The Jeep Hacking Case Is Problematic

Law360, (January 28, 2019)

Greg Brower

Samantha Reviglio

In one of the first civil lawsuits involving cybersecurity vulnerabilities in the automobile context, Flynn v. FCA US LLC, the U.S. Supreme Court recently declined to consider an appeal by an automaker alleged to have concealed the "hackability" of its vehicle-based computer system from consumers.[1]

Flynn was the second of several "car hacking" suits filed in 2015 following media reports that revealed the hackability of certain makes and models of motor vehicles through their on-board computer systems. Despite no evidence of any consumer's car actually being hacked and controlled remotely, these suits were filed alleging various state and federal statutory and common law claims for relief.

The first such case, a class action filed in the U.S. District Court for the Northern District of California, alleged that certain Ford, General Motors and Toyota vehicles contained computers that could be hacked, and that the companies had knowledge of this vulnerability but did not disclose such to consumers.[2] The case was ultimately dismissed upon a finding by the judge that the plaintiffs lacked standing because the alleged risk of hacking was too speculative to constitute actual injury.[3] On appeal, a three-judge panel of the U.S. Court of Appeals for the Ninth Circuit agreed, unanimously concluding that the plaintiffs failed to allege a "concrete and particularized injury."[4] This decision seemed to confirm the high bar for bringing suits based on nothing more than theoretical hackability. So, it was a surprise to everyone when the Flynn case took a different turn.

In Flynn, the allegations are very similar to those rejected in the Toyota case. Specifically, the Flynn plaintiffs alleged the vulnerability of the Uconnect system in some of Chrysler's 2013-2015 Jeep models allowed hackers to gain access to and take control of the vehicles' powertrain and safety-related functions. The Flynn plaintiffs claimed their damages related to these claims included (1) a risk of injury or death, and (2) pecuniary loss because they allegedly overpaid for a deceptively defective vehicle and/or were damaged by their vehicles' diminution in value resulting from the defect. The plaintiffs further alleged that the susceptibility to remote hacking was known to the defendants, but not disclosed to consumers. The plaintiffs are seeking more than $440 million in damages.

In response, defendants Fiat Chrysler Automobiles (the vehicles' manufacturer) and Harman International (the manufacturer of the Uconnect system) moved to dismiss the suit, arguing, inter alia, that the plaintiff class lacked standing, even assuming the allegations of the complaint to be true, because they did not allege any actual injury or damages, and, in any event, a recall issued by FCA had corrected the alleged vulnerability defect to the satisfaction of the National Highway Traffic Safety Administration.

After reviewing the motion to dismiss, the U.S. District Court for the Southern District of Illinois first concluded that the plaintiffs did, on the facts alleged, lack standing to bring the first category of claims, observing that "[t]his isn't like a data breach case where

cybercriminals who have stolen credit card data will likely use that data in the future even if they haven't at the start of a suit."[5] "[I]n this case," the court explained, "there is no allegation that a real world hacker has ever hacked the Uconnect system to cause injury, nor is there any suggestion that hackers with knowledge of these kinds of vulnerabilities take advantage of them to injure hapless drivers."[6] However, the court was much more sympathetic to the second category of claims, finding that the plaintiffs did in fact plead a "fair probability" of financial injury and concluded that, under relevant precedent, that was sufficient to survive a motion to dismiss.[7]

In response to this mixed result, the defendants sought and obtained a certification from the district court to file a request for an interlocutory appeal on a procedural question concerning Federal Rule of Civil Procedure 23(f) class certification. The U.S. Court of Appeals for the Seventh Circuit denied the request, which led defendants to file a petition for a writ of certiorari to the U.S. Supreme Court on Sept. 26, 2018. The defendants' petition argued that a split between the circuit courts of appeal on the Federal Rule of Civil Procedure 23(f) issue, namely whether "manifest error" is a basis for interlocutory appeal of a class-certification decision, demanded Supreme Court review. The defendants argue the "manifest error" was the lower court's holding that the plaintiffs had standing to pursue the matter based on speculative harm from nonexistent hacks.

Several interested parties shared concerns about the potential consequences of the class certification decision and filed amicus briefs with the Supreme Court in support of the petitioners. For example, one amicus brief filed by the National Association of Manufacturers and the American Tort Reform Association outlined the following concerns: that the mere risk of a "hack" is not a violation of a manufacturer's standard of care; the risk of a future hack is not a compensable harm under traditional tort law; and abstract consumer class actions should not overtake products liability.

Two additional amicus briefs were filed by (1) the Alliance of Automobile Manufacturers Inc. and (2) the CTIA — The Wireless Association, Cause of Action Institute and the Association for Unmanned Vehicle Systems International, addressing the potential ramifications of allowing the certification to stand, particularly in regard to innovation and security. Nonetheless, on Jan. 7, 2019, the Supreme Court denied the petition for writ of certiorari, thus declining to hear the case, and setting the stage for a trial.

Allowing this case to proceed to trial will have potentially significant ramifications and will likely lead to future design defect claims against manufacturers of a range of smart devices based on nothing more than an alleged potential vulnerability to hacking.

Class actions based on nothing more than speculation should not drive cybersecurity policy. With an estimated more than 5 million such products out there, a number that is growing significantly with each passing month, novel theories of liability for cybersecurity vulnerabilities, if allowed to flourish, are likely to turn the internet of things into a class action lawyers' bonanza. This may generate millions in fees for the lawyers who bring these suits, but will also stifle innovation, discourage collaboration, and undermine effective vulnerability management, all of which will eventually harm the very consumers they purport to represent.

Gregory A. Brower is a shareholder and Samantha J. Reviglio is an associate at Brownstein Hyatt Farber Schreck LLP.

[1] FCA US LLC v. Flynn, U.S., No. 18-398, cert. denied (Jan. 7, 2019).

[2] Cahen, et al. v. Toyota Motor Corp., et al., 147 F. Supp. 3d 955 (N.D. Cal. 2015).

[3] Id.

[4] Cahen, et al. v. Toyota Motor Corp., et al., 147 F. Supp. 3d 955 (N.D. Cal. 2015), aff'd, 717 F. App'x 720 (9th Cir. 2017).

[5] Flynn v. FCA US LLC, No. 15-CV-0855-MJR-DGW, 2016 WL 5341749, at *2 (S.D. Ill. Sept. 23, 2016) (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694-95 (7th Cir. 2015).

[6] Id.

[7] Id. at *3.