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

Top Privacy Cases of 2016: Midyear Report

By **Allison Grande**

Law360, New York (July 1, 2016, 12:12 PM ET) -- The U.S. Supreme Court made a big splash this year establishing a murky threshold for standing that has already been widely cited by both sides of the bar, while consumers snagged significant victories in disputes over their ability to sustain putative class actions over a data breach at P.F. Chang's and Facebook's facial recognition technology.

Here, Law360 takes a look back at some of the most significant privacy decisions from an active and memorable start to the year.

The Blockbuster

After months of buildup, a shorthanded Supreme Court in May handed down its hotly-anticipated decision in Spokeo v. Robins, a case that posed the question of whether a mere statutory violation was enough to satisfy Article III's injury-in fact requirement for standing.

In its 6-2 decision, which was authored by Justice Samuel Alito, the justices ruled 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.

"The case that has potentially the most far-reaching implications for privacy and data security class actions is the Spokeo decision," Snell & Wilmer LLP partner James Melendres said. "The takeaway point is that technical violations of statutory rights alone is not going to be sufficient to satisfy standing in class actions, and that reasoning is going to have significant consequences.

However, exactly what those consequences will be is a question that is still very much up in the air. While the justices did attempt to set out some parameters, they did not undergo the task of applying them to the specific dispute in front of the court, but instead took the rare step of sending the dispute back to the Ninth Circuit to consider whether Robins had pled harm that was particularized and concrete.

"The bottom line is that what the Supreme Court was supposed to decide, it didn't," Hughes Hubbard & Reed LLP data privacy and cybersecurity group co-head Seth Rothman said. "So we ended up not getting a hard answer. What we got was some guidance."

The uncertainty has resulted in the strange phenomenon of both plaintiffs and defense attorneys flooding the lower courts with briefs in pending cases **asserting that the ruling** supports their arguments

to either allow the case to continue or to kick it out of court.

Plaintiffs attorney Ryan Andrews of Edelson PC — who represented Robins before the high court and is continuing with the case as it goes before the Ninth Circuit for another look — told Law360 that the outcome of the case has been "consistently misreported," and that the decision was actually a "key victory for privacy" because it recognized that intangible harm can be concrete injury and that Congress has the power to identify these harms and create statutory frameworks under which plaintiffs can sue without alleging any additional harm beyond the one Congress has identified.

"Consumers don't need any more protection than that, and that's what the Supreme Court gave them," Andrews said.

But defense attorneys have countered that the high court's reasoning operates to essentially wipe out claims under a broad range of privacy statutes — including the Fair Credit Reporting Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act — in situations which consumers don't allege any harm beyond a mere statutory violation.

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

The lower courts have slowly begun to deal with the fallout, albeit with mixed results — for example, a New York federal judge **cited Spokeo** as support for her refusal to dismiss a dispute over Hearst's data-selling practices, while a Maryland federal judge **sent back to state court** an action over a data breach at Children's National Health System in light of Spokeo — and attorneys on both sides of the bar expect this confusion to continue well into 2016 and beyond.

"A few rulings have trickled out, and over the next weeks and months we will get better clarity on the metes and bounds on what constitutes a 'particularized,' 'concrete,' 'intangible' injury sufficient to open the gates to federal court," Cooley LLP privacy practice co-chair Michael Rhodes 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 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.

The Seventh Circuit Stands Alone

Several federal and appellate courts have taken on the issue of standing in the data breach litigation context and the majority have concluded that plaintiffs don't have standing if they have yet to suffer any harm as a result of the breach — with the notable exception of the Seventh Circuit.

Following its precedential ruling last year that revived a dispute over a data breach at Neiman Marcus, the Seventh Circuit in April **again reversed** a lower court's ruling that a proposed class of P.F. Chang's

China Bistro Inc. customers suing the restaurant chain over a data breach can't pursue their claims, declaring that the customers have standing to sue for fraud-prevention expenses.

"It's really significant that the court recognized that when there's a data breach and individual information is compromised, that at that point in time there's a sufficient risk of identity theft to bring a suit and you don't have to wait for all the big things to happen," Andrews said. "It's a really strong privacy decision and carves the right path, and I hope other courts recognize it."

However, other courts have been reluctant to back the standard that the Seventh Circuit established in the Neiman Marcus case and strengthened in the latest P.F. Chang's ruling, leading attorneys to believe that a split may form that may entice the Supreme Court to take up the issue of standing again, only this time as it relates to harm stemming from data breaches rather than statutory violations.

"The Neiman Marcus case and the P.F. Chang's decision were trending a different way — and in a way that most people would agree is the minority view from that which has been staked out at the circuit court level — and as courts continue to address this question, I do expect that broader questions about standing in the post-breach class action context will work its way up to the Supreme Court in one of the next high-profile battles," Melendres said.

P.F. Chang's is represented by Thomas A. Lidbury and Jon P. Kardassakis of Lewis Brisbois Bisgaard & Smith LLP.

The customers are represented by Joseph J. Siprut of Siprut PC, Katrina Carroll and Kyle A. Shamberg of Lite DePalma Greenberg LLC, and Richard R. Gordon of Gordon Law Offices Ltd.

The case is John Lewert and Lucas Kosner v. P.F. Chang's China Bistro Inc., case number 14-3700, in the U.S. Court of Appeals for the Seventh Circuit.

Dueling Video Privacy Decisions

Appellate courts in the first half of 2016 also grappled with how to apply outdated statutes such as the Video Privacy Protection Act, which was enacted in 1988, to modern technologies such as tracking cookies and GPS technology.

The First Circuit came out of the gate in April with a ruling that revived a USA Today smartphone app user's putative class action alleging the paper's parent Gannett illegally collected his browsing data to sell to advertisers. In that decision, the panel held that the title of the video viewed along with the device's unique device identifier and GPS coordinates that Gannett sent to Adobe amounted to personally identifiable information covered by the statute.

"The ruling is a game changer, because finally there's a federal appellate court that recognizes what scholars, the government and the tech industry has known for years, and that is that anonymous identifiers aren't anonymous," said Andrews, who represented the plaintiff in the case. "They're like pseudonyms that when given to someone who has enough information can figure out who you are, and the appellate court finally recognized that's true."

However, less than two months later, the Third Circuit weighed in with a decision that struck down video privacy claims being asserted against Google and Viacom on the grounds that the "static digital identifiers" such as internet protocol addresses that Viacom shared with Google could not be considered

personally identifiable information under the statute

"The recent decisions in the VPPA cases addressing what constitutes personally identifiable information will have a profound impact on those companies looking to ascertain whether data collected from a device — rather than associated with a unique user ID — is specific to an individual and must be treated as PII," Troutman Sanders LLP partners Ron Raether, Mark Mao and David Anthony said in an email that they drafted together.

But while the two recent decisions appear to be at odds with one another, the Third Circuit took pains in its ruling to stress that it did not believe that its decision created a split with the looser definition of PII endorsed in the First Circuit because its sister circuit had acknowledged that there was a certain point when linking information becomes too uncertain to trigger liability — creating **a potential opening** for plaintiffs and additional pitfalls that video service providers would be wise to carefully consider.

"These cases represent the need to consider the issue of de-identified or anonymized data more carefully when deciding the legal implications of marketing or other data analytic programs," the Troutman Sanders attorneys said.

The cases are Alexander Yershov v. Gannett Satellite Information Network Inc., case number 15-1719, in the U.S. Court of Appeals for the First Circuit, and In re: Nickelodeon Consumer Privacy Litigation, case number 15-1441, in the U.S. Court of Appeals for the Third Circuit.

Illinois Biometric Privacy Law's Long Reach

Another privacy statute courts are wrestling with is the Illinois Biometric Information Privacy Act, which has been raised in several suits accusing companies including Snapchat Inc. and video game maker Take-Two Interactive Inc. of collecting and retaining face scans and similar biometric data without providing consumers with the proper notice.

The ability of plaintiffs to wield the increasingly popular statute was given a boost in May, when a California federal judge rejected Facebook's argument that the parties' California choice-of-law provision barred the plaintiffs' claims under Illinois law in a dispute over the legality of the site's facial-recognition and tagging features.

"In this case, the judge basically said that despite the choice-of-law provision, Illinois has a fundamental interest in the privacy of its citizens and if it lets Facebook or any other big corporation basically use boilerplate choice-of-law provisions, state laws that protect consumer privacy would be written out of existence," said Andrews, who represented the plaintiff in that case as well. "It's a strong decision recognizing the right of states to protect consumers."

Fenwick & West LLP privacy and information security group co-chair Tyler Newby agreed that, although the ruling was a non-precedential district court opinion, it held significance because it highlights the limits of companies' ability to use choice-of-law provisions in their terms of use to reduce their risk of being held to different states' privacy laws.

"The court's ruling shows that even when a company has an enforceable terms of service with a choice of law provision, a company can still be subject to litigation under conflicting state privacy laws," Newby said.

Facebook is represented by John Nadolenco, Lauren R. Goldman and Archis A. Parasharami of Mayer Brown LLP.

The plaintiffs are represented by Paul Jeffrey Geller, Frank Anthony Richter, Mark Dearman, Shawn A. Williams, Stuart Andrew Davidson and James E Barz of Robbins Geller Rudman & Dowd LLP, Jay Edelson, Rafey S. Balabanian, J. Dominick Larry and Alexander Nguyen of Edelson PC, and Corban S. Rhodes, Joel H. Bernstein and Ross M. Kamhi of Labaton Sucharow LLP.

The case is In re: Facebook Biometric Information Privacy Litigation, case number 3:15-cv-03747, in the U.S. District Court for the Northern District of California.

Privacy Victories For Celebrities

The first half of 2016 saw the culmination of a pair of headline-grabbing trials involving celebrities who claimed that their privacy had been violated through the capture and dissemination of intimate videos of them.

In March, a Florida jury awarded Hulk Hogan a total of $140 million in a verdict against Gawker, its founder and a former editor for the gossip website's publication of a secretly recorded video of the wrestling icon having sex. The award came mere weeks after a separate jury in Nashville handed sportscaster Erin Andrews $55 million after a two-week trial against the hotel where a stalker was able to reserve a room next to Andrews' and secretly film a video that was later released on the Internet.

"When you take these case together, the verdicts seem to demonstrate how the average person is really outraged with how the internet and various actors online are crossing certain boundaries and lines regarding people's privacy, and deciding that this is not how we want to be, that anyone can post anything online without repercussions," said Bradley S. Shear, managing partner of Shear Law LLC.

In both disputes, the financial and reputational fallout for the businesses involved loomed large. Gawker in June was forced into Chapter 11 bankruptcy due to the financial strains of the case and verdict, which is currently on appeal, while in the Erin Andrews case, which was subsequently settled confidentially between the sportscaster and the Nashville Marriott a month after the verdict, the jury found hotel operator Windsor Capital Management 49 percent at fault and the stalker 51 percent to blame, highlighting the importance of companies in the hospitality and related industries to take steps to make sure that their guests and customers feel safe and secure.

"What this says to people who are in this business is that they have a duty of care and a responsibility to make sure that their property and business are safe and if something does happen, in certain situations they may be held liable," Shear said. "At least in the hotel industry, businesses have to make sure that they have not just strong cybersecurity but also physical security policies and that employees understand privacy breaches and the implications of those."

Shear also noted that he viewed the Erin Andrews verdict as a "turning point in privacy harms" given that the jury focused on the emotional harm of having the peephole video on the web indefinitely rather than any financial windfall or struggles she may have had as a result of the video being publicly released.

"Obviously with Spokeo, there seems to be a lot of unsettled issues about what constitutes a privacy harm, but in state court the juries are willing to put themselves in the shoes of someone who had their privacy breached and realize that this stuff is permanent and once someone has uploaded it online it's

nearly impossible to take down," he said. "This may just be the tip of the iceberg and something that employers and companies really have to grapple with."

The cases are Bollea v. Gawker Media LLC et al., case number 12-012447-CI, in the Sixth Judicial Circuit Court of the State of Florida, and Erin Andrews v. Marriott International Inc. et al., case number 11C4831, in the Circuit Court for Davidson County, Tennessee.

— Editing by Ben Guilfoy.
