wiley

NEWSLETTER

Creative Pleadings, the Growing Role of the Class Action Bludegeon as the Primary Privacy Regulator, and the Cost to American Innovation

February 2019

Privacy in Focus®

There are numerous different options for how to regulate privacy. The United States has generally taken a collaborative self-regulatory approach. The European Union has opted for a much more onerous regulatory regime in the General Data Protection Regulation (GDPR). There are certainly many options in between those two positions. However, recent years have seen the rise of an altogether new and more heavy-handed American privacy regulatory regime not subject to democratic accountability: class action lawsuits.

The U.S. Supreme Court has traditionally been skeptical of allowing lawsuits to proceed on speculative privacy harms. In a 2013 case, *Clapper v. Amnesty International*, the Court considered a challenge to government surveillance of communications. The plaintiffs were attorneys and activists who engaged in sensitive communications with individuals allegedly likely to be surveilled. The Supreme Court held that these plaintiffs lacked standing because it was "highly speculative" that any injury from the surveillance was "certainly impending" because a convoluted chain of events was necessary before the government could or would monitor the plaintiffs' communications.

More recently, in a 2016 case, *Spokeo, Inc. v. Robins*, the Supreme Court considered a plaintiff's suit against a website that allegedly posted incorrect information about him online, in violation of a

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

statute. At issue was standing: The only harm alleged was the statutory violation. The Supreme Court held that simply alleging "a bare procedural violation" of a statute cannot satisfy standing where the alleged procedural violation would "result in no harm." The Court declined to lay down a bright-line rule but, as an example, noted that posting "an incorrect zip code" would probably not result in "any concrete harm."

In the intervening years, class action plaintiffs' lawyers have engaged in a series of clever pleadings to bypass the "certainly impending" and concreteness standards laid down in *Clapper* and *Spokeo*, respectively.

In 2015, a group of consumers filed a class action lawsuit in federal court against vehicle manufacturer FCA after *Wired* magazine published an article describing how two cybersecurity researchers hacked a Jeep Cherokee in a controlled setting. But there was no allegation that any consumer's vehicle had *ever* been hacked outside of a controlled setting. To get around the "highly speculative" problem from *Clapper*, the lawyers couched their harm as an "overpayment theory," arguing that had the consumers known of the security vulnerabilities exposed by *Wired*, they would have paid less for their vehicles or not purchased them at all. For the time being, the overpayment theory was enough for standing. (We have a full article on *FCA v. Flynn* here).

The problems with finding standing in *Flynn* are twofold. First, as noted in a brief filed by CTIA-The Wireless Association, Cause of Action Institute, and Association for Unmanned Vehicle Systems International (drafted by one of the authors of this article), the "overpayment theory" is a clear end-run around *Clapper*'s prohibition on speculative harms. Second, there are hundreds of thousands of known vulnerabilities in software and products. In theory, plaintiffs could allege that any one of these vulnerabilities had some effect on consumer behavior, essentially requiring perfect cybersecurity and allowing class action plaintiffs to attempt to extract huge verdicts based on 20:20 hindsight.

In another recent case, the United States District Court for the Northern District of Georgia refused to dismiss a class action suit against Equifax for its 2017 data breach (No. 17-CV-3463). While one should rightfully sympathize with anyone whose identity was compromised due to Equifax's data breach, that is *not* what the class action involves. Rather, the lead plaintiff, "Union Asset Management Holding AG, seeks to represent a *putative class of investors that purchased ... securities of Equifax* ... ." The claim is essentially the finance version of the *Flynn* overpayment theory, alleging that: (1) Equifax materially misrepresented the strength of its cybersecurity protections to investors; (2) that misrepresentation inflated Equifax's stock price; and (3) Equifax's data breach revealed that inflation, caused the stock price to fall, and hurt investors.

Taking this theory to its logical endpoint raises the same issues as in *Flynn*. The theory is not limited to situations involving massive data breaches. Rather, under the Equifax theory, plaintiffs could argue that they have a colorable allegation against any company where (1) an agent of the company represents that it has adequate cybersecurity protections; and (2) a cybersecurity deficiency that the company knew or should have known about becomes public. For example, the court highlighted Equifax's CEO's response to a question at a college that was uploaded to YouTube, where he said that preventing data fraud was a "huge priority." Thus, although *In re Equifax* involved a data breach, the opinion opens the door for plaintiffs to obtain class

certification, and attempt to extract massive sums from public companies, by bringing claims that would impose a *de facto* perfect cybersecurity requirement without having to meet Article III standing requirements.

In a pair of cases in the United States District Court for the Northern District of California, plaintiffs are trying to push the limits of Article III standing by utilizing a state law to extract liquidated damages from Facebook (Nos. 3:15-cv-03747 and 3:16-cv-00937). The state law – the Illinois Biometric Information Privacy Act (BIPA) – imposes numerous obligations on private entities that collect biometric information, like fingerprints and retina scans. If the entity fails to meet the requirements of the Act, any person "aggrieved" is provided a "right of action … against an offending party." The plaintiffs in this litigation are arguing that Facebook's "Tag Suggestions" – which uses facial recognition technology to associate individuals' names with faces in photos – collects users' biometric data without meeting BIPA's procedural requirements, thus entitling plaintiffs to liquidated damages.

Thus far, this standing theory has prevailed. In early 2018, the court refused to dismiss the cases on standing grounds, finding that unlike the mere zip code mentioned in *Spokeo*, a right to privacy of biometric identifiers was (1) "particularly crucial in our digital world because technology now permits the wholesale collection and storage" of these identifiers and they "cannot be changed if compromised or misused"; and (2) the legislature's judgments were well-grounded in "a long tradition of claims actionable in privacy law" under both the "common law and the literal understanding of privacy." Accordingly, the court declined to require plaintiffs to show "real-world harms," paving the way for potential liability by companies using innovative technologies that – as plaintiffs admit – have not actually harmed anyone.

Moreover, even if BIPA's procedural "harms" are eventually held to be inadequate for Article III standing purposes by a federal appellate court, that will not halt the tide of litigation stemming from BIPA. This is because in January, the Supreme Court of Illinois held that plaintiffs could state a cause of action under BIPA without "[p]roof of actual damages." (We wrote about this problematic holding here). And since state courts, unlike federal courts, are not bound by Article III standing requirements, class plaintiffs will no doubt file their BIPA suits in state courts going forward.

Ultimately, the cases above demonstrate that the most dominant privacy "regulators" are increasingly class action lawyers. But these plaintiffs' lawyers are not bound to the electorate, and their incentive is to extract the largest payout possible for their clients and themselves, *not* to craft the most efficient privacy regulation. This ham-fisted approach to privacy and cybersecurity – if left unchecked – will clutter the dockets of courts and force companies to consider expensive settlements even when there is no actual consumer harm. And this problem is not limited to the Facebooks and the FCAs of the world; 43% of cyberattacks target small businesses. Accordingly, allowing *ex post* privacy suits with massive damages will have a real and substantial impact on technological development in the American economy writ large.

Applying the blunt instrument of "harm-free" class action lawsuits is simply not the way to vindicate privacy interests. Congress, the federal courts, and state legislatures can and should take action to correct this misguided course.

Boyd Garriott, a Law Clerk in Wiley Rein's Telecom, Media, and Technology practice, contributed to this article.