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 Top Cybersecurity And Privacy Rulings So Far In 2020

By **Ben Kochman**

Law360 (July 10, 2020, 11:04 PM EDT) -- From a Maryland federal judge recognizing the value of personal data in today's economy to a Virginia court sending companies scrambling to keep post-data breach discussions quiet, it's been a busy few months in cybersecurity and privacy litigation.

Here are five rulings worth revisiting as we head into the year's second half.

Judge in Marriott Case Notes the Value of Personal Data in 2020

In February, while keeping alive litigation stemming from hotel giant Marriott International Inc.'s massive data breach, U.S. District Judge Paul Grimm sided with consumers on a key issue: the spiking value of their personal data, both for corporations and cybercriminals.

The Maryland federal judge found that guests had **adequately claimed** injuries traceable to Marriott's failure to detect the historic hack, in part because of what the court called "the value that personal identifying information has in our increasingly digital economy."

The judge cited the consumers' allegations that Marriott "recognizes the value of this information and collects it to better target customers and increase its profits," as well as a statement from U.S. Attorney General William Barr linking the cyberattack to the Chinese military and accusing China's spies of using the data for unknown intelligence purposes.

The Marriott case also includes claims that some of the up to 383 million guests impacted by the breach have suffered identity theft, while others have an "imminent threat" of identity theft. But February's ruling could boost consumers' counterargument to businesses' claims that cases **relying solely** on the prospect of immediate or future identity theft should be tossed for lack of standing.

"The expanded notion of economic value that was recognized in this case, encompassing not just identity theft by economic actors but also breaches carried out by nation-state actors for intelligence purposes, is something that companies should be mindful of going forward," said William Ridgway, partner in the privacy and cybersecurity practice at Skadden Arps Slate Meagher & Flom LLP.

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.

German High Court Deals Blow to Facebook in Privacy Antitrust Mashup

In the U.S., Facebook agreed last summer to pay a historic $5 billion fine to resolve a Federal Trade Commission probe into its privacy breaches, but the company **largely escaped** the deep structural changes to its business model that some advocates had demanded.

But in Germany, enforcement actions so far appear to be playing out differently. The country's antitrust watchdog — which has broader legal authority than its American counterpart — scored a key win in June, when Germany's high court **provisionally signed off** on its ability to enforce an order requiring the social network to change how it collects user data.

The Federal Cartel Office, or Bundeskartellamt, had accused Facebook of abusing its market dominance by forcing users to agree to nearly limitless data collection in order to use its services, and experts viewed the office's order to change those practices as a **precedent-setting mashup** of privacy and competition law.

Germany's highest court, the Federal Court of Justice, agreed with the antitrust watchdog, reversing an August 2019 ruling from a lower court **that prevented** the authority from enforcing its order while Facebook appeals the case.

"There are no serious doubts about Facebook's dominant position in the German market for social networks or that Facebook is abusing this dominant position with the terms of use prohibited by the Cartel Office," the high court said, in a statement translated from German.

Representatives for Facebook, meanwhile, vowed to keep fighting the accusations of antitrust violations, and said that there would be "no immediate changes" to how it collects Germans' data.

More Confusion on What an 'Autodialer' Is, Exactly

The U.S. Supreme Court's decision Thursday to **jump into** the raging debate over what qualifies as an "autodialer" under the Telephone Consumer Protection Act comes after several appeals courts came down differently on that issue in the first half of 2020.

In February, the Seventh Circuit **further widened** the circuit court split by finding that a dialing system AT&T used to distribute unwanted survey text messages doesn't fall under the disputed statutory term. The three-judge appellate panel refused to revive a putative class action against the telecom giant, holding that equipment must have the capacity to generate random or sequential numbers in order to be considered an automatic telephone dialing system, or autodialer, under the TCPA.

That ruling aligned with the Eleventh Circuit's **late January decision** in Glasser v. Hilton Grand Vacations, which similarly adopted a narrow reading of the litigation-fueling statutory term. In that case, the panel sided with Hilton Grand Vacations Inc. and Pennsylvania Higher Education Assistance Agency's stance that an autodialer requires random or sequential number generation and doesn't encompass equipment that dials from preexisting lists of numbers.

However, both rulings, as well as more limited but similar holdings out of the Third and D.C. circuits, conflict with the Ninth Circuit's 2018 decision in Marks v. Crunch San Diego to embrace a broad reading of "autodialer" that covers all devices with the mere capacity to automatically dial numbers — setting the stage for the high court to address the issue.

"The stakes have never been higher for the fate of the TCPA," said Eric J. Troutman, a Squire Patton Boggs LLP partner who specializes in TCPA litigation, in an interview earlier this month.

The Seventh Circuit case is Ali Gadelhak v. AT&T Services Inc., case number 19-1738.

The Eleventh Circuit consolidated appeals are Melanie Glasser v. Hilton Grand Vacations Co., case number 18-14499, and Tabitha Evans v. Pennsylvania Higher Education Assistance Agency, case number 18-14586.

Illinois Biometric Privacy Law Standing Gets Another Boost

A trend of plaintiff wins in the early stages of cases filed under Illinois' uniquely powerful biometric privacy law continued in May, when the **Seventh Circuit held** that allegations that food service company Compass Group USA Inc. failed to get an employee's informed consent before collecting fingerprints is enough for a lawsuit to have standing.

The appeals panel found that former Compass employee Christine Bryant has the right to pursue her Illinois Biometric Information Privacy Act case in federal court, because her claim that Compass failed to disclose its intentions before collecting her biometric information through a vending machine at work is in itself a concrete and particularized injury under the law.

Compass' alleged failure to disclose deprived Bryant of substantive information that she was legally entitled to, the panel said.

"Equipped with the missing information, she may have chosen not to use the vending machines and instead brought her own lunch or snacks," the judges wrote. "She did not realize that there was a choice to be made and what the costs and benefits were for each option."

The ruling comes after consumers filing BIPA suits received a major boost in January 2019, when the Illinois Supreme Court, in Rosenbach v. Six Flags, found that a theme park season pass holder has **standing to claim** that the company illegally collected her son's thumbprint without permission, even without alleging a separate, real-world harm.

"The ruling in Bryant continues this trend of allowing BIPA cases to proceed ... without any alleged data misuse by a third party," said Aaron Charfoos, a partner in the privacy and cybersecurity practice at Paul Hastings LLP.

"Rosenbach was the seminal case on this issue, but Bryant takes it one step further,'" Charfoos added.

The case is Bryant et al. v. Compass Group U.S.A. Inc., case number 20-1443, in the U.S. Court of Appeals for the Seventh Circuit.

Virginia Court Makes It Harder to Hide Consultants' Breach Reports

As hackers exploited the coronavirus outbreak to cause what cybersecurity experts **described as a spike** in data breaches, a Virginia court sent lawyers scrambling to re-examine how they respond to such episodes.

In May, U.S. Magistrate Judge John F. Anderson ordered Capital One Financial Corp. **to disclose** a cybersecurity firm's forensic analysis of its massive 2019 data breach, rejecting an argument that the report should be shielded from disclosure as attorney-work product.

The Virginia-based bank, which faces an onslaught of litigation after a cybercriminal allegedly exposed the sensitive data of more than 100 million people, had claimed that it should not be forced to turn over the analysis from cybersecurity consultant Mandiant, because the document

was prepared to help Capital One's attorneys deal with the lawsuits.

But Capital One, which bears the legal burden of proving why the data breach analysis should be shielded, would have still likely commissioned the report even if it did not expect legal action, the judge suggested.

The opinion **struck a nerve** with lawyers who counsel businesses as they respond to data breaches, with attorneys claiming that the decision, along with similar recent rulings, could chill efforts to respond to cyberattacks in real time given fears that conversations about the breaches could someday be used against companies in court.

"For companies hit by a cyberattack, it's a virtual journey of Alice in Wonderland, where the perpetrators are rarely caught, where the ultimate victims of the cyberattack are rarely identified, and where the victim company is pilloried like a degenerate corporate criminal," said John Reed Stark, a data breach response consultant and senior lecturing fellow at Duke University Law School.

"Now, to make matters even worse, revered legal rights and protections of attorney-client communications and work product have come under fire," Stark added.

Lawyers for consumers and other parties suing businesses in the wake of data breaches have countered, meanwhile, that they have the right to see the forensic reports, which can provide a rare third-party perspective on how a breach actually happened.

The MDL is 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.

--Additional reporting by Allison Grande, Matthew Perlman and Lauraann Wood. Editing by Emily Kokoll and Michael Watanabe.

All Content © 2003-2020, Portfolio Media, Inc.