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

The Biggest Privacy & Cybersecurity Stories Of 2018

By **Ben Kochman**

Law360 (December 20, 2018, 4:26 PM EST) -- With Facebook's series of data leaks spurring calls for a national privacy law, Europe's new data protection rules coming on the books and Marriott suffering one of the largest data breaches the world has ever seen, 2018 was a massive year for privacy and cybersecurity. Here's a closer look at some of the year's biggest stories.

Europe Finally Gets Its New Data Regime

Companies entered a new world of privacy law on May 25, when the European Union's long-anticipated General Data Protection Regulation came into effect. National privacy regulators can now impose fines of up to 4 percent of a firm's annual global revenue if it breaches the new rules, which in part require that firms provide legal justification for why they sweep up data, notify authorities of data breaches within 72 hours and delete certain portions of EU citizens' data on request.

Observers are still waiting for the first GDPR megafine, but within hours of the rules taking effect, Facebook and Google were hit with complaints claiming they bully users into illegal "forced consent." Ireland's data protection commissioner announced in October that it was separately investigating whether Facebook flouted the GDPR in its handling of a data breach in which intruders accessed 50 million user accounts, though an office spokesman said the social network appeared to have provided notice within the required three days.

Other complaints have claimed Google manipulates cellphone users into turning on location tracking, and challenged how tech giants have used the regulation's "legitimate interest" provision to justify data collection. Meanwhile, Britain's data privacy regulator hit a Canadian data analytics firm that reportedly produced targeted advertisements for pro-Brexit campaigns with the first enforcement notice under the GDPR, threatening to ban the firm from processing EU citizens' data for political purposes.

Many of the national privacy authorities have said their goal in GDPR enforcement is not to punish companies but to inform them of steps they can take to comply, as well as to encourage firms to be transparent about why and how they process data. But even without a major fine to date, the compliance process has still been a headache for many companies under investigation, said Alja Poler De Zwart, Brussels-based of counsel for Morrison & Foerster LLP.

"Companies are focused too much on the fines and too little on the investigations that precede the fines," she told Law360, noting that probes can drain company resources by giving staff members

another job on top of existing duties.

As the year comes to a close, many questions about the scope of the GDPR remain. Many companies still don't understand which cases and contexts require them to seek user consent, De Zwart said.

Other legal battles are likely to bubble up over other gray areas in the new regulation, such as when a user has the right to force a company to delete data and to what extent the GDPR applies to subjects outside the EU.

Facebook Scandals Spur Calls to Regulate Big Tech

Mark Zuckerberg spent much of 2017 traveling the U.S., meeting with locals and posing for pictures in the 30 American states he said he had not yet visited. The monthslong road trip fueled speculation that Facebook's founder and chief operating officer, who boasts of his platform's ability to connect people, would someday run for president.

Then 2018 happened. By the end of the year, Zuckerberg had been grilled at hearings of Congress and the European Parliament as governments across the globe investigated Facebook's data privacy scandals, while consumer advocates lodged lawsuits and asked whether Facebook's more than 2 billion users should move away from the platform.

Cambridge Analytica, a political research firm with ties to President Donald Trump's campaign and pro-Brexit campaigns, was revealed to have exploited Facebook's privacy settings to sweep up personal data from up to 87 million unwitting users. Indictments unsealed by Special Counsel Robert Mueller described how Russian spies used inauthentic accounts on Facebook and its subsidiary Instagram to spread misinformation and sow discord among the U.S. electorate.

Facebook itself announced a series of data leaks, security flaws and breaches, including the episode in which intruders accessed 50 million accounts and, in December, a "bug" that exposed private photos that more than 6.8 million users uploaded but didn't authorize for sharing with third parties.

The resulting backlash, which touched other tech giants dealing with data privacy and misinformation concerns, such as Google and Twitter, has spurred Big Tech to accept that some sort of U.S. national **law** granting consumers privacy rights is inevitable. The debate over how that law should look, however, including to what extent it should resemble the GDPR, is just beginning.

Thought Equifax's Breach Was Big? Try Marriott's

With lawsuits and regulatory inquiries into Equifax's massive 2017 data breach still pending, hotel chain Marriott earlier this month announced a breach that dwarfs the incident suffered by the credit reporting giant, at least in terms of numbers of consumers affected.

Marriott said sensitive data of roughly 500 million travelers, including their passport numbers, travel dates, encrypted credit card numbers and possibly a means to decrypt them, was exposed on a network hosted by subsidiary Starwood Hotels dating back to 2014. The episode immediately prompted questions over how Marriott, which said it discovered the intrusion in September, could have missed the breach during its due diligence process before it acquired Starwood in 2016.

The incident became the second high-profile breach an acquiring company has inherited as part of a

billion-dollar deal in recent years, after Yahoo announced a breach affecting 3 billion users in 2016 while telecom giant Verizon was in the process of purchasing its assets for nearly $5 billion. It could spur technical and aggressive cybersecurity research to take on a more central role in future mergers.

Recent news reports suggesting that hackers linked to the Chinese government may have been behind the intrusion could throw a wrinkle into the company's strategy of defending the bevy of proposed class actions already filed against it by consumers and shareholders. If Marriott can show the attack into Starwood's systems was particularly complex and hard to detect, the hotel chain could have a stronger defense, said Behnam Dayanim, a partner at Paul Hastings LLP.

"There's no strict liability standard for data breaches, so if the attack really came from a nation-state and if it employed highly sophisticated techniques, it would not necessarily mean that they would win the case, but it would be a more favorable set of facts," Dayanim said.

U.S. High Court Changes the Privacy Game

Privacy advocates cheered in June when the U.S. Supreme Court, in Carpenter v. U.S., held that law enforcement generally needs a warrant to access historical cellphone location records. In a 5-4 decision, the high court agreed with convicted bank robber Timothy Carpenter that the government's acquisition of phone records showing his past movements deserves the heightened protections provided by the Fourth Amendment.

In his decision for the majority, Chief Justice John Roberts wrote that cell-site data — which pinpoints someone's location when their phone connects to a nearby cell tower — is different from other types of information held by third-party service providers. Cellphones are indispensable to participating in modern life, Justice Roberts wrote, and a cellphone logs cell-site data that can be used for tracking purposes "by dint of its operation, without any affirmative act on the part of the user beyond powering up."

The government had defended the FBI's use in Carpenter's case of what is known as a 2703(d) order under the Stored Communications Act, which requires authorities to show the requested data is "relevant and material to an ongoing investigation," a lower threshold than the probable cause required for a warrant.

Although the high court insisted its decision was "a narrow one," privacy advocates and ex-prosecutors say it **won't be a stretch** to see lower courts try to apply the Carpenter ruling's logic to other sensitive data sets, like online browsing history, that are both indispensable to investigators and the subject of privacy concerns. The American Civil Liberties Union has already cited Carpenter in cases in Massachusetts and Maine state court, claiming the Fourth Amendment protections the high court granted to Carpenter's historical records should apply to tracking someone's movements in real time.

California Becomes U.S. Privacy Capital Overnight

Also in June, the U.S. got its first GDPR-inspired state privacy law when California Gov. Jerry Brown signed the California Consumer Privacy Act just days after it was introduced in the state Legislature. The new law, set to be enforceable starting in 2020, gives consumers the right to know which information companies are collecting on them and to opt out of having it shared with third parties. It also gives consumers a private right of action, which could lead to a flood of litigation.

Soon after the law was passed, concerned business lobbies representing tech, health, banking, retail and other industries began pushing California lawmakers to amend the law before its enforcement date. A report from the International Association of Privacy Professionals indicated that more than half a million U.S. companies, many of them small to medium-sized businesses, could end up being affected.

Meanwhile, privacy advocates urged California not to water down the new law and to broaden the avenues consumers have to bring lawsuits. Consumer groups have also asked that Congress' version of a privacy law not override the landmark state legislation, as has been requested by tech giants like Google, Amazon, Twitter and Apple, but instead serve as a baseline that state laws can build from.

--Editing by Brian Baresch and Marygrace Murphy.