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 2021

By **Ben Kochman**

Law360 (January 3, 2021, 12:02 PM EST) -- With federal courts keeping alive claims in Marriott and Capital One's data breach suits, facial recognition app Clearview AI claiming a First Amendment right to scrape billions of photos from the internet, and retail giants facing a test of the limits of California's privacy law, 2021 should be another busy year for cybersecurity and privacy litigation.

Here, Law360 takes a closer look at the cases worth watching.

Plaintiffs Chart Favorable Path in Marriott, Capital One Breach Suits

Combined class actions stemming from two of the most high-profile data breaches in recent years — at hotelier Marriott International Inc. and banking giant Capital One Financial Corp. — are still pending in Maryland and Virginia courts, respectively, where attorneys for consumers scored several key wins in 2020.

In February, a Maryland judge found that those who stayed at Marriott properties while hackers infiltrated a network managed by its then-subsidiary Starwood have **adequately claimed** injuries traceable to Marriott's failure to detect or stop the intrusion.

Later, in September, a Virginia judge used a similar rationale while **keeping alive** a proposed class action filed against Capital One and Amazon after the bank's 2019 data breach, finding that cardholders and applicants have plausibly claimed that the episode led to an "imminent threat" of identity theft.

Both companies have also struggled to keep quiet forensic analyses of their breaches by third-party consultants — **despite their claims** that such material is privileged "work product" because it was prepared to help prepare for lawsuits — opening them up to potentially damaging details about their security practices being exposed to plaintiffs' lawyers as the discovery process continues in 2021.

"The inclination to retain, or keep on hand, a digital forensics firm that can quickly and knowledgeably combat a cyberattack and restore systems is a commendable one. Yet it now seems that when a company does so, the company is essentially penalized for their efforts," said John Reed Stark, a data breach response and digital compliance consultant and senior lecturing fellow at Duke University Law School. "This makes little practical sense and forces the company, already a victim of an attack, to become victimized yet again."

Lawyers for consumers and other parties suing businesses in the wake of data breaches have countered that they have the right to see forensic reports, which any company handling sensitive

data should commission as a general business matter, even if they are not breached and expecting litigation.

The cases are In re: Marriott International Inc. Customer Data Security Breach Litigation, case number 8:19-md-02879, in the U.S. District Court for the District of Maryland, and In Re: Capital One Customer Data Security Breach Litigation, case number 1:19-md-02915, in the U.S. District Court for the Eastern District of Virginia.

SCOTUS To Weigh in on Computer Crime Law, Robocalls

The U.S. Supreme Court is set to issue two decisions in 2021 that will reverberate through the privacy and cybersecurity world: one that could set limits on the enforcement of a hotly disputed 1984 computer crimes law, and another that could stem the tide of robocall and text message litigation that exposes companies to hefty statutory penalties.

In November, the high court heard arguments in Van Buren v. U.S. , a case that hinges on whether a former Georgia police officer breached a federal law barring "exceeding authorized access" to computer networks when he searched through law enforcement records for inappropriate reasons. Several justices appeared open **during the session** to claims that the Computer Fraud and Abuse Act is "dangerously vague," and could criminalize innocuous online activity, while expressing skepticism of the government's claim that the statute "unambiguously" covered the ex-officer's search.

The case could affect millions of internet users who may technically violate a website's terms of service during everyday activities. But it has more immediate consequences for employees accused of abusing access to networks by either companies or federal prosecutors citing the CFAA, which has both civil and criminal remedies.

"We are now in an age when nearly every organization places purpose-based restrictions on their data, meaning that nearly any employee could be held responsible for violating the CFAA by acting inconsistent with those restraints," said William Ridgway, a partner in the privacy and cybersecurity practice at Skadden Arps Slate Meagher & Flom LLP.

A high court ruling curbing the CFAA's scope could lead to companies taking more aggressive measures to defend themselves from the threat of insiders making off with confidential data, including by enacting technical controls limiting such access, Ridgway added.

Meanwhile, the justices in December heard arguments on an issue that has split federal appeals courts around the country: the definition of an "autodialer" under the Telephone Consumer Protection Act, the federal law regulating the use of robocalls.

In Facebook v. Duguid, the social media giant and its supporters have argued that the Ninth Circuit was wrong to conclude that the TCPA's ban on using an automatic telephone dialing system, or ATDS, to call or text consumers without consent applies to any equipment that has the capacity to store and dial numbers, even if the numbers haven't been generated by a random or sequential number generator.

Noah Duguid and his backers have countered that interpreting the term narrowly to exclude equipment that dials from preexisting lists of numbers, as Facebook is proposing, would result in companies that already know "nearly everything about us" being given the unfettered ability to bombard consumers with automated calls and texts without consequences.

During arguments, the justices struggled to find **common ground** about how the language in the

1991 statute should be applied to modern calling technologies, while agreeing that the law was outed and an "ill fit" for today's digital age.

Attorneys are eagerly awaiting the high court's ruling, which they say could **have an impact** on thousands of lawsuits filed around the country.

The cases are Van Buren v. U.S., case number 19-783, and Facebook Inc. v. Duguid, case number 19-511, at the U.S. Supreme Court.

Facial Recognition App Pushes Novel First Amendment Claim

As protests about systemic racism and police misconduct raged across the U.S. this summer, technology giants like Microsoft Corp. and Amazon.com Inc. announced **one-year-moratoriums** on selling facial recognition technology to law enforcement, in moves the companies said would give Congress time to regulate use of the systems.

Facial recognition startup Clearview AI, on the other hand, doubled down. The New York-based company has continued lobbying law enforcement to purchase use of its database of personally identifiable images scraped from the internet.

Clearview's clients can identify people by uploading fresh pictures of their faces for comparison with the images filed away in Clearview's database, the company says. Clearview now faces a slew of lawsuits claiming that its practices violate Illinois' biometric privacy law by sweeping up images of people's faces without their consent and that they breach other general consumer privacy laws as well.

But in what is considered the first argument of its kind, the company has turned to First Amendment attorney Floyd Abrams of Cahill Gordon & Reindel LLP to argue that its mass-scraping is, in effect, computer "language" that amounts to constitutionally protected speech.

"Clearview transforms, via sophisticated computer technology, public photographs in a manner that when a client of theirs … sends them a picture, they can quickly answer as to whether they have photos that already have been published of the same person," Abrams **told Law360** in October. "We think that is protected by the First Amendment."

Clearview's argument would have a profound impact on the future of online privacy, if it is successful, attorneys say.

"They are claiming a First Amendment right to gather information off the internet and create a product or service, but that's in direct conflict with privacy laws that say there are categories of information that need to be reasonably regulated," said Laura Jehl, who heads the privacy and cybersecurity practice at McDermott Will & Emery LLP.

"The stakes would be huge if companies are granted an absolute right to create anything they want with information 'publicly' available online," Jehl added. "Given that all of us have publicly accessible information available on the internet, would we then have any mechanism to protect how that data is used?"

Advocates at the American Civil Liberties Union, Electronic Frontier Foundation and other organizations have criticized Clearview's First Amendment claim.

"That's not speech; it's conduct that the state of Illinois has a strong interest in regulating in order to protect its residents against abuse," ACLU attorney Nathan Freed Wessler argued in a May blog

post.

The cases are In Re: Clearview AI Inc. Consumer Privacy Litigation, MDL No. 2967., in the U.S. Judicial Panel on Multidistrict Litigation, and David Mutnick v. Clearview AI Inc. et al., case number 1:20-cv-00512; Anthony Hall v. Clearview AI Inc., case number 1:20-cv-00846; Chris Marron v. Clearview AI Inc., case number 1:20-cv-02989, in the U.S. District Court for the Northern District of Illinois; and American Civil Liberties Union et al. v. Clearview AI Inc., case number 2020-CH-04353, in the Circuit Court of Cook County.

California Consumer Privacy Act Tested in Retailer Suit

Litigation filed against a software company that works with retailers to create "risk scores" that are used to identify potentially fraudulent consumer returns is one of the first tests of the scope of the private right of action in California's Consumer Privacy Act, which took effect in January 2020.

In a federal complaint amended in August, California consumer Shadi Hayden accused 12 retail giants — including Best Buy, The Home Depot, Sephora and Bed Bath & Beyond — of illegally sharing customer transaction data with a software firm called The Retail Equation without informing consumers or getting consent.

The amended complaint included a claim under the CCPA, which allows consumers to bring suits when their personal data "is subject to an unauthorized access and exfiltration, theft, or disclosure" by businesses that fail "to implement and maintain reasonable security procedures and practices."

Notably, the California law's private right of action includes statutory violations of up to $750 per consumer per incident, a factor considered attractive to plaintiffs attorneys because they apply even in cases where it may be difficult to prove that someone has suffered harm as a direct result of a data breach.

Defense attorneys have argued that Hayden's claims misinterpret the California law, which allows for private suits only in narrow circumstances when entities suffer cyberattacks or other forms of breaches that expose sensitive data like Social Security numbers, payment card data or medical information.

The retailers in Hayden's case, by contrast, are accused of voluntarily handing over consumer data to The Retail Equation. Motions to dismiss the case were filed in late November, giving the court a chance to decide the key issue of whether such practices could be considered a "data breach" under the CCPA.

"The question is: Is there a private right of action based on data use allegations when there are no allegations consistent with what we could call a 'traditional' data breach?" said Craig Cardon, co-leader of the privacy and cybersecurity group practice at Sheppard Mullin Richter & Hampton LLP, who is among the attorneys defending Sephora in the litigation.

The case is Shadi Hayden v. The Retail Equation et al., case number 8:20-cv-01203, in the U.S. District Court for the Central District of California.

--Additional reporting by Allison Grande and Dave Simpson. Editing by Cole Hill.