No Signs of Slowing Down

Privacy Litigation Update

By Elaine F. Harwell

Right now relatively few data breach lawsuits make it past the pleadings stage. With the rise in these lawsuits, the law surely will develop. But can it keep up with the technology?

Without a doubt, privacy litigation is on the rise, and no industry appears to be safe. Public attention to large data breaches (Yahoo and Equifax), as well as high-profile hacks (Democratic National Committee and HBO), have likely contributed to an uptick in privacy litigation, including consumer class actions, single-record lawsuits, and regulatory enforcement actions. As a result of the increased litigation over the past few years, privacy attorneys have been honing their craft, and burning legal questions—including what exactly plaintiffs need to allege to meet Article III standing requirements—are being battled out in trial courts across the nation.

Despite the increased litigation, relatively few data breach lawsuits make it past the pleadings stage. In 2016, the Supreme Court of the United States decided *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), and held that plaintiffs must allege concrete harm and cannot rely on statutory violations to establish standing. *Spokeo* was by far the biggest privacy decision in recent years, and the fallout continues to divide lower courts across the nation and shape privacy litigation as it moves forward, including damage theories, which continue to evolve, in privacy cases.

Standing

It is impossible to discuss the current legal landscape of standing in privacy litigation without first setting the stage with the landmark case of *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). In *Spokeo*, the high court addressed whether a plaintiff could bring and maintain an action based on allegations of a bare violation of a statue, specifically the Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq.* Robins, on behalf of a putative class, alleged that Spokeo, an online "people search" engine and aggregator of personal information, violated the Fair Credit Reporting Act by including inaccurate information in his online profile.

Ultimately, the Supreme Court held in *Spokeo* that whatever statutory violation may have occurred, a plaintiff must suffer an injury in fact that is concrete and particularized to satisfy Article III standing. The Court's decision focused particularly on the application of the "concreteness" prong. The Court found that although "intangible"

■ Elaine F. Harwell is of counsel in Selman Breitman's San Diego office and heads up the firm's cyber law department. She practices in the areas of complex tort and business litigation, with a current emphasis on privacy and information security. Over the past few years, Ms. Harwell has devoted substantial time and effort to the rapidly expanding area of law involving privacy and cybersecurity. She has earned the ANSI-accredited Certified Information Privacy Professional/United States (CIPP/US) credential through the International Association of Privacy Professionals (IAPP).

injuries can be concrete, and the "violation of a procedural right" can be sufficient in some circumstances, a mere statutory violation is insufficient to confer standing in the absence of any concrete harm. In the end, the Court remanded the case to the Ninth Circuit Court of Appeals to determine whether Robins had adequately alleged a concrete injury.

While some circuits appear to be more "plaintiff friendly" than others, it is difficult to make sweeping generalizations. In most data breach cases finding standing, however, the courts typically find a cognizable injury when plaintiffs can show that they had to take steps to ensure their own personal and financial security after a breach.

Most tellingly, after *Spokeo*, both sides declared victory. The defense bar declared victory based on the fact that the Court ultimately remanded the case to the Ninth Circuit to determine whether Robins had adequately alleged a concrete injury, and the plaintiffs' bar has made good use of the portion of the decision that found a "concrete" injury need not be tangible. Notably, the Court found that an injury could be intangible, as long as it relied on a harm that Congress recognized, such as misreporting of one's credit information, or if it bore a "close relationship" to an already recognized harm.

The Ninth Circuit heard oral arguments in December 2016 on the remanded case, and in August 2017 issued a ruling. A unanimous Ninth Circuit panel rejected Spokeo's argument that Robins' allegations of harm were too speculative to establish a "concrete" injury. The Ninth Circuit instead concluded that Robins had met the standing bar since he had alleged Fair Credit Reporting Act violations that clearly implicated his "concrete interests in truthful credit reporting" that Congress had solidified in enacting the statute.

While at first blush, the ruling seems to give plaintiffs a low standing bar and in turn present difficulties for defendants trying to challenge standing for statutory injury cases in the Ninth Circuit, the Court's fact-dependent decision and insistence that there must be an "examination of the nature of the specific alleged reporting inaccuracies to ensure that they raise a real risk of harm," may ultimately give defense attorneys a boost. As a result of the ruling, courts may be led to focus greater emphasis on each plaintiff's specific allegations of harm or wrongdoing. This is especially true given the Ninth Circuit's insistence that some harm must be alleged and that not every "minor inaccuracy reported in violation of the [Fair Credit Reporting Act]" would give rise to standing.

Notably, circuits across the country have been grappling with the post-*Spokeo* landscape. While some circuits appear to be more "plaintiff friendly" than others, it is difficult to make sweeping generalizations. In most data breach cases finding standing, however, the courts typically find a cognizable injury when plaintiffs can show that they had to take steps to ensure their own personal and financial security after a breach.

In a pre-*Spokeo* published opinion from the Seventh Circuit, *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015), after a 2013 data breach, the court permitted a suit when it found that the plaintiffs suffered concrete injuries for the trouble and expense of preventing fraud on their accounts. The court noted,

> it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.

Ultimately, what makes the precedential ruling in *Remijas* particularly notable is that the court ruled that not only do customers whose payment card information was compromised in a breach have standing to sue after they suffer fraudulent charges, but they also have standing based on incurring fraud-prevention expenses such as credit monitoring.

Similarly, in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 386 (6th Cir. 2016), the Sixth Circuit stated,

> although it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when Nationwide recommended taking these steps.

(internal citations omitted).

In *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 2017 WL 242554, at *11 (3d Cir. Jan. 20, 2017), the Third Circuit revived a data breach class action, finding that the disclosure of the plaintiff's personal information was a "cognizable injury." The court explained:

> Our conclusion that it was within Congress's discretion to elevate the disclosure of private information into a concrete injury is strengthened by the difficulty that would follow from requiring proof of identity theft or some other tangible injury. "[R]equiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own.…" Namely, the "more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach.

(internal citations omitted).

In the more recent *Attias v. CareFirst Inc.*, No. 16-7108, (D.D.C., Aug. 1, 2017), the court reversed the district court's dismissal for standing finding that the district court's

view of the complaint was too narrow under *Spokeo*. Indeed, the court found the plaintiff had "cleared the low bar to establish their standing at the pleading stage." The court also noted plaintiffs' allegations that they were exposed to a "heightened risk of identity theft" was sufficient to "plausibly allege[] a risk of future injury that is substantial enough to create Article III standing."

Interestingly, the court's holding in *Attias* appeared to rest on the particular type of data exposed, including names, social security numbers, medical information, and credit card numbers. The court concluded that at the very least, it was plausible to infer that the type of information exposed could be used to commit fraud. In the context of a data breach, the court concluded that there was not a long sequence of uncertain contingencies that needed to occur before the plaintiffs suffer harm. Based on the court's reasoning, exposure of personally identifying information may be all that is needed for the court to find the injury-in-fact requirement satisfied in the D.C. Circuit.

Conversely, after a 2014 payment card breach, the plaintiff in *Whalen v. Michaels Stores, Inc.*, No. 16-260 (L), 2017 WL 1556116, at *1 (2d Cir. May 2, 2017), asserted instances of attempted unauthorized use of her credit card and a future risk of identity theft as her injuries. The Second Circuit affirmed the district court's finding that the plaintiff did not sufficiently allege standing in that she "neither alleged that she incurred any actual charges on her credit card, nor, with any specificity, that she had spent time or money monitoring her credit." *Id*. The court explained that the claims did not raise a "particularized and concrete injury suffered from the attempted fraudulent purposes." *Id*. at *2.

The important difference for defense counsel to note between *Whalen* and the other cases finding standing is that the plaintiff in *Whalen* was unable to establish that (1) she had to pay any money (fraudulent charges were forgiven); (2) she suffered any other consequences in an effort to prevent or correct fraud on their accounts; or (3) she was at risk of any future fraud (the stolen credit card was cancelled, and no other information was alleged to have been stolen).

Despite this general summarization, defense counsel should be aware that the standing issue in privacy litigation is not yet settled. Counsel should pay particular attention to where their case is venued because some circuits have issued more "plaintiff friendly" rulings than others. For example, the Seventh and Sixth Circuits tend to find standing more often than not, whereas the other circuits have more mixed results. If the circuit tends to issue more pro-plaintiff rulings, defense counsel may need to be prepared to distinguish earlier rulings.

Causation

As relatively few data breach cases make it out of the pleadings stage (and those that do often settle quickly), the development of the causation defense in them is still in its infancy. At its core, the causation question depends on whether a plaintiff can prove that the subject breach caused the claimed loss. In *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), the Eleventh Circuit considered standing and causation after the theft of unencrypted laptops from a health insurer, which contained personally identifiable information (PII). The plaintiffs alleged that they were victims of identity theft after the data breach. First the court analyzed and found that the plaintiffs met the Article III standing requirements. Then the court considered whether the plaintiffs' causation allegations were sufficient to support their claims, including, among others, of negligence, breach of contract, and breach of the implied covenant of good faith and fair dealing. Specifically, the plaintiffs' complaint alleged that that the unencrypted, stolen laptops contained their sensitive information, their identities were stolen, and the stolen identities were used to open unauthorized accounts.

The *Resnick* court held that the plaintiffs' claims adequately demonstrated a "nexus" between the data breach and identity theft because the allegations indicated that the compromised information was the same information that was used to steal the plaintiffs' identities and the plaintiffs had taken "substantial precautions" to protect their personal information. The court reversed the district court's dismissal of these claims, concluding that these allegations showed "more than a coincidence of time and sequence."

When faced with causation questions in a data breach case, defense counsel should probe whether a "nexus" truly exists, or whether the connection is simply too tenuous. Because many unknown factors and circumstances potentially can lead to stolen identities, counsel should be diligent in probing basic questions. Ask questions such as, when and where have the credit cards been used? Which entities have the plaintiffs given their personal information to? And how many of those entities have been compromised? While still a developing area, causation can be a difficult hurdle for many data breach plaintiffs.

At its core, the causation question depends on whether a plaintiff can prove that the subject breach caused the claimed loss.

Damage Theories

In recent months and years courts have seen an increase in the number of data breach cases filed. The large number of data breaches reported in the news has likely led to the increase in privacy litigation. Since a significant number of these cases never make it past the pleadings stage, the plaintiffs' bar has responded by continuing to develop new theories in an effort to demonstrate the harm that plaintiffs have suffered.

Increased Risk of Future Harm

By far one of the most frequently asserted harms is that a plaintiff faces an increased risk of future harm due to the compromise of the litigant's PII. Plaintiffs' attorneys argue that the harm lies in the *potential* for the compromised information to be exploited by bad actors. Many courts have rejected this theory, including the district court in *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 959 (D. Nev. 2015), noting, "years that have passed without Plaintiffs making a single allegation of theft or fraud demonstrate that the risk is not immediate. [ ] The possibility that the alleged harm could transpire in the as-of-yet undeter-

mined future regulates Plaintiffs' injuries to the realm of speculation." (Internal citations omitted.)

Not all courts, however, have rejected this theory. In a pre-*Spokeo* case from the Ninth Circuit, *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the court addressed Article III standing in the context of stolen personal information. There, a thief stole a laptop from Starbucks, which contained unencrypted names, addresses, and Social Security numbers of thousands of Starbucks employees. *Id*. at 1140. The Ninth Circuit held that "the possibility of future injury may be sufficient to confer standing" when the plaintiff is "immediately in danger of sustaining some direct injury as the result of the challenged conduct." *Id*. at 1142 (alteration omitted) (internal quotation marks omitted). The Ninth Circuit held that the plaintiffs here alleged "a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." *Id*. at 1143. Based on this "credible threat of real and immediate harm," the plaintiffs "sufficiently alleged an injury-in-fact for purposes of Article III standing." *Id*.

Misrepresentation or Overpayment

Essentially a new take on the "benefit of the bargain" theory, plaintiffs asserting a misrepresentation theory have been making a very powerful argument that has seen recent success. In short, in a misrepresentation theory, plaintiffs assert that they relied on a defendant's misrepresentation about the security measures used to safeguard sensitive information, and a subsequent data breach provided evidence that the measures were either insufficient or improperly implemented. Plaintiffs typically argue that *had they known* of the deficient security measures, they would not have paid—or they would have paid less—for the defendant's products or services. In essence, the plaintiffs claim that they did not receive the benefit of the bargain from the transaction.

Likely the most well-known example of the success of the benefit-of-the-bargain theory involved a class action claim against LinkedIn. In *In re LinkedIn User Privacy Litig.*, No. 5:12-cv-03088, (N.D. Cal. 2015), the plaintiff alleged that she paid for LinkedIn's premium subscription service under the belief that the company used "industry standard" security measures to protect customer data, when, in fact, the company's outdated and insufficient security led to a massive 2012 data breach during which millions of passwords were leaked. The plaintiff alleged that but for the security promise, she would not have paid for the premium subscription. The court refused to grant a motion to dismiss; LinkedIn ultimately settled, to the tune of $1.25 million; and class members (everyone who paid a fee to LinkedIn for a premium subscription), received up to $50.

Notably, under this theory, the focus is not on the data breach itself and any potential risk of future harm, but rather, it is on the breach of a contract or claim of overpayment. In short, plaintiffs argue that the "harm" or injury occurred as soon as the PII or sensitive data was handed over to a company with lax security because the company never provided the benefit of the bargain. Lawyers counseling their clients should be sensitive to the promises that their clients make with regard to data security. Now that privacy and data security are widely used as a marketing tool, companies overpromising security may potentially open themselves up to limitless liability. It should also be noted that a company may not even need to make an express promise with regard to security to open itself up to liability. Merely handling or accepting certain types of particularly sensitive information, *e.g.*, medical, financial, or legal information, may illicit certain expectations from consumers that the data is safe, even if no express promise is ever made.

In defending against these types of claims, the defense attorney should consider and probe whether the consumer truly has relied on the promises for security. Indeed, did the consumer even read the privacy policy?

Consumption of Time or Money

As discussed previously, some courts have recognized as harm suffered by consumers the consumption of their time or money to rectify or monitor their personal and financial information after a breach. For example, courts have found that a plaintiff has suffered injury in these situations:

- A consumer has had to spend time dealing with, or addressing, unauthorized charges to credit or debit cards;
- A company has recommended the purchase of identity theft protection;
- A consumer has had to engage a tax preparer or to incur accountant expenses to deal with a fraudulent tax return; and
- A consumer has experienced a loss of funds, or a loss of the use of the funds, in an account.

Injury, however, is not always a given. Practically speaking, many consumers suffer few compensable injuries when a data breach occurs. Often consumers are not responsible for fraudulent charges on their credit cards, breached companies offer free credit monitoring to help prevent or to mitigate identity theft, and it can be difficult to prove that a person's identity was stolen as a result of a particular breach. Thus, the circumstances of each litigant's claims should be closely examined on a case-by-case basis.

Conclusions and Takeaways

In looking at the jurisprudence based on past data breach cases, it is apparent that courts were often reluctant to recognize data breach harms. Cases that do recognize harm are often narrow, and courts rarely make progressive leaps in this area of the law. That said, plaintiffs' attorneys have become more creative in their pleadings, and the courts' attitudes toward redress in these types of cases have noticeably shifted in recent years. Interestingly, in an increasing number of data breach cases, the focus has turned to the security that defendants establish (or the lack of it) and the elusive standard of "reasonable security." At this point, no case appears to address the "reasonable security" issue directly, and with technology changing at such a rapid pace, it is intriguing to consider how the law will keep pace.

Privacy litigation does not appear to be slowing. The recent rise in privacy litigation can most certainly be traced to the increase in consumer awareness, aided by the heavy media coverage of large data breaches and high-profile hacks. Consumers are now more educated and thoughtful when it comes to their privacy, and cognizant of their privacy rights. As a result, and as consumers continue to hand over more and more data, it is likely that we will continue to see development in this area of the law. FD