed some light on whether plaintiffs ... are truly willing to seek and whether courts are willing to award — and uphold on appeal— outlandish damages for what are simple statutory violations," Jaszczuk said. "In 2015 the district court hearing this case, and potentially the Seventh Circuit and perhaps the U.S. Supreme Court, will have the opportunity to set things right and protect hardworking American businesses from annihilating damages that serve no purpose."

Dish is represented by Henry T. Kelly, Joseph A. Boyle and Lauri A. Mazzuchetti of Kelley Drye & Warren LLP.

The case is U.S. et al. v. Dish Network LLC, case number 3:09-cv-03073, in the U.S. District Court for the Central District of Illinois.

--Editing by Kat Laskowski and Edrienne Su.