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

4 Privacy Disputes Ripe For Supreme Court Review

By **Allison Grande**

Law360 (October 11, 2019, 9:53 PM EDT) -- While the U.S. Supreme Court doesn't currently have a blockbuster privacy case on its docket, several hot-button issues are primed to be added to the justices' agenda, such as the standards for certifying massive privacy classes and the harm that has to be shown to prop up data breach claims.

During its past several terms, the court has taken up a range of major privacy issues, including the standing threshold for statutory privacy claims, whether police need warrants to access historical cellphone records and how much input federal agencies should have on how privacy laws are interpreted.

The court's privacy caseload for its latest term, which began Oct. 7, is light. A Fourth Amendment case involving motor vehicle stops, which the justices are slated to hear in November, is the most noteworthy thus far. But attorneys say that could change by the time the court gavels out at the end of June, with several notable cases brewing in federal appellate courts that could attract the justices' attention.

Another Round for Standing?

Appellate courts across the country continue to issue conflicting rulings on what plaintiffs suing over purported privacy and data security missteps need to allege to establish Article III standing and push their claims past the pleading stage.

The Supreme Court hasn't been shy to intervene in this debate in recent years, first with its 2013 decision in Clapper v. Amnesty International that injuries must be real or imminent and not merely speculative. It followed that up with its 2016 holding in Spokeo v. Robins that harm must be concrete and that mere statutory violations won't suffice.

Despite these outcomes, lower courts continue to struggle with applying these standards to novel data breach and privacy claims, and the question is again working its way back up to the high court.

The justices last year declined to consider the growing standing divide in the context of a data breach suit being pressed against Zappos. But court watchers believe that a similar dispute stemming from a data breach at the U.S. Office of Personnel Management — which the full D.C. Circuit has been asked to rehear — could fare better.

"The OPM case was just another nail in the coffin on the circuit split on standing," Baker Botts LLP special counsel Cynthia Cole said. "It highlights the whole philosophical debate over at what point is it no longer an issue that your personal information is no longer private and is out in the world."

In the OPM case, which involves the data of millions of government employees, a three-judge D.C. Circuit panel split with several sister circuits in concluding that the heightened risk of identity theft was enough to clear the "low bar" for establishing standing at the pleading stage. The panel held that, even though evidence of widespread identity theft and financial fraud had yet to emerge, the plaintiffs had plausibly alleged the sophisticated nation-state hackers believed to be behind the 2015 hack could still use the sensitive pilfered data for these nefarious purposes.

OPM and its contractor KeyPoint Government Solutions filed separate petitions for rehearing en banc last month, arguing that the plaintiffs had asserted only speculative risk of injury and that the panel was wrong to establish a "categorical rule" that individuals have standing to sue "in the event of any cyberattack on a database that includes their personal information."

The plaintiffs shot back in a Sept. 30 filing that the panel had reached the correct conclusion, given that the "acutely confidential" nature of the stolen data rendered them vulnerable to identity theft "indefinitely."

"It would be surprising if the Supreme Court didn't have to address standing for alleged privacy violations sometime soon," Nicole Saharsky, co-head of Mayer Brown LLP's Supreme Court and appellate practice, said, adding that any ruling on the issue would "provide some pretty helpful guidance."

However, given the conservative makeup of the court and the growing appetite of states to add privacy laws to the books that provide more clarity on when plaintiffs are able to sue, the wait for the high court's input may end up being longer than many hope, according to Cole.

"It's likely that the Supreme Court might not want to jump into that fray pretty quickly and, even though there's a circuit split, they may be more inclined to wait until the political climate shakes out and see how local legislatures handle the issue," Cole said.

However, if states start coming to different conclusions on when consumers have suffered damages and have legs to sue, "then maybe it starts to get more pressing for the Supreme Court to intervene," she said.

The case is In re: Office of Personnel Management Data Security Breach Litigation, case numbers 17-5217 and 17-5232, in the U.S. Court of Appeals for the D.C. Circuit.

Biometric Privacy Damages Challenged

Facebook is pushing the full Ninth Circuit to reconsider a unanimous three-judge panel ruling that upheld the certification of a class of what is expected to be at least 6 million Illinois Facebook users who are accusing the social media giant of violating the state's unique Biometric Information Privacy Act through its alleged development and use of facial recognition technology without users' consent.

Given that the biometric privacy law allows for consumers to recoup uncapped statutory damages of between $1,000 and $5,000 per violation, Facebook has argued that permitting the case to proceed to

trial as a class action "throws open the door to class claims threatening draconian liability" without users proving that they've been harmed.

"The question is, at what point does the Supreme Court feel enough pressure to step in and mitigate what looks like a runaway train of damages that will affect a lot of companies," Cole said.

Aside from challenging the panel's conclusions that common issues predominate over individual ones and that class treatment is superior to individual actions despite the potential for a large judgment, Facebook is disputing the finding that the plaintiffs had alleged a sufficiently concrete injury to allow them to meet the Spokeo standing bar. That could provide the high court with another way to tackle the deepening circuit split on the issue.

Facebook has argued that the panel's conclusion that its alleged conduct constituted an invasion of the concrete privacy interests that BIPA is intended to protect "eliminates Article III standing as a meaningful check on any lawsuit" targeting alleged privacy violations. That determination would allow these disputes to move forward even if plaintiffs admit they weren't harmed or that they knowingly chose to share the information with the company they're suing, Facebook has said.

The Facebook users pressing the suit have countered that the Ninth Circuit correctly applied Supreme Court and appellate precedent on standing and the requirements for certifying class actions, and that Facebook's concerns about a massive statutory penalty violating its due process rights are "premature" because a damages award has yet to be assessed.

The case is Patel et al. v. Facebook Inc., case number 18-15982, in the U.S. Court of Appeals for the Ninth Circuit.

TCPA Autodialer Debate Could Get Its Day

The growing body of litigation under the Telephone Consumer Protection Act has prompted a wave of conflicting decisions on key statutory interpretation issues that could convince the Supreme Court to soon step into the fray.

"In the TCPA world, a couple of cases that have found their way to the federal courts of appeals could potentially end up before the Supreme Court due to the varying jurisdictional perspectives on the key legal issues," said Jaszczuk PC partner Margaret Schuchardt.

The case that is perhaps the closest to garnering the justices' attention is a putative class action accusing Facebook of blasting consumers' cellphones with unwanted security notification text messages.

A Ninth Circuit panel resurrected the dispute in June, finding that plaintiff Noah Duguid had adequately alleged that Facebook had sent the messages using an automatic telephone dialing system, or autodialer, in violation of the TCPA. Courts have reached divergent conclusions on what constitutes an autodialer, with the D.C. Circuit striking down the Federal Communication Commission's expansive reading of the term and the Ninth Circuit broadly construing the term to encompass any equipment that has the capacity to store and dial numbers.

After the full Ninth Circuit refused to review the decision, Facebook moved in August for the panel's ruling to be put on hold until it could petition the Supreme Court to weigh in. Duguid opposed the move, arguing that there was no reason for the Supreme Court to hear the case, and the Ninth Circuit last

month denied Facebook's motion to stay the mandate being issued. A Supreme Court petition has yet to be filed.

Schuchardt said the Seventh Circuit is also considering the autodialer issue, in a case involving survey text messages disseminated by AT&T. The court is poised to rule soon in that case on whether to overturn a district court decision that rejected the Ninth Circuit's broad construction of the term, she said.

"Regardless of whether the case makes it to the Supreme Court, the Seventh Circuit's decision will be an important addition to the legal landscape on this issue," Schuchardt added.

The case is Duguid v. Facebook Inc., case number 17-15320, in the U.S. Court of Appeals for the Ninth Circuit.

Fourth Amendment Disputes Show No Signs of Abating

The Supreme Court has tackled a range of thorny Fourth Amendment issues in the past several years, including whether police need warrants to access historical cellphone records, data stored in cellphones and GPS tracking information.

The high court concluded that heightened privacy protections should be afforded to the data at issue in all these cases. But the justices kept their rulings fairly narrow, leaving open the question of whether other types of digital records — such as real-time cellphone records, internet browsing histories, toll transactions and smart meter usage — are similarly protected.

"The Supreme Court has said that some settled rules in the Fourth Amendment context don't do the job in the digital world," said Saharsky, who worked on these issues in her former role as an assistant to the U.S. solicitor general. "It will be interesting to see how the Supreme Court continues to apply its settled precedent in the brick-and-mortar context to the digital world."

While fresh disputes involving government access to digital data are still making their way through the lower courts, the high court is scheduled to hear at least one Fourth Amendment case this year that should be of interest to privacy advocates and others tuned into these issues.

The case, Kansas v. Glover, concerns the question of whether it's reasonable for an officer conducting an investigative stop to assume that the driver is also the registered owner of the vehicle absent any evidence to the contrary. The Kansas Supreme Court, breaking with 12 state high courts and four federal circuits, held that such a stop violated the Fourth Amendment.

While the issue "appears to be a classic Fourth Amendment question," it could have implications far beyond the question at hand, according to Electronic Privacy Information Center President Marc Rotenberg.

"As EPIC explains in an amicus brief for the court, when the rule [that the owner's suspended license is sufficient to provide probable cause for a stop] is joined with the widespread use of automated license plate readers, which make possible these determinations on hundreds or thousands of vehicles, the court's decision could have a profound impact on privacy," Rotenberg said.

The case, which the high court agreed to take up in April, has been fully briefed, and the justices are

slated to hear oral arguments on Nov. 4.

The case is Kansas v. Glover, case number 18-556, in the U.S. Supreme Court.

--Editing by Aaron Pelc.