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

Cybersecurity & Privacy Cases To Watch In 2018

By **Allison Grande**

Law360, New York (January 1, 2018, 3:04 PM EST) -- The U.S. Supreme Court is gearing up to decide a pair of blockbuster privacy disputes that will set the bar for access to cellphone location records and data stored overseas, while lower courts will have their hands full with the continued fallout from the high court's Spokeo decision and the scope of the Federal Trade Commission's data security authority.

After a year of relative calm on the privacy and cybersecurity litigation front, 2018 is shaping up to be busy, with long-running disputes over the reach of the FTC's privacy authority, Illinois' unique biometric privacy law and the Telephone Consumer Protection Act ready to yield some definitive results and the high court tackling a docket that has two pivotal privacy fights on it — with the potential for the justices to add at least one more, according to attorneys.

"Litigation [in 2018] could redefine government enforcement in privacy and security, significantly change the constitutional landscape for privacy, and dramatically alter all data breach class action litigation," said Wiley Rein privacy practice chair Kirk Nahra.

Here, cybersecurity and privacy attorneys flag several litigation fights that will bear watching in 2018.

High Court Takes On Location Privacy

The Supreme Court will soon decide whether the government needs a warrant to access historical cellphone location records, in a case that attorneys are calling one of most significant Fourth Amendment disputes that the high court has ever taken up.

"It's very important not just for the kinds of information at issue in the case, namely cellphone location information, but also for what the court's approach says about the standard the government is going to have to meet to get a lot of other information in our online world that is held by third parties but reveals a lot about our digital lives," said Andrew Pincus, a Mayer Brown LLP partner who helped the Center for Democracy and Technology draft an amicus brief in support of petitioner Timothy Carpenter.

The dispute before the high court stems from a Sixth Circuit ruling that upheld the government's warrantless collection of 127 days of historical cellphone location records that were ultimately used to help convict Carpenter of six robberies in Michigan and Ohio.

The lower court found that these records counted as routinely collected business records that fell under

the third-party doctrine, a standard set by the Supreme Court in a pair of cases from the 1970s that allow the government to obtain business records without a warrant. Carpenter has countered that location information, especially when collected over a long stretch of time, paint a far more detailed account of a person's life than other business records and cannot be covered by the third-party doctrine because their disclosure to service providers isn't voluntary.

Attorneys will be watching the dispute to see whether the justices back a strict reading of the third-party doctrine, or if they set a new standard for location records that are more in line with their recent decisions in U.S. v. Jones and Riley v. California, which found that individuals have a reasonable expectation of privacy in their movements over a long period of time and the contents of their cellphone, respectively.

"In recent decisions, the court has showed some unease with allowing unlimited government access to digital data," said Cooley LLP privacy and data protection practice group chair Michael Rhodes.

During oral arguments on Nov. 29, a majority of the justices seemed open to requiring a higher standard for access to historical location records due to their increased sensitivity, but differed on what reasoning they would use to get to that conclusion.

"If oral arguments are any indication, we're likely to see a sea change in digital privacy law in 2018," said Ed McAndrew, a Ballard Spahr LLP partner and a former federal cybercrime prosecutor. "In Riley, the court said that digital is different, and 2018 is shaping up to be the year in which digital truly becomes different in terms of privacy protections under the Fourth Amendment."

The tech community — including companies such as Apple, Facebook, Google, Microsoft, Twitter and Verizon, which have filed amicus briefs backing neither party but advocating for a search warrant standard — in particular is closely watching the dispute, both for its impact on its strategy for responding to law enforcement data requests and its ability to use such location records for its own purposes, attorneys added.

"Carpenter, whatever its outcome ... will indicate whether the Supreme Court has truly and fully adopted the view that consumers' cellphones deserve heightened privacy protections under the Fourth Amendment — an outcome suggested by its unanimous 2014 ruling [in Riley] that information on cellphones is not subject to a warrantless search," said Jay Edelson, the founder of plaintiffs' firm Edelson PC. "A ruling here will most certainly bleed over into civil litigation related to technology and privacy."

Carpenter is represented by Nathan Freed Wessler, Ben Wizner, David D. Cole, Cecillia D. Wang, Daniel S. Korobkin, Michael J. Steinberg and Kary L. Moss of the American Civil Liberties Union Foundation, Harold Gurewitz of Gurewitz & Raben PLC, and Jeffrey L. Fisher of the Stanford Law School Supreme Court Litigation Clinic.

The government is represented by Deputy Solicitor General Michael R. Dreeben of the U.S. Department of Justice.

The case is Carpenter v. U.S., case number 16-402, in the U.S. Supreme Court.

Microsoft Looks to Preserve Overseas Data Warrant Win

The Supreme Court in October added another closely watched privacy case to its docket: the government's challenge to a Second Circuit decision quashing a warrant issued under the Stored Communications Act that would have forced Microsoft Corp. to produce customer email content data that it had housed on a server in Ireland.

"The issue before the court is going to tell us something very important not just about the scope of the U.S. government's authority to require production of information stored outside the U.S., but it's also going to set an important precedent about other countries' right to get information from service providers in America, especially if Congress doesn't act," Pincus said.

The government has argued that it should be allowed to use a warrant to access data stored overseas because service providers control this information and the disclosure of this data to law enforcement officials takes place within the U.S. Microsoft has countered by echoing the Second Circuit's conclusion that requiring a service provider to disclose electronic communications stored outside the U.S. constitutes an impermissible extraterritorial application of the SCA because the data is physically located abroad.

The high court's ruling is poised to have a sizable impact on the cloud computing industry, with attorneys noting that an affirmation of the Second Circuit's decision would allow service providers to keep their customers' data out of law enforcement's grasp by storing it outside the U.S.

"Tech companies now have servers in many jurisdictions both inside and outside the U.S., so they'll be watching this closely to see what the government's authority will be to compel the production of data not in the U.S.," Morgan Lewis & Bockius LLP partner Mark Krotoski said.

Besides the tech industry, the international community has also taken a special interest in the dispute, especially in the European Union, where officials have raised concerns during the past year about how adequately multinationals are protecting the consumer data that they transfer from the EU to the U.S. as part of the fledgling Privacy Shield data transfer agreement.

The European Union, the U.K. and Irish governments, and the New Zealand privacy commissioner's office have already filed amicus briefs in the case, and attorneys expect Microsoft's argument related to the international discord that allowing the U.S. government to reach overseas data without a warrant would spark to factor prominently into the justices' consideration of the dispute.

"The idea that data is physically present only in one state or country is really under assault, and what we're seeing through the Microsoft case is that the issues really are global in nature and it's going to be very difficult for one country to assert dominance or dominion over data in transit," McAndrew said.

Microsoft's reply brief in the case is due Jan. 11, and the high court is expected to decide the case before the end of the term, although the justices have yet to set a date for oral arguments.

The federal government is represented by acting Solicitor General Noel J. Francisco, acting Assistant Attorney General John P. Cronan, Deputy Solicitor General Michael R. Dreeben, Assistant to the Solicitor General Morgan L. Goodspeed and Ross B. Goldman of the U.S. Department of Justice.

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 Bradford L. Smith, David M. Howard,

John Frank, Jonathan Palmer and Nathaniel Jones.

The case is In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., case number 17-2, in the U.S. Supreme Court.

Spokeo May Get Encore at Supreme Court

Since the Supreme Court ruled in May 2016 that plaintiffs must allege tangible or intangible concrete injuries to establish Article III standing, lower courts have been grappling with how to apply the high court's harm standard to a range of statutory privacy and data breach disputes, with severely mixed results.

"It's fair to say that courts have been struggling," said Skadden Arps Slate Meagher & Flom LLP counsel William Ridgway, adding that plaintiffs seem to be having the most success with overcoming standing challenges when the dispute involves contractual cybersecurity promises that they can point to or when a privacy or cybersecurity statute is involved.

But that jumble may soon find a stabilizing force, as two companies — health insurer CareFirst as well as the company that started it all, Spokeo — are petitioning the high court to clarify when exactly the theft of consumer data or the breach of a statutory privacy right is enough to allow plaintiffs to stay in federal court.

"Spokeo has not been uniformly interpreted by the lower courts, and there's been some division on how Spokeo changes the standing analysis, so if the Supreme Court decides to go back and pick up the issue again, that could answer those questions more definitely and have a significant impact on both privacy and cyber cases," said Aravind Swaminathan, an Orrick Herrington & Sutcliffe LLP partner and global co-chair of the firm’s cybersecurity and data privacy team.

In the CareFirst case, the health insurer in an October petition urged the high court to review the D.C. Circuit's decision that the risk of future harm alleged by policyholders suing over a 2014 data breach was enough to meet the Spokeo standing bar, arguing that the dispute provides an "ideal vehicle" for resolving a much wider Article III standing debate.

The D.C. Circuit's decision to revive the dispute came down on the side of the Sixth and Seventh Circuits, which have also embraced the premise that the risk of future harm is enough to meet the Spokeo standing bar, while cutting against the Second, Third, Fourth and Eighth Circuits, which have ruled the opposite way in similar disputes. CareFirst argued in its petition that it's time the high court tackled this growing divide.

"That case could redefine the landscape for data breach litigation," Nahra said. "The plaintiffs’ bar has been chipping away at a brick wall of precedent, but hasn’t had a true breakthrough yet. A win by the plaintiffs in this case would likely be that breakthrough, with implications for any company that has a data breach."

Tara Swaminatha, a Squire Patton Boggs partner, agreed that if the high court agrees to hear the case and finds that a threat of future harm is sufficient for standing, "then a lot more of these cases will be able to go forward."

"CareFirst will be interesting because it could potentially open the floodgates for plaintiffs to get to the

next phase of litigation," Swaminatha said, adding that a decision from the Supreme Court on the issue could help to reduce "hyperventilation" and start building toward an established doctrine that provides clearer rules of the road for what companies that are breached can expect on the litigation front.

The high court justices will also have the choice to tackle the standing issue by revisiting more familiar territory. Less than two years after the high court remanded its dispute over alleged violations of the Fair Credit Reporting Act to the Ninth Circuit to apply the standing test that it established in the case, Spokeo in early December again petitioned the Supreme Court to weigh in on the issue of whether plaintiff Thomas Robins had alleged a sufficient injury to support his claims that the company unlawfully reported inaccurate information about his education, wealth and job status.

The Ninth Circuit found on remand that Robins' claims did meet the concreteness bar set by the high court and that he had alleged more than a bare procedural violation of the FCRA. But Spokeo in its petition to the high court argued that not only had the Ninth Circuit misapplied this test, but the high court's determination in its earlier ruling that some intangible injuries could meet this threshold has spurred “widespread confusion” among scores of lower courts that “cried out” for an immediate resolution.

"Since the Supreme Court's decision, there have been hundreds of lower court decisions reaching conflicting results because these standing issues come up in so many cases, and the Supreme Court gave little guidance about how to determine what constitutes concrete harm, especially when there's no physical harm or monetary loss," said Pincus, who is representing Spokeo. "We're hoping with this petition to get clarity on how the lower courts can go about defining this concrete injury that is necessary for standing."

Gregory Parks, the head of Morgan Lewis’ privacy and cybersecurity group, added that the first Spokeo go-around was like "the Super Bowl of privacy cases from a litigation perspective" due to the importance of the standing question in these class action disputes, and that the high court's decision to revisit its concrete injury standard in any capacity would be a welcome development.

"Ultimately, the Supreme Court will have to look at the issue again because right now, everybody is looking at the Spokeo ruling and the language that to have standing someone has to have an injury that's concrete but not necessarily tangible, and everyone's spending a lot of time scratching their heads," Parks said.

CareFirst is represented by Robert D. Owen, Francis X. Nolan IV and Matthew O. Gatewood of Eversheds Sutherland. Spokeo is represented by John Nadolenco, Andrew J. Pincus, Archis A. Parasharami, Daniel E. Jones and Donald M. Falk of Mayer Brown LLP.

The policyholders were represented before the D.C. Circuit by Jonathan B. Nace and Christopher T. Nace of Paulson & Nace PLLC. Robins was represented in the Ninth Circuit 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 cases are CareFirst v. Attias, case number 17-641 and Spokeo Inc. v. Thomas Robins, case number 17-806, both in the Supreme Court of the United States.

Biometric Privacy Battle Lines Further Sketched

What once had been a trickle of putative class actions under Illinois' unique Biometric Information Privacy Act has now turned into a full-fledged wave, with companies ranging from Facebook and Google to United Airlines and McDonald's facing lawsuits over their use of fingerprints, facial scans and other biometric identifiers for both commercial and employment purposes. And privacy attorneys expect these disputes to yield some important decisions in the coming year about both the scope and reach of the Illinois statute.

"Companies, especially those that do work in the internet of things space and are consistently developing new products that rely on biometric sign-ins and indicators, will be watching these cases carefully to see what the court has to say about what's covered by the statute and where the injury is from collecting this information," Hogan Lovells privacy litigation partner Michelle Kisloff said.

The crush of pending biometric privacy litigation raises a host of threshold issues such as whether biometric data collection and record-keeping claims meet the Spokeo standing bar, whether the state law can apply extraterritorially and whether the the statute applies to information derived from photographs through tagging features.

Facebook, Google and Shutterfly have all fallen short in their attempts to use these arguments to shake suits accusing them of unlawfully storing consumers' facial scans without permission, and these cases will be important to track in 2018 as courts in Illinois and California dive deeper into the disputes.

Justin Kay, a partner at Drinker Biddle & Reath LLP, in particular flagged the unresolved argument raised in all three disputes that applying the biometric privacy statute to companies that operate outside of Illinois violates the dormant commerce clause of the U.S. Constitution.

"Accepting the dormant commerce clause argument would make it much harder to pursue these cases," Kay said. "It would really restrict the scope of the Illinois law because so much activity goes on beyond Illinois that wouldn't be subject to these suits, so it would be very much focused on only what's happening in the state and classes would be much smaller."

Edelson, who is representing the Facebook users pressing the biometric privacy class action in California federal court against the social media giant, noted that a decision is looming in that dispute on a motion to certify a class of as many as 6 million Illinois Facebook users, and a trial has been scheduled to begin in late May.

"This case will produce a landmark ruling in modern privacy law, regardless of its outcome, as it presents the first major test for Illinois' unique Biometric Information Privacy Act," Edelson said. "It may also suggest an answer to a now-fundamental question for many Americans: do Facebook's widespread data-gathering and -analyzing activities cross the line?"

Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali, added that he hoped that 2018 brought with it a better understanding of how biometric information is collected, which may help stem the tide of litigation companies are currently facing under the state privacy statute.

"The plaintiffs' bar has done a good job of scaring legislators and consumers into believing that their fingerprints are being stored by biometric scanners and that hackers can break into those machines, steal the biometric information and misuse it," he said. "To quote the E-surance ad, 'That's not how it works; that's not how any of this works!' The scores of BIPA lawsuits being filed are based on a foundation that is fundamentally wrong, and I hope a campaign to educate people and reduce the fear-

mongering takes place."

The Facebook users are represented by Jay Edelson, Benjamin H. Richman, Alexander G. Tievsky, Rafey S. Balabanian and Lily Hough of Edelson PC, Shawn A. Williams, David W. Hall, Paul J. Geller, Stuart A. Davidson, Frank A. Richter, Christopher C. Martins, Mark Dearman, Travis E. Downs III and James E. Barz of Robbins Geller Rudman & Dowd LLP and Corban S. Rhodes, Joel H. Bernstein and Ross M. Kamhi of Labaton Sucharow LLP.

Facebook is represented by John Nadolenco and Lauren R. Goldman of Mayer Brown LLP.

The case is In re: Facebook Biometric Information Privacy Litigation, case number 3:15-cv-03747, case number 3:16-cv-00937, in the U.S. District Court for the Northern District of California.

FTC, LabMD Data Security Showdown Comes to a Head

While most companies that have been accused by the FTC of failing to employ reasonable data security methods have elected to settle with the regulator, LabMD is one of the notable few that have chosen to fight back — and that pivotal battle promises to produce some meaningful results this upcoming year.

The Eleventh Circuit heard oral arguments in June on the issue of whether the agency's heads had erred when they overturned their own administrative law judge in declaring 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 of the FTC Act.

Depending on how the justices rule, the "never-ending" battle could be "enormously important" to the regulator's ability to continue to be top dog in the privacy and cybersecurity regulation space, Nahra said.

The dispute, which dates to 2013, could generate several potential outcomes. For one, the appellate panel could decide to back the FTC's more than decade-old strategy of aggressively pursuing data security enforcement actions, which would "essentially be status quo," according to Nahra.

A more earth-shattering outcome would be for the appellate court to strike down the regulator's data security enforcement approach, which would set up a split with the Third Circuit's 2015 decision in a similar challenge mounted by Wyndham Worldwide Corp. that found that the commission has the power to bring such cases under the unfairness prong of Section 5, and would raise the specter of a possible Supreme Court showdown.

Such a ruling would "be enormously disruptive, especially for consumers, and might actually prompt even this Congress to finally act in this area," Nahra added.

The Eleventh Circuit could also decide to settle on some type of middle ground by restricting the FTC's ability to regulate entities such as LabMD that are already covered by statutory privacy schemes such as the Health Insurance Portability and Accountability Act or set a new standard for what constitutes consumer harm in data breach cases — a question that the FTC is also currently trying to answer through its own fact-finding mission — that would limit but not kill the commission's authority in this space.

"Both the courts and the FTC are grappling with the meaning of 'harm,' and I believe 2018 will be the

year when these efforts will converge, with a more sophisticated understanding of the concepts than we have had so far," Covington & Burling LLP data privacy and cybersecurity chair Kurt Wimmer said.

During oral arguments, the justices focused on this issue of whether the patient data leak at the center of the dispute had actually harmed consumers, with at least one justice appearing skeptical that it had, and sharply questioned the commission over why it hadn't set forth specific data security rules for companies to follow. The panel's highly anticipated decision is expected in the coming months.

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 Michael Hoffman, Joel Marcus and Theodore Metzler.

The case is LabMD Inc. v. Federal Trade Commission, case number 16-16270, in the U.S. Court of Appeals for the Eleventh Circuit.

Make or Break for TCPA Litigation

Plaintiffs across the country in recent years have seized on vague statutory terms and the potential for uncapped statutory damages of between $500 and $1,500 to file a barrage of TCPA suits against a wide range of businesses, and both sides have been eagerly awaiting a ruling from the D.C. Circuit that will have a significant impact on the future ebb and flow of such disputes.

The dispute, led by ACA International, centers on a June 2015 Federal Communications Commission order that expanded the scope of the TCPA by taking steps such as broadening the definition of "autodialer," setting strict conditions on calling reassigned numbers, and giving consumers wide latitude to revoke consent. Businesses have argued that the order went too far, while the FCC has countered that its order was carefully considered and well-reasoned.

The D.C. Circuit heard oral arguments in October 2016, and attorneys are hoping that the long wait for a resolution will finally come to an end this year, whether it be through the courts or through action by the Republican-led commission itself.

"Once the D.C. Circuit rules on the consolidated appeals that were filed regarding the FCC's July 2015 Omnibus TCPA Order, we expect to see significant action at the FCC in 2018 on this issue," said Yaron Dori, co-chair of Covington’s communications and media practice group. "The current leadership of the FCC opposed several aspects of the July 2015 order. If the D.C. Circuit does not strike down that order, we expect the FCC to revisit it, which could change the TCPA landscape."

The petitioners are represented by Shay Dvoretzky and Jeffrey R. Johnson of Jones Day, Helgi C. Walker, Scott P. Martin and Lindsay S. See of Gibson, Dunn & Crutcher LLP, Kate Comerford Todd, Steven P. Lehotsky and Warren Postman with the U.S. Chamber of Commerce, Brian Melendez of Dykema Gossett PLLC, Tonia Ouellette Klausner and Keith E. Eggleton of Wilson Sonsini Goodrich & Rosati PC, Christopher J. Wright, Jennifer P. Bagg and Elizabeth Austin Bonner of Harris Wiltshire & Grannis LLP, Amy L. Brown and Jonathan Jacob Nadler of Squire Patton Boggs (US) LLP and Robert A. Long and Yaron Dori and Michael Beder of Covington & Burling LLP.

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

The 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.

--Editing by Rebecca Flanagan and Kelly Duncan.