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 Cybersecurity & Privacy Developments Of 2017

By **Allison Grande**

Law360, New York (December 20, 2017, 5:28 PM EST) -- Cybersecurity and privacy attorneys had their hands full in 2017 keeping track of a slew of legal and policy developments, including global cyberattacks that hit DLA Piper and a range of other organizations, massive breaches that put the spotlight on the data security practices at companies such as Equifax, and a crush of conflicting decisions on when privacy plaintiffs should be allowed in the courthouse door.

"2017 saw a number of important privacy trends come to a head, from massive data breaches at some of the largest companies in the world to a sharp uptick in spam cellphone calls nationwide," said Jay Edelson, the founder of plaintiffs firm Edelson PC. "As a result, American consumers are becoming more and more skeptical that the companies they trust to protect their privacy will actually do so."

Here, cybersecurity and privacy attorneys reflect on some of the most notable developments from a busy 2017.

Global Cyberattacks Make Firms WannaCry

On the afternoon of May 12, word broke that a number of hospitals in Britain's National Health Service had been hit by a ransomware attack that locked them out of their computer systems until they met the hackers' monetary demands. It soon became much worse.

When the dust settled, at least 230,000 computers in more than 150 countries had been infected by what was dubbed the WannaCry ransomware, which researchers found exploited a known vulnerability in Microsoft's file-sharing mechanism. The malware had been built by and stolen from the National Security Agency, and Microsoft had discovered the vulnerability and issued a patch weeks before the cyberattack, but the companies that were hit didn't act quickly enough to install that fix. The Trump administration on Tuesday publicly blamed North Korea for carrying out the attack.

"WannaCry was important because while ransomware had been on people's mind and they had been preparing for it, this was one of the first times we saw big companies have their operations substantially disrupted by a virus that went after mission critical systems," said Mayer Brown LLP partner Stephen Lilley. "Sometimes in the cyber world we think about scenarios like a shipping company getting shut down and those threats seem like they're far away, but WannaCry made it clear that we're in that future already."

While the WannaCry virus was shut down within a few days, the threat reemerged in June, when DLA Piper, British advertising group WPP plc, Russian state-run oil company Rosneft and scores of others confirmed they had been hit by a similar cyberattack that blocked their access to systems in exchange for a ransom. Security experts believed the attack was spread by a variation of a ransomware called Petya, and entered systems through the same exploit of Windows that led to the spread of the WannaCry ransomware.

Attorneys say that the headline-grabbing cyberattacks are the latest and perhaps most notable examples of an evolving cyberthreat landscape where hackers are no longer just interested in stealing personally identifiable information, or PII, but also in targeting a wider range of systems and information.

"You see a lot of companies focus on locking down PII the best they can and having traditional incident response plans," Lilley said. "But with attacks like WannaCry, companies suddenly realize that their entire company can be shut down if they get infected and that it's not just about traditional data breaches any longer. There's a whole other world of issues that they need to think about that go beyond that."

The WannaCry and Petya attacks also highlighted the powerful hacking capabilities that the U.S. government has developed and the danger to all businesses if and when they get out, said Ballard Spahr LLP partner Edward McAndrew.

"The release of intelligence-grade hacking tools into the wild of the internet was probably one of the greatest changes to the threat landscape in 2017," McAndrew said.

Equifax, Uber, SEC Join Data Breach Roster

Global ransomware attacks weren't the only cyberthreat that dominated headlines in 2017. Equifax joined the fray in September, when the credit reporting giant disclosed that it had been hit by hackers who exploited a website application vulnerability to gain access to names, Social Security numbers, addresses and other personal data belonging to roughly 143 million consumers in the U.S. The number of affected U.S. consumers was soon upped to 145.5 million, which is nearly half of the country's population.

"In 2017, the Equifax hack was the most noteworthy data breach because the data broker collects not just traditional credit and financial data on consumers but also other opaque data points and the company has refused to be transparent about their practices," said Bradley S. Shear, managing partner of Shear Law LLC. "It will take lawsuits and federal legislation to try to make them more transparent and accountable."

That interest from private litigants and policymakers came immediately, with scores of putative class actions being filed in nearly every state, investigations being launched by regulators ranging from the Federal Trade Commission to a broad coalition of state attorneys general, and multiple congressional hearings being held to piece together the timeline of the breach — which Equifax said it first discovered at the end of July — and how such a vast quantity of sensitive data could have been exposed by a company that many consumers don't even realize is scooping up so much information about them.

"The Equifax breach totally changed people's perception of how widespread data breaches can be,"

said Fenwick & West LLP of counsel Hanley Chew. "It was notable not only for the sheer amount of people involved, but also because Equifax is one of the three major credit reporting agencies that provide identity theft prevention services that people generally rely on after a breach and, in this role, holds all this personal information about consumers that could be used as the basis for identity fraud."

Equifax wasn't alone in attracting attention from regulators and private litigants over data security and response practices in 2017. Ride-sharing giant Uber experienced this backlash at the end of November, when it admitted that hackers had stolen personal information on 57 million drivers and riders worldwide in 2016, but that the company had elected not to disclose the breach and chose instead to pay the hackers to delete the pilfered data and keep quiet about the attack.

"The Uber attack is interesting in that it highlights the complicated nature of when and how a company discloses an attack or theft when there isn't a clear deadline involved, or it's arguable whether a reporting threshold has been triggered," Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch said.

While the Equifax attack exposed the impact of large-scale data breaches on individuals who don't have a direct relationship with companies that are collecting their data, the hack at Uber — which claims that it didn't report the incident when it first surfaced because it didn't initially believe that any personally identifiable information had been compromised — "exposed the tremendous harm that can be done to organizations that cover up data breaches," McAndrew noted.

"The takeaway is that the cover-up is going to be much worse than the breach," he added.

On the government side, the U.S. Securities and Exchange Commission also took a walk in companies' shoes when, in another memorable development of 2017, the regulator announced in September that a 2016 cyberattack potentially exposed securities data that could have led to the theft of investor dollars through insider training.

"From companies' perspective, that incident was significant because it makes them realize that while you hope the information that you give to a regulator is safe, it may not be," Lilley said. "The SEC incident was very unfortunate, but hopefully it will spark some realization among regulators that no one can be perfect on cybersecurity and it's important for everyone to work together to collectively raise security instead of finger pointing."

Taken together, the major breaches of 2017, along with the scores of smaller breaches that also hit companies around the globe, highlight the constant threat that companies face and the need to continue to do work behind the scenes to avoid being the next business to generate global headlines, according to attorneys.

"To me there isn't one single breach that is a 'game changer.'" Finch said. "Instead, I find it fascinating that they keep happening, often in new and creative ways. To me that’s not a sign of a particular weakness in the corporate cybersecurity environment, rather it shows that this is an issue that is not going to go away any time soon."

Spokeo Split Widens

Since the U.S. Supreme Court ruled in May 2016 that plaintiffs need to allege a tangible or intangible concrete injury to establish Article III standing, confusion among lower courts has abounded over how to apply this standard to a range of statutory privacy and data breach disputes — and 2017 only served to

exacerbate this divide.

"More than a year after the landmark decision in Spokeo Inc v. Robins, U.S. circuit courts remain divided on data breach and privacy litigation, leaving litigants likely to reach disparate results on Spokeo-based motions to dismiss," said Troutman Sanders LLP partner David Anthony.

The last year saw many of these disputes work their way up to the appellate level, offering more authoritative guidance while deepening the split on how courts view the requirement that plaintiffs must plead concrete harm and not a mere procedural violation to be allowed to move forward with their suits.

Spokeo again drew attention in 2017, with the Ninth Circuit in August ruling on remand from the Supreme Court that plaintiff Thomas Robins had standing to pursue his claims that the company violated the Fair Credit Reporting Act by inaccurately reporting information about his wealth, education and job status.

Appellate and district courts around the country also continued to add to the divide over standing for claims brought under a range of other statutes, including the Telephone Consumer Protection Act, the Video Privacy Protection Act and the Fair and Accurate Credit Transaction Act.

Most recently, the Ninth Circuit ruled at the end of November that a plaintiff had standing to pursue his claims that ESPN violated the VPPA by disclosing app users' data with an analytics company, and the Second Circuit shortly before that affirmed the toss of a suit accusing Take-Two interactive Software Inc. of violating the Illinois Biometric Privacy Act on the grounds that the plaintiffs hadn't shown they had standing, as they were not actually injured by the game’s scanning of their faces.

And in the data breach context, the D.C. and Third Circuits issued decisions finding that the risk of future harm was sufficient for plaintiffs to pursue claims against Carefirst and Horizon Healthcare, respectively, while the Fourth Circuit rejected this argument in backing the toss of similar allegations against a South Carolina veterans hospital.

Even within the same circuit, different fact patterns yielded different results, with separate Eighth Circuit panels finding that allegations that a Scottrade customer had paid for data security protections he never received was sufficient for standing, but the threat of future identity theft from a breach at SuperValu was not enough of an injury for standing.

"We're seeing circuits developing certain inclinations about the way to interpret Spokeo, and that's creating two totally different standards and a definite circuit split that will likely work its way up to the Supreme Court," Chew said.

Both Spokeo and CareFirst have petitioned the Supreme Court to review the panel decisions finding standing in their cases, so the issue is likely to only heat up in 2018, attorneys noted.

"There wasn't a lot of resolution in 2017, so those debates remain alive and open," said Lilley.

Biometric Privacy Quilt Grows

Plaintiffs continued to find success in wielding Illinois' unique biometric privacy law in 2017, with several decisions being issued that rejected bids by companies such as Google and Shutterfly to shed claims that

face-scanning features violated the law, and the plaintiffs' successes spurring a wave of new suits, particularly against employers.

"We're seeing more and more of these cases, and companies are watching the developments closely as they use this technology for security, authentication and a range of other services such as making avatars for video games and tagging photos," said Squire Patton Boggs privacy and cybersecurity group co-chair Robin Campbell.

An Illinois federal judge in refusing to nix a putative class action against Shutterfly ruled in September that the state's Biometric Information Privacy Act covers data derived from photos and doesn't require consumers to allege actual damages, while Google also fell short in its bid to shake similar allegations over the use of its face-scanning technology in March.

A California federal judge forecasted a similar outcome for Facebook at a hearing late last month, when he indicated that the social media giant may have violated users' statutory "right to say no" and that he was unconvinced the Supreme Court's Spokeo decision required that they allege real-world harm.

Aside from establishing the scope and reach of the Illinois law, the cases are also having an impact on the spread of similar biometric privacy law to other states, attorneys noted.

Earlier this year, Washington became the third state to enact a law governing the collection and use of consumers' biometric information. But the measure notably contains several departures from the Illinois law that attorneys attributed to lessons learned from the application of the first-of-its-kind law, including the absence of a private right of action and the explicit exclusion of photographs from the definition of "biometric identifier."

"As this litigation continues to wind through the courts, we're going to see the broad contours of the law become more well defined, and states that are contemplating more privacy laws are going to be looking very closely at the outcome of this litigation to see how they want to craft their own laws on this topic in the future," said Emily Tabatabai, a founding member of the cybersecurity and data privacy team at Orrick Herrington & Sutcliffe LLP.

Government Showdowns

Disputes between the government and private sector over access to user data also continued to escalate in 2017, with the Supreme Court agreeing to take up a pair of privacy cases that will more clearly delineate each side's roles and the U.S. Department of Justice amending policies governing how they obtain information from service providers in response to pushback from private companies.

"One thing we saw the past year and will continue to see in 2018 is the tension between the government and the tech sector in terms of privacy and in terms of notification to subscribers," Chew said.

The most notable disputes in this arena involved Microsoft, which continues to be at the center of a dispute with the U.S. government over the legality of a warrant issued under the Stored Communication Act that requires it to turn over email content data that it had housed on a server in Ireland.

The Second Circuit in July 2016 ruled in Microsoft's favor, finding that the government couldn't use these warrants to access data stored overseas. The Supreme Court in October granted the government's

request to review this decision.

Microsoft's separate challenge to the government's practice of indefinitely barring internet service providers from telling users about data warrants also came to a close in 2017, when the government took the step of implementing a formal policy change to limit the frequency and duration of these gag orders.

The U.S. Department of Justice again moved to tweak its procedures for obtaining data from private companies earlier this month, when it issued internal guidance to prosecutors seeking consumer data stored on the cloud that advised them to request the information from underlying businesses rather than their third-party data storage providers, in a shift that drew praise from companies such as Microsoft.

Attorneys expect this dynamic to carry through to 2018, when the sides will face off at the Supreme Court in both the Microsoft dispute and in another case that challenges the government's ability to access without a warrant historical cellphone location records held by service providers, and issues such as law enforcement access to encrypted data promise to be back in the spotlight.

"In the law enforcement world, the biggest stories of 2017 may well be the biggest stories of 2018," McAndrew said.

--Editing by Rebecca Flanagan and Catherine Sum.