# Class Certification Obstacles In Suits Over Connected Devices

By **Mark Raffman and Katie Kissinger**

Mark Raffman

Katie Kissinger

As modern technologies become increasingly integrated into our daily lives, questions have emerged as to how the law will react to the harms that ensue as a result of reliance on these new technologies.

In early November, Google Inc. disclosed that its team of malware hunters found a number of high-impact vulnerabilities in Chrome, Android, Windows and iOS devices.[1] Google's team stated that these vulnerabilities were "actively exploited in the wild," thus exposing unknowing people to hackers across various devices — including iPhones and Android devices.[2]

While future lawsuits regarding the breach remain uncertain, events such as this one highlight the possibility that the vulnerabilities thus exposed may give rise to class action litigation. And as the 2020 holiday season invites a new surge of internet of things devices into homes around the world, it is fitting to consider the potential liability risks.

The internet of things refers to the interconnection, via the internet, of computing devices embedded in everyday physical objects like vehicles or thermostats, that enable those devices to send and receive data.[3] Despite the relatively recent advent of such connected devices, class actions have arisen challenging them on a variety of grounds — including claims of negligence, breach of implied contract, intrusion upon seclusion and breach of warranty.[4]

One baseline question is whether future internet of things class actions will mirror the experience of data security class actions that do not involve physical-world devices. Despite two decades' worth of data privacy class actions,[5] there is no glut of reported decisions.

The case law that does exist suggests two significant obstacles to bringing class action lawsuits involving connected devices: standing and class certification. If data security cases are any guide, those obstacles may prove formidable.

**Standing for Future Injuries**

The first major issue that future internet of things device plaintiffs will encounter involves whether a plaintiff has asserted a cognizable legal injury — represented, in federal court, by Article III standing.

Courts across the U.S. are split regarding which alleged injuries provide enough basis for

standing in data privacy suits.[6] While the U.S. Court of Appeals for the Ninth Circuit and the U.S. Court of Appeals for the Seventh Circuit have set a relatively low bar for Article III standing at the pleading stage, other circuit courts have insisted upon a more substantial showing of present or future injury.[7]

This split in authority regarding standing for future injuries is especially problematic for data breach and connected device suits, as it complicates claims for damages based on risk of future theft or injury. Hypothetically, if thousands of smart doorbells[8] were infiltrated across the U.S., enabling hackers to access video and audio recordings, customers could fear that hackers might abuse or misuse the personal information they acquire. However, unless real injuries emerge as a result of that hack, potential plaintiffs may face issues of standing until the risk of future harm solidifies.

In situations where courts have conferred standing for class action future injury damages claims, the courts' rulings are highly fact-specific. Notably, in 2019, in In re: U.S. Office of Personnel Management Data Security Breach Litigation, the U.S. Court of Appeals for the D.C. Circuit permitted Article III standing based on an alleged increased risk of identity fraud following a data breach.

Here, the court was able to find a substantial risk of future identity theft based on the type of information stolen (social security numbers, birthdates, fingerprints, addresses), the fact that the hacker had intentionally targeted that information, and because plaintiffs had already experienced instances of identity theft.[9] The court differentiated the facts in the case from two facially similar cases decided in the U.S. Court of Appeals for the Third Circuit and the U.S. Court of Appeals for the Fourth Circuit, [10] where both sets of plaintiffs failed to allege that the personal information was intentionally targeted or that identity theft had since occurred.[11]

In the internet of things realm, where vulnerabilities may give rise to physical-world bodily injuries or property damage, the absence of choate harm may signal a similar reluctance on the part of courts to recognize actions for incipient harm — at least absent the kind of equal amount of specificity alleged in In re: U.S. Office of Personnel Management Data Security Breach Litigation.

Notably, changes in legislation on a state level may provide an expanded avenue for standing for data privacy and connected device class action plaintiffs. In 2018, for example, California passed the California Consumer Privacy Act, or CCPA, giving consumers in California additional protections regarding how businesses may use their personal information.[12]

The CCPA primarily requires that businesses provide notice to consumers about the collection, use and disclosure of personal information, and allows consumers to exercise certain rights over personal information — including the right to opt out of the sale of personal information.[13] Despite the fact that the CCPA first came into effect in the past year, cases citing the legislation[14] have already emerged, signaling the potential for future successful data privacy claims.

While the CCPA will likely have a modest effect, if any, on future internet of things claims, it is indicative of how state legislation may give plaintiffs a broader basis for standing in novel technology cases.

**Class Certification**

Future connected device plaintiffs will also have to overcome the issue of class certification. Like plaintiffs involved in data security class actions, plaintiffs involved in internet of things cases may experience highly individualized damages as a result of a potential breach.

Frequently, class action plaintiffs who require individualized causation assessments are poor candidates for a finding of general causation necessitated by a class action. As a result, as of early 2020, there still had been no decisions that certified data breach class actions for both damages and liability.[15]

Salient parts of the federal rules for civil procedure require that, in cases in which there are claims for damages, questions of law and fact must predominate over any issues affecting individuals.[16] While all class actions must comply with one of the requirements of Federal Rule of Civil Procedure 23(b), 23(b)(3) applies mostly to damages claims.[17] This has proved to be problematic for a number of class actions in the data security realm, as courts have been hesitant to find predomination.

Data breach class actions in courts across the United States have frequently been denied class certification for an inability to meet the requirements of Federal Rule of Civil Procedure 23(b). In most cases, when denying class certification under Rule 23(b)(3) for data privacy class actions, courts have found that plaintiffs failed to meet predomination requirements because they neglected to prove damages on a classwide basis.[18]

In In re: Hannaford Brothers Customer Data Security Breach Litigation[19] and Opperman v. Kong Technologies Inc.,[20] courts denied class certification, finding that the plaintiffs' claims of injury following debit/credit card and connected device breaches failed to predominate, as the harms were individualized and could not be proven.

Similarly, other courts have denied class certification in data privacy cases under Rule 23(b)(3) after finding that the proposed class was not "sufficiently cohesive to warrant adjudication by representation," as the plaintiffs possessed "a constellation of individualized issues."[21]

Cases in which internet of things devices have a real-world impact that results in physical injury will be even more problematic from a predomination standpoint, as the damages will likely be highly individualized. Often, the more individualized plaintiffs damages are, the less likely a court will certify a class action.

In In re: Katrina Canal Breaches Consolidated Litigation, residents of New Orleans claimed damages for damage to property, personal injury and wrongful death after a barge struck and breached a canal during Hurricane Katrina, causing flooding throughout a residential area.[22] However, the U.S. District Court for the Eastern District of Louisiana refused to certify the class of plaintiffs, finding they failed to meet the predominance requirement under Rule 23(b)(3).

The court found that:
[The] proposed class suffers from individual issues measuring various types of property damages (including real property, business loss, and personal property), measuring personal injury damage, determining causation, and assessing affirmative defenses. … [All aspects of this case] present enough individualized issues to predominate over those that are common to the class.[23]

While this case was not representative of data privacy or connected device class action, it represents one of the largest problems future plaintiffs will have to overcome in order to

achieve class certification.

**The Future of IoT Class Actions**

So, what does this mean for plaintiffs involved in future connected device class actions? While such suits are still few and far between, there are early signs that internet of things plaintiffs will face the same challenges as those in data privacy class actions.

One sign of things to come can be found in a case recently out of the U.S. District Court for the Southern District of Illinois, Flynn v. FCA U.S. LLC et al. In Flynn, owners and lessees of Jeep Cherokee vehicles brought an action against FCA US LLC, and its parent company after a 2015 Wired article revealed a defect in thousands of vehicles, leaving them vulnerable to hackers.[24]

In the class action, plaintiffs alleged that the defendants misrepresented the vehicles' vulnerabilities, and that they would not have purchased, or would have paid less for, the vehicles if they had knowledge of the defect.[25] Nevertheless, the court ruled that the parties ultimately lacked standing to sue, finding that (1) because the vehicles could have been made safer did not make them defective; and (2) a theory based on a risk of future injury was too speculative to be deemed "certainly impending."[26]

The court explained that the plaintiffs lacked standing, as:
[T]the allegation that the Defendants wrongfully induced them to purchase their vehicles by concealing the alleged defect … and that their vehicles are worth substantially less than they would be without the alleged defect is conclusory and unsupported. A "concrete" injury must be "de facto;" that is, it must actually exist.[27]

While a vast majority of the early connected device class actions have been settled or dismissed before they reached the class action certification stage, there is occasionally a rare class that will be certified by a court. In In re: Vizio Inc. Consumer Privacy Litigation, the U.S. District Court for the Central District of California issued an order conditionally certifying the class for settlement purposes.[28]

Unlike the cases previously discussed, the plaintiffs in Vizio did not possess a panoply of injuries. Instead, they alleged that defendant Vizio used their smart TVs to collect and share personal data without class members' knowledge or consent.[29] In their 23(b)(3) ruling, the court found that the plaintiffs' claims regarding Vizio's collection and sharing of their personally identifiable viewing data were common questions, and their corresponding legal requirements predominated.

Unlike in In re: Katrina Canal Breaches Consolidated Litigation, a lack of individualized harms was an asset to the class action plaintiffs in Vizio. As a result, successful internet of things class actions in the future may benefit from a Vizio-style approach, while unsuccessful cases may veer dangerously into the territory of individualized and plaintiff-specific claims.

While these are just two examples of internet of things device class action, they are emblematic of the issues that future cases will face. As shown by the data privacy suits that precede them, whether these cases are thrown out for a lack of standing because of a lack of concrete injury, or are denied class certification because common questions do not predominate, future connected device plaintiffs will have an uphill battle ahead of them.

Lawyers must prepare for these complications when contemplating class action litigation.

While internet of things devices pose serious harms that will require litigation soon, they may not be adequately addressed through class action.

---

*Mark Raffman is a partner and Katie Kissinger is an associate at Goodwin Procter LLP.*



[1] Lorenzo Franceschi-Bicchierai, Mysterious Bugs Were Used to hack iPhones and Android Phones and No One Will Talk About It, Vice (Nov. 11, 2020), https://www.vice.com/en/article/xgzxmk/google-project-zero-bugs-used-to-hack-iphones-and-android-phones.

[2] Id.

[3] Internet of Things, Lexico, https://www.lexico.com/definition/internet_of_things (last visited Nov. 16, 2020).

[4] Ijay Plaansky, Legal Liability for IoT Vulnerabilities, 25 (2018), https://i.blackhat.com/us-18/Thu-August-9/us-18-Palansky-Legal-Liability-For-IoT-Vulnerabilities.pdf (last visited Nov. 12, 2020) (potential internet of things class action claims include negligence, strict product liability, breach of warranty, fraud and fraudulent omission, and consumer protection statutes).

[5] Dan Swinhoe, The 15 biggest data breaches of the 21st century, CSO (April 17, 2020), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (notable breaches include the 2013 hack of Adobe, 2017 hack of Equifax, and 2014-2018 hack of Marriott International).

[6] Melissa J. Sachs, Next Trend in Data-Breach Litigation is Class Certification, Report Says, 24 No. 5 Westlaw Journal Class Action 6, 1, 1-2 (2017).

[7] Paul Karlsgodt et al, Entering the '20s — A New Era for Data Breach Class Actions?, BakerHostetler (Feb. 21, 2020), https://www.bakerdatacounsel.com/data-breaches/entering-the-20s-a-new-era-for-data-breach-class-actions/ (hereinafter Karlsgodt et al).

[8] Katheryn Andresen, et al., Recent IoT Class Actions Highlight Need for Manufacturers & Vendors of Connected Products to be Aware of Liability Risks, J.D. Supra (Jan. 15, 2020), https://www.jdsupra.com/legalnews/recent-iot-class-actions-highlight-need-93483/ (two class action lawsuits were filed in California this past year following hacks of Ring security devices in Alabama, Mississippi, and Texas alleging product failures and torts).

[9] In re: U.S. Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42, 58-60 (D.C. Cir. 2019).

[10] Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

[11] In re: U.S. Office of Personnel Management Data Security Breach Litigation at 58.

[12] California Consumer Privacy Act (CCPA), State of California Department of Justice, https://www.oag.ca.gov/privacy/ccpa (last visited Dec. 7, 2020).

[13] What the Zoom Class Action Means for Your Business, TermsFeed (May 15, 2020), https://www.termsfeed.com/blog/zoom-class-action-ccpa-privacy/.

[14] Id.; see In re: Zoom Video Communications Inc. Privacy Litigation, 2020 WL 1561732 (N.D. Cal. 2020).

[15] Karlsgodt et al, supra note 7.

[16] F.R.C.P. Rule 23(b).

[17] It is important to note that courts have also denied class action certification under Federal Rule of Civil Procedure 23(a). Under FRCP 23(a), class action plaintiffs must show (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy. In In re: TJX Companies Retail Security Breach Litigation, the court found that the class action plaintiffs failed to meet the adequacy requirement, as class representative banks had different interests than other plaintiffs.

[18] See In re: Hannaford Bros. Co. Customer Data Security Breach Litigation, 293 F.R.D. 21 (D. Maine 2013); Opperman v. Kong Technologies Inc., 2017 WL 3149295 (N.D. California 2017).

[19] In re: Hannaford Bros. Co. Customer Data Security Breach Litigation, 293 F.R.D. 21 (D. Maine 2013).

[20] Opperman v. Kong Technologies Inc., 2017 WL 3149295 (N.D. California 2017).

[21] In re: TJX Companies Retail Security Breach Litigation, 246 F.R.D. 389, 397 (D. Massachusetts 2007).

[22] In re: Katrina Canal Breaches Consolidated Litigation, 495 F.3d 191 (E.D. L.A. 2007), Order and Reasons, No. 18852 (E.D. L.A. May 21, 2009).

[23] Id.

[24] Andy Greenberg, Hacklers Remotely Kill a Jeep on the Highway — With Me in It, Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[25] Flynn v. FCA US LLC, WL 1492687 (S.D. Ill. 2020).

[26] Id.

[27] Id. (citing Black's Law Dictionary 479 (9th ed. 2009)).

[28] In re: Vizio Inc. Consumer Privacy Litigation, 238 F. Supp.3d 1204 (C.D. Cal. 2017), Order Granting Plaintiff's Motion for Preliminary Approval of Class Settlement (C.D. Cal. 2019) (No. 282).

[29] Id.