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 2020

By **Ben Kochman**

Law360 (January 1, 2020, 12:04 PM EST) -- With Facebook asking the U.S. Supreme Court to rein in Illinois' unique biometric privacy law and Marriott attempting to escape liability for its extensive data breach, 2020 could see several twists and turns in the world of cybersecurity and privacy litigation.

Here are a handful of cases worth keeping an eye on in the coming months.

High Court Asked To Check Standing in Facebook Face-Scan Case

A potentially multibillion-dollar class action suit filed over Facebook Inc.'s face-scanning practices could give America's high court a chance to weigh in on an issue it has been hesitant to directly address in recent years: when plaintiffs have constitutional standing in privacy lawsuits.

In December, the social media giant **asked the justices** to review a Ninth Circuit ruling clearing the way for a class of millions of Illinois Facebook users accusing the company of violating the state's unique Biometric Information Privacy Act to take the case to trial, potentially leading to billions of dollars in damages.

Lead plaintiffs Nimesh Patel, Carlo Licata and Adam Pezen have said that Facebook breached BIPA by using facial recognition technology without their consent to fuel its feature that allows users to tag each other in photos. Facebook has argued that the feature has caused users no harm, but the Ninth Circuit in August held that the company's **collection, storage and use** of users' facial scans itself amounts to a sufficiently concrete injury to keep the claims alive.

That ruling echoed a January 2019 decision by Illinois's Supreme Court, which similarly **sided with consumers** by finding that Six Flags season pass holder Stacy Rosenbach can claim that the theme park operator illegally collected her son's thumbprint without permission, even without alleging a separate, real-world harm.

If the U.S. high court agrees to take up the case, it could be a game-changer both for the hundreds of BIPA cases pending in Illinois and for the privacy and cybersecurity bar at large, which has been waiting for some sort of clarity on standing in privacy cases in the wake of the court's 2016 holding, in Spokeo v. Robins , that harm in such cases must be "concrete," without defining exactly what that means.

"The fact that individuals who suffered no actual harm could recover billions of dollars in damages is going to be concerning to the court, which increases the likelihood that the court steps in," said Al Saikali, chair of the data security and privacy group at Shook Hardy & Bacon LLP.

"Given the more politically conservative nature of the court, we could absolutely see an opinion that limits privacy plaintiffs' claims to those where they suffer actual harm, effectively reversing Rosenbach," Saikali said. But "we could also see an opinion where there's some key ambiguity, which creates uncertainty for the future of privacy litigation."

A decision not to hear the case, meanwhile, could lead to a costly settlement for Facebook — or set up a precedent-setting trial in California federal district court.

The case is Facebook Inc. v. Nimesh Patel et al, case number 19-706, in the Supreme Court of the United States.

Marriott Data Breach Harm Claims Put to the Test

Marriott International Inc. has so far failed to convince a Maryland federal court to dismiss sprawling multidistrict litigation stemming from the hotel giant's November 2018 admission that it inherited a massive data breach **when it merged** with rival Starwood Hotel & Resorts Worldwide Inc. in 2016. But the company may have more chances to sway U.S. District Judge Paul W. Grimm in 2020.

Classes of consumers, financial institutions and governments have all attempted to hold Marriott liable for the breach, which Marriott has admitted allowed unidentified intruders on Starwood's network to steal more than 5 million unencrypted passport numbers. So far, the court has ordered the company to unseal a **third-party report** that could reveal key details about the breach and found that the city of Chicago **has the authority** to sue Marriott for injuries to city residents.

But Judge Grimm has yet to weigh in on Marriott's argument that the court should toss claims from hotel guests because they have not made valid claims that they have been "harmed" by the cyberattack. The company has argued that the case should be dismissed because the majority of the class have not said that the episode led to any "actual misuse of their information," instead relying on claims that they will be harmed in the future.

In a bid to boost its claim that hotel guests have not suffered harm, Marriott even included in its court papers an affidavit from Brenda Sprague, former U.S. deputy assistant secretary of state for passport services, who claimed that U.S. passports are "virtually impossible to forge successfully" even with access to stolen passport numbers.

The theories of liability that ultimately survive or are swatted away in the Marriott case will be closely watched by the legions of other companies who have themselves suffered a data breach, or may eventually encounter one.

"Marriott's losses are unfortunately not just their own," said John Reed Stark, a data breach response and digital compliance consultant and senior lecturing fellow at Duke University Law School who once led the U.S. Securities and Exchange Commission's internet enforcement division.

He added that the "playbook" that those suing the hotel giant have used in the case so far "has enabled the plaintiffs class action bar to usher in a new wave of favorable precedent, incentivizing an already burgeoning cottage industry of data breach class action lawsuits."

The case is In re: Marriott International Inc. Customer Data Security Breach Litigation, case number 2879, in the U.S. Judicial Panel on Multidistrict Litigation.

Facebook, Equifax Megadeals Face Challenges

In 2019, Facebook and Equifax Inc. reached settlements within days of each other stemming from their headline-grabbing data privacy incidents — and now both face claims that those deals are not fair, reasonable or adequate.

Facebook is fending off a challenge from advocacy groups to its $5 billion **privacy deal** with the Federal Trade Commission over the company misleading users about how their data was shared, including by allowing political analytics firm Cambridge Analytica to sweep up data on tens of millions of unsuspecting people.

Led by the Electronic Privacy Information Center, or EPIC, objectors in D.C. federal court have **ripped the FTC** for making major concessions to Facebook — including granting the company a massive **liability shield** for its past behavior — in order to convince the social media giant not to challenge the fine with a lawsuit.

Critics have also pointed out that Facebook had faced a potential penalty in the trillions of dollars for violating a 2012 FTC consent order about its past data privacy problems, and have argued for the FTC to order deeper structural changes at the company.

"Unless this settlement is overturned and increased, Facebook will have handsomely profited from abusing its consumers' data, showing that the consent decree wasn't really worth the paper it was printed on," said Bradley Shear, a privacy attorney and managing partner of Shear Law LLC.

In Equifax's case, a Georgia federal judge in December granted final approval to a settlement calling for the credit reporting giant to provide compensation it says is worth up to $425 million to consumers affected by a breach that exposed the Social Security numbers of nearly 150 million Americans.

But the deal, which **sparked outcry** from some consumers after miscommunications about a restitution fund that offered a cash payout of up to $125, could still face an appeal in the Eleventh Circuit. Ted Frank, a frequent class action objector who in October 2018 challenged a Google LLC **privacy settlement** at the Supreme Court, said he will argue to the circuit court that Equifax's deal unfairly lumps together class members in states with more valuable statutory-damage claims — like Utah, whose residents could have sought up to $2,000 — with consumers from other states where no statutory damages are available.

The cases are U.S. v. Facebook Inc., case number 1:19-cv-02184, in the U.S. District Court for the District of Columbia, and In re: Equifax Inc. Customer Data Security Breach Litigation, case number 1:17-md-02800, in the U.S. District Court for the Northern District of Georgia.

More Chances To Address Standing in Data Breaches

Any appellate court's reckoning with the issue of whether the threat of data misuse is enough to allow data breach litigation to go forward is worth watching, though it's an open question whether two cases at the D.C. Circuit will provide clarity on that front.

Litigation filed over a breach at the U.S. Office of Personnel Management that exposed the personal data of millions of government employees is among the privacy disputes **most ripe** for Supreme Court review, industry attorneys have said. The D.C. Circuit revived the case in June, finding that 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 nefarious purposes.

The appeals court in October denied a bid to rehear the case, setting the stage for the OPM and

its contractor KeyPoint Government Solutions to potentially petition the high court.

In another high-profile data breach case that has been batted back and forth between appellate and district courts for years, the D.C. Circuit in December **expressed reservations** about reviving for the second time litigation pending against health insurer CareFirst Inc. over a 2014 data breach.

CareFirst policyholders saw most of their claims axed in January 2019, when a district court judge ruled that the alleged injuries that prompted the D.C. Circuit to **resurrect the suit** in August 2017 **weren't enough** to establish the actual damages necessary for the plaintiffs to move forward with the bulk of their allegations.

Without the Supreme Court eventually stepping in to have its say, companies facing consumer data breach litigation can still face frustratingly different legal standards depending on what circuit the case is filed in, attorneys say.

"We are still waiting, after all these years, for a definitive and helpful standard for considering standing in these data breach cases," said Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale. "While there are some cases percolating in the system that may help or provide useful guidance, it's not clear that any of these cases will apply across the broad range of types of incidents."

The cases are Attias et al. v. CareFirst Inc. et al., case number 19-7020, and 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.

--Additional reporting by Allison Grande and Khorri Atkinson. Editing by Brian Baresch.
