On the WLF Legal Pulse

Timely commentary from WLF's blog

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

April 29, 2019

Supreme Court Leaves Standing for Privacy and Cybersecurity Cases Unresolved

by Michelle Visser, David Cohen, and Nicole Gelsomini

Two recent Supreme Court developments—within just a week of each other—highlight both the central role of Article III's injury-in-fact requirement in privacy and cybersecurity cases and the still-fractured state of the law on the issue of what satisfies that requirement in this area. First, on March 20, 2019 in *Frank v. Gaos*, the Court vacated and remanded the Ninth Circuit's approval of a class action settlement between Google and a class of Google users, directing the lower courts to determine whether the named plaintiffs had suffered a sufficiently concrete injury before approving any settlement. 586 U.S. ___ (2019) (available here). *Frank* reinforces that injury in fact is a requirement at all stages of a litigation, even class settlement, but declines to answer whether the plaintiffs, who alleged a statutory violation premised on Google's sharing of their information but arguably no resulting harm, met that bar.

Five days later, the Court again declined to clarify the injury-in-fact standard in the privacy and cybersecurity context when it denied certiorari in *Zappos.com v. Stevens*. Zappos had appealed a Ninth Circuit decision holding that consumers whose personal information was involved in a data breach, but who suffered no resulting financial losses, had Article III standing. (We previously analyzed the Ninth Circuit's *Zappos* decision here.) A Supreme Court judgment in *Zappos* would have resolved a circuit split over whether the risk of identity theft or fraud in the wake of a data breach is sufficient to confer standing. Unfortunately, that resolution will have to wait.

Article III Injury in Fact

To establish an injury in fact sufficient to support standing, a plaintiff must allege and prove an injury that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560. The "concrete" and "imminent" prongs have provided the most fertile battleground for injury-in-fact disputes in the privacy and cybersecurity context.

Concrete

In *Spokeo v. Robins*, the Supreme Court ruled that concreteness is required even in the context of a statutory violation. 136 S. Ct. 1540 (2016). To determine whether a statutory violation creates an Article III injury, the Supreme Court explained that courts should look to history and the judgment of Congress. at 1549. In the three years since *Spokeo*, lower courts have grappled with what exactly "concrete" means in the case of an intangible privacy or cybersecurity statutory violation, such as

---

Michelle Visser is a Partner, **David Cohen** is Of Counsel, and **Nicole Gelsomini** is an Associate, with Orrick.

whether and when the mere exposure of information may qualify.

Imminent

In *Clapper v. Amnesty International*, the Supreme Court stated that any allegedly imminent harm that has not yet occurred must be "*certainly* impending" to constitute an injury in fact, 568 U.S. 398, 409 (2013); a "speculative chain of possibilities" will not suffice, at 414. In the privacy and cybersecurity context, plaintiffs have frequently argued that, even if the exposure of information does not constitute an injury in fact, the risk of harm resulting from a privacy or cybersecurity incident does. The Sixth, Seventh, Ninth, and D.C. Circuits have held in data breach cases that an alleged threat of future misuse conferred standing, whereas the First, Second, Third, Fourth, and Eighth Circuits held that it did not.

The Supreme Court declined to weigh in on either of these questions in *Frank* or *Zappos*.

Frank v. Gaos

In *Frank v. Gaos*, the plaintiffs alleged that Google transmitted user information, including search terms, to third-party servers when users clicked on links that appeared in their Google searches. They claimed that these transmissions violated the Stored Communications Act ("SCA"), which prohibits some entities from "knowingly divulg[ing]" the contents of certain communications, 18 U.S.C. § 2702(a)(1), and provides a private right of action for "aggrieved" persons to recover for violations, § 2707(a). The parties reached an $8.5 million settlement in which all of the funds (after attorneys' fees, named plaintiff awards, and administrative costs were paid) would be distributed to *cy pres* recipients—and none would go directly to absent class members. The Supreme Court granted *certiorari* solely on the issue of whether the *cy pres*-only arrangement was appropriate. However, during the Supreme Court proceedings, the Solicitor General filed an *amicus* brief questioning whether any named plaintiffs had standing in light of the Court's decision in *Spokeo*. The Court ordered supplemental briefing on that issue.

The plaintiffs argued that they had alleged two concrete Article III injuries: (1) the disclosure of their search terms alone (without any information identifying them as the searchers); and (2) the risk that their search terms would be used to reidentify them as the searchers. The Solicitor General and Google contended that plaintiffs' first asserted harm could not satisfy *Spokeo* because neither the SCA nor any common-law tort recognize this harm as creating a right of action, and that the second asserted harm could not satisfy *Spokeo* or *Clapper* because the allegations of reidentification were too speculative.

In a *per curiam* opinion, the Supreme Court held that the settlement could not be evaluated until the threshold standing issue was resolved. Because no lower court had yet analyzed the plaintiffs' standing under *Spokeo*, the Court remanded the case for lower courts to address the jurisdictional question in the first instance. Justice Thomas dissented, stating that the plaintiffs did have standing in his view, but that the *cy pres*-only settlement was improper.

Although the Court did not purport to rule on whether the named plaintiffs in *Frank* had suffered an injury in fact, it described the issue as posing "substantial questions," Slip Op. 1, and reiterated that standing is not "automatically" satisfied "whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right," Slip Op. 5. This language and the Court's 8-1 consensus may indicate that the Court will be receptive to standing challenges involving alleged privacy or cybersecurity violations in the future.

The Court's opinion in *Frank* also underscores that parties may not settle their way around standing deficiencies on a class-wide basis. Unlike in individual actions, in which parties are free to settle their disputes on their own terms, a class-wide settlement may be settled only with the court's approval. And "[a] court is powerless to approve a proposed class settlement if it lacks jurisdiction over the dispute." Slip Op. 6. Thus, if there is a question about Article III standing in a case, defendants may want to tee it up early in the litigation. The court will already be obliged to consider the issue, and a dismissal on standing grounds may save litigation costs.

Zappos v. Stevens

Zappos v. Stevens arose out of a 2012 attack in which hackers allegedly gained access to the personal information of 24 million Zappos customers. In the class action litigation that ensued, the District of Nevada held that plaintiffs who alleged fraudulent charges resulting from the breach had Article III standing, while those who alleged only a risk of future harm did not. The Ninth Circuit reversed the district court with respect to the "risk of harm" plaintiffs, finding that these plaintiffs had alleged a sufficiently imminent injury in fact.

However, as we previously pointed out, any fear of future fraud relies on exactly the "speculative chain of possibilities" that the Supreme Court confirmed does not satisfy Article III in *Clapper*. Indeed, as Zappos noted in its *certiorari* petition, in the more than seven years since the Zappos breach, plaintiffs have identified 24 customers—representing 0.00001% of the 24 million affected—who claimed that their information was misused as a result. The Supreme Court's denial of Zappos' petition for an appeal allows these plaintiffs' claims to proceed. It also unfortunately allows the Ninth Circuit's faulty reasoning to stand and the circuit split to deepen.

Statutory Injuries

The Supreme Court's dodging of the injury-in-fact inquiry in both *Frank* and *Zappos* comes at a time when state legislatures are increasingly attempting to take the issue of injury off the table. States across the country are enacting statutes that purport to remove any requirement that a plaintiff actually suffered a harm beyond the statutory violation in order to bring a suit under the statute.

For instance, the California Consumer Privacy Act of 2018 ("CCPA") purports to create a private right of action for consumers whose personal information has been subject to unauthorized access and exfiltration, theft, or disclosure—whether or not any financial loss resulted. *See* Cal. Civ. Code § 1798.150. Other states are considering similar legislation. *See, e.g.,* Mass. Senate Bill 120 ("A violation of this chapter shall constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this chapter.").

Likewise, although the Illinois Biometric Information Privacy Act ("BIPA") does not explicitly eliminate any injury requirement, the Supreme Court of Illinois recently held that no injury apart from being subject to a violation of BIPA is required for someone to qualify as an "aggrieved" person eligible to sue under the statute. *See Rosenbach v. Six Flags Entm't Corp.*, No. 123186 (Ill. Jan. 25, 2019). Accordingly, as the barriers to alleging statutory injury in privacy and cybersecurity cases fall, guidance on the Article III injury-in-fact threshold in federal courts has never been more needed.

