Spokeo Speedwagon: Employers Forced To Take Privacy Breach Cases On The Run

Insights
10.02.17

By now, most everyone has *heard it from a friend who, heard it from a friend who, heard it from another* about the U.S. Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins*. It is the case being cited across the country in privacy litigation cases – primarily data breach and Fair Credit Reporting Act (FCRA) class actions – to determine whether those impacted by data breaches and other privacy violations have proper "standing" to bring their claim in court. Depending on the court of appeals claiming jurisdiction, both plaintiffs and defendants have used this decision to their advantage.

Now, however, another court has weighed in with a pivotal decision in this ongoing saga, and let's just say companies *don't want it around*. On remand from the Supreme Court, the 9th Circuit Court of Appeals recently gave a boost to individuals seeking to sue companies collectively for intangible harms in privacy cases. Although Thomas Robins did not suffer harm in the traditional sense when Spokeo published incorrect information about him on their online database, the 9th Circuit agreed on August 15 that Robins' allegations the company violated procedural requirements of the FCRA were sufficiently concrete to confer standing under Article III of the U.S. Constitution.

In privacy cases like those involving the FCRA and data breaches, demonstrating "actual or imminent" harm at the pleading stage proves difficult. Often, plaintiffs' information has not yet been used in a way that has caused any actual harm. Companies have successfully used this fact, along with the reasoning in the Supreme Court's *Spokeo* decision, to challenge plaintiffs' standing when they bring claims alleging intangible harms, such as those alleged by Robins.

Such quick wins save companies hundreds of thousands of dollars. The new decision from the 9th Circuit and cases like it, however, give plaintiffs a path to defeat such challenges. Now companies are certainly *under the gun* and must prepare to *take it on the run.*

Setting The Stage: Talk Is Cheap When The Story Is Good

Spokeo operates a "people search engine" that generates background reports about individuals upon request, using information it gathers from various public records, social media, and other online sources. You can search for people by name, social media account, phone number, and address. Spokeo's website states that it should be used for "research" and to "reconnect" with friends and family.

Robins sued Spokeo after learning that one of the reports about him compiled by the company contained inaccurate information, including that he had completed a higher level of education and that he was wealthier than in reality. Robins filed the suit as a class action, hoping that anyone else who fell victim to misinformation could join his claim. Spokeo promptly moved to dismiss Robins' case for lack of standing.

In order to bring suit in federal court, plaintiffs must have "standing" under Article III of the U.S. Constitution. Standing requires, among other provisions, a plaintiff to have suffered an "injury in fact." Here, Spokeo argued that Robins failed to adequately plead that he suffered any harm as a result of the inaccurate information contained on his report, and thus did not meet this requirement. The district court agreed and dismissed the case, but the 9th Circuit reversed the district court's decision, prompting Spokeo to appeal to the Supreme Court.

In its May 16, 2016 ruling, the Supreme Court punted on the ultimate question of whether Robins had standing, finding the 9th Circuit's analysis incomplete. The Court said that the appeals court's analysis failed to determine whether the alleged injury was particularized to Robins, and therefore sufficiently concrete. The Court vacated the 9th Circuit's opinion and remanded the case with instructions to determine whether Robins' alleged injuries met the concreteness standard imposed by Article III.

You Won't Believe It, Not For A Minute: The Latest Analysis

You may not believe it, but the 9th Circuit held on August 15, 2017 that Robins satisfied Article III's concrete harm requirement. To reach this conclusion, the court examined two questions: (1) Were the statutory provisions at issue established to protect his concrete (as opposed to purely procedural) rights? (2) Did the specific procedural violations alleged in this case actually harm, or present a material risk of harm, to those interests?

For the first step, the 9th Circuit found that the FCRA was, in fact, intended to protect consumers' concrete interest in accurate credit reporting about themselves. To reach this conclusion it looked to legislative history, comparing the interests protected by the FCRA to other reputational and privacy interests that have been historically protected, including protections against defamation and libel. Even if the harm protected by the FCRA is not the exact harm protected in defamation or libel claims, "Congress has chosen to protect against a harm that is at least closely similar *in kind* to others that have traditionally served as the basis for lawsuit."

As for the second step, the court found that Robins sufficiently alleged FCRA violations that constituted a legitimate and material risk of actual harm to him. The court reasoned that, in many cases, a plaintiff will be unable to show a concrete injury by alleging that a consumer reporting agency simply failed to comply with an FCRA procedure. A similar difficulty arises for a data breach plaintiff when his or her information has been stolen, but is not evidenced to have been used (yet).

Because of this conundrum, the 9th Circuit stated that the specific alleged reporting inaccuracy must be examined to ensure it raises a real risk of harm to the concrete interest protected by FCRA

must be examined to ensure it raises a real risk of harm to the concrete interest protected by FCRA.

The court found that the alleged false information in the case – including the misstating of Robins' marital status, education, employment history, and wealth – was the type of false information that could cause a real harm. Accordingly, the court concluded that Robins' complaint sufficiently alleged he suffered a concrete injury, and therefore had standing to proceed.

The Tales Grow Taller On Down the Line

This latest case provides insight on how federal courts, especially those in the 9th Circuit (including California, Nevada, Washington, Oregon, Arizona, and other west coast states), may resolve standing challenges involving FCRA and other privacy claims. The decision also shows a trend in courts' leniency on standing requirements in privacy litigation in general. Take, for example, the D.C. Circuit's recent decision in *Attias v. CareFirst,* where the court found on August 1 that a plaintiff's heightened risk of future identity theft is sufficient to show standing.

Courts are still split, however, on whether plaintiffs can properly bring a claim based solely on the risk that hackers **might** misuse personally identifiable information. For instance, the 4th Circuit held earlier this year in *Beck v. McDonald* that a group of plaintiffs could not establish injury-in-fact to constitute standing under Article III allegations simply because they incurred costs to guard against identity theft and monitor their credit information. Similarly, in *Fero v. Excellus Health Plan, Inc.*, the Western District of New York determined that standing exists if customer data is stolen and misused, but a plaintiff will not have standing if there are no actual allegations of the misuse.

On the other hand, the 6th Circuit held in a similar case that plaintiffs satisfied the injury-in-fact requirement and had Article III standing based solely on the theft of their personal data because it placed them at an **increased risk** of identity theft.

So What Should Companies Do? Take It On the Run

The *Spokeo* saga will likely not end here, as the 9th Circuit's decision does little to clear up the confusion surrounding standing in privacy litigation. The case evidences an even greater split among the federal courts of appeal, and will likely result in another petition to the Supreme Court. One thing, however, is clear; the latest decision gives privacy plaintiffs yet more case law to use to show standing.

Do not fear, however. The 9th Circuit's focus on the particular facts alleged in *Spokeo* leaves room for companies to run with their standing arguments. Both the Supreme Court and the 9th Circuit noted that "mere technical violation[s]" may not be enough to confer standing. They declined, however, to offer any guidance as to what varieties of misinformation should fall into the harmless category, beyond the example of an erroneous zip code. As such, there is no precise inquiry to determine what sort of information tips the scales. Thus, in any case, you should still be able to argue the violations alleged against you are harmless and do not rise to the same level as those in *Spokeo*.

Nonetheless, companies everywhere must pay attention, as data breach and FCRA cases are increasingly brought as large, expensive class actions. Take the recent Equifax data breach, for

increasingly brought as large, expensive class actions. Take the recent Equifax data breach, for example, which has impacted over 143 million people. Moreover, the trend among the federal courts of appeal suggests that an increasing number of jurisdictions are finding intangible harms sufficient to withstand standing challenges in privacy litigation. Thus, these sorts of cases are more apt to survive a motion to dismiss and move more quickly to class certification and discovery, which means increased litigation and settlement costs to companies.

You can hedge against the increased costs associated with cases like *Spokeo* through the design and implementation of effective privacy programs. For example, by identifying and categorizing data based on its requisite sensitivity level, you can design privacy programs that work to ensure sensitive information is accurate and properly protected. This, in turn, reduces the probability of such information falling into the wrong hands or being of the type that could cause harm in the hands of a third party, regardless of whether a minor technical statutory violation or massive data breach has occurred.

For more information, contact the authors at ABridgers@fisherphillips.com (704.778.4173) or MNorvell@fisherphillips.com (704.778.4169).

Service Focus

Class and Collective Actions

Privacy and Cyber

FCRA and Background Screening

Litigation and Trials

Counseling and Advice