THOMSON REUTERS

Westlaw®

When the levee breaks: Tackling data breach litigation in 2017

By Karl Siganporia, Esq.

JULY 28, 2017

There may come a time when technology is sufficiently advanced to prevent data breaches altogether, a time when the only people who can conceivably access a given piece of data are those who are authorized to do so.

Until then, organizations, consumers and legal bodies the world over are grappling with how the risks and costs associated with vastly increasing data sharing and usage ought to be apportioned. In the context of data breach litigation, these contours are still evolving.

Given the absence of domestic congressional intervention, the landscape is somewhat fractured. This is true especially with existing, already-precarious international frameworks for data transfer between jurisdictions facing potentially fatal (and possibly inadvertent) political headwinds in the nationalism and isolationism ascendant in western democracies.

> U.S. courts are gradually congealing around the idea that disclosure of one's private information in a data breach constitutes a distinct, cognizable harm in and of itself.

Unsurprisingly, U.S. courts are gradually congealing around the idea that disclosure of one's private information in a data breach constitutes a distinct, cognizable harm in and of itself, separate from whether that information has yet been injuriously misused by the time of suit.

An individual consumer's data are now routinely spread across countless containers that are potentially accessible to malevolent actors — every store we shop at, every wireless-enabled refrigerator or television or pacemaker, and so much more — and each container has the potential to be compromised by a data breach.

Consumers who share their data with the companies that serve them ostensibly do so voluntarily, but as a practical matter, participating meaningfully in society now virtually requires sharing of personal information.

Some of the associated risk stems from the fact that seemingly meaningless data points can be leveraged for misuse when combined with publically available information on social media that, in isolation, may not strike the average person as being particularly sensitive.

Though the challenges companies face regarding data breaches are novel in some respects, external pressure to govern corporate-held data is an all too familiar story, driven for most of the new millennium by compliance and e-discovery requirements, as well as regulation around protection of especially sensitive information (such as health care information or personally identifiable information).

This article explores the state of data breach litigation in 2017 and examines both the potential consequences for litigants and action items for at-risk organizations.

THE STATE OF DATA BREACH LITIGATION IN 2017

Can plaintiffs in class-action privacy litigation establish Article III standing merely by pleading that each plaintiff suffered a statutory violation?

The U.S. Supreme Court answered in the negative in a May 2016 decision, *Spokeo Inc. v. Robins*, 136 S. Ct. 1540 (2016).

The high court found the 9th U.S. Circuit Court of Appeals erred in its determination that plaintiffs had standing to bring a class action against Spokeo Inc. for disseminating false information in its people search engine.

The 9th Circuit analyzed particularity but overlooked concreteness, the high court said.

According to the Supreme Court's opinion, plaintiffs must show both to prove that an alleged injury is an injury-in-fact — which, in turn, is a prerequisite for Article III standing.

The *Spokeo* court instructed that "Article III requires a concrete injury even in the context of a statutory violation. For that reason, [plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."

A statutory violation, standing alone, was insufficient to confer standing, the opinion said.

The Supreme Court went on to say that a consumer reporting agency's failure to provide a required notice, or the dissemination

of an incorrect zip code are examples of mere procedural violations of the applicable statute that would not cause harm or present a material risk of harm.

Post-*Spokeo*, several courts have addressed the question of what kind of statutory violations can form the basis of a concrete injury.

It may make a difference, however, whether a defendant's conduct is alleged to have violated state law or federal law.

In *Van Patten v. Vertical Fitness Group LLC*, 847 F.3d 1037 (9th Cir. 2017), the 9th Circuit held that a man who sued a gym owner and marketing company for sending text messages that allegedly violated the federal Telephone Consumer Protection Act, 47 U.S.C.A. § 227, would have standing to pursue a class action.

It distinguished the claimed TCPA violations from merely procedural statutory violations that the high court mentioned in *Spokeo*.

> In an environment where every organization is susceptible to data breaches, complete prevention appears to be an unrealistic goal from a technical perspective.

"The telemarketing text messages at issue here, absent consent, present the precise harm and infringe the same privacy interests Congress sought to protect in enacting the TCPA," the 9th Circuit said.

The 3rd Circuit employed similar, though distinct, reasoning in *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016), and *In re Horizon Healthcare Services Inc. Data Breach Litigation*, 846 F.3d 625 (3d Cir. 2017).

In *Nickelodeon* the 3rd Circuit held that Viacom and Google caused the plaintiffs — a group of children younger than 13 — to suffer a de facto injury by unlawfully disclosing information about their online behavior, which is legally protected information.

"Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress' judgment, ought to remain private," the opinion said.

In *Horizon Healthcare Services* a group of customers sued Horizon alleging the health insurer failed to protect their personal information after two unencrypted laptops containing customer information were stolen from the company.

The 3rd Circuit reversed the district court's determination that none of the plaintiffs had suffered a cognizable injury because they did not allege that the information had been misused.

The court held that the plaintiffs' allegation that Horizon disclosed their information (by way of the stolen laptops) constituted a de facto injury under the Fair Credit Reporting Act, 15 U.S.C.A. § 1681.

The appellate court pointed out that Congress had established that this kind of disclosure causes injury in and of itself, regardless of whether there was a corresponding increase in the risk of identity theft or other harms.

Overall, putative classaction plaintiffs who allege statutorily defined injuries may be better positioned to survive standing challenges if they can argue that Congress' intent in passing the corresponding legislation (or, perhaps, in passing other similar legislation) was prevention of that injury.

STATE COURT OR FEDERAL COURT?

Another option for shoring up standing is to forgo federal court altogether.

Some state courts are preferable to federal court with respect to the issue of standing in the privacy litigation context, while other states' notion of standing aligns with the federal perspective. California would be an example of the former.

In *Jasmine Networks Inc. v. Superior Court*, 180 Cal. App. 4th 980 (Cal. Ct. App., 6th Dist. 2009), the California Court of Appeal held that Section 367 of the state's Code of Civil Procedure, Cal. Civ. Proc. Code § 367, does not impose a standing requirement analogous to that of Article III. Rather, California's standing analysis arises where a plaintiff attempts to assert the rights of third parties.

Illinois, on the other hand, has standing requirements that are substantially similar to those for Article III standing. *Maglio v. Advocate Health & Hosps. Corp.*, 40 N.E. 3d 746 (Ill. App. Ct., 2d Dist. 2015).

The Michigan Supreme Court struck down a common law standing regime analogous to Article III standing in 2010. Instead, the court said the only requirement for a plaintiff to have standing in state courts is a legal cause of action. *Lansing Schs. Educ. Ass'n v. Lansing Bd. of Educ.*, 792 N.W. 2d 686, 699 (Mich. 2010).

Another factor to consider is the existence of state statutes that may more clearly encompass the alleged harm than existing federal laws.

GLOBAL CONSIDERATIONS

One of the tenets of the center-far-right populisms gaining popularity in some Western democracies (including the U.S.) is to look more inward than outward.

Under these circumstances, cooperation between nations may not be feasible, or may face incipient delays — sometimes inadvertently.

This makes it increasingly important to adopt a single universal standard, since, even if the flow of people is limited by changes in national policies, the flow of information between nations is virtually unstoppable.

Commonality avoids problems further down the road with inconsistent, unanticipated privacy issues that blindside consumers.

Given the explosion in data volumes, the potential for having to face unknown and unpredictable liabilities arising out of data breach litigation, and the practical, virtually unavoidable need to move data between jurisdictions, companies have strong incentives to develop a viable framework around these issues.

ACTION ITEMS

In an environment where every organization is susceptible to data breaches, complete prevention appears to be an unrealistic goal from a technical perspective.

Organizations, however, should ensure that their approach to data is defensible.

The more well-governed your data environment is, the better it will be at enabling rapid response to data breaches.

The recent Cloudbleed vulnerability exemplifies this idea. Cloudflare is an obscure but crucial internet infrastructure company that serves millions of websites. The platform inadvertently inserted data about six million customers from sites such as Fitbit, Uber and OkCupid, onto the pages of a smaller subset of users. The vulnerability remained open for six months.

It must be presumed that organizations like Cloudflare are at risk for a data breach, and as such, the focus must shift to detecting breaches, minimizing the number of people affected, and having a process in place for reporting and remediation.

In addition to careful planning, defensible data breach readiness requires practice.

Organizations should perform simulated exercises to identify any weaknesses in process or policy, and enable key employees to rehearse how they will respond to a data breach, including legal, public relations, information technology and administrative personnel, and the chief information officer.

Depending on an organization's needs, these activities can be contained, table top-based read-throughs or all-day sessions.

Such an exercise requires an open atmosphere, where criticism is constructive and appropriate, feedback is taken seriously, and everyone is prepared to learn from what happens in order to remedy any gaps in practice or policy.

In order to narrow the focus of these meetings and make them more digestible, companies might consider holding different sessions based on function or role and then hold a single team session at the end that is of shorter duration.

Though it is impossible to completely avoid data breaches, there is much that organizations can do to limit the risk.

Employing a defensible approach puts companies in the best possible position given the unpredictable nature of data security threats and the environment in which breaches will be litigated.

This article first appeared in the July 28, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Karl Siganporia recently served as corporate counsel for ZL Technologies. He can be reached at gc@voxpopuli.co.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.