Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lessons For Data Breach Lawyers From Product Liability

By **Michael Ruttinger** (January 26, 2018, 11:09 AM EST)


Michael Ruttinger

On its surface, the explosion of interest in data breach and privacy litigation promises a cutting-edge new field, with innovative legal issues and challenges that evolve almost as rapidly as the technologies on which the cases are based. Yet like those technologies, the issues data breach lawyers face are built on what came before and serve as a reminder of Judge Posner's adage, "law lags science; it does not lead it." Rosen v. Ciba-Geigy Corp., 78 F.3d 316, 319 (7th Cir. 1996).

There are numerous lessons that lawyers in data breach litigation can learn from their contemporaries in more established fields such as product liability, where the law has developed well-established approaches to many of the same issues that will arise in the merits stage of data breach cases.

Overlap Between the Worlds of Data Breach and Product Liability Litigation

Although the facts underlying data breach cases speak to the pace of technology, the law applicable to such cases moves much more deliberately. Nowhere is this clearer than in the scenario where a data breach victim brings a lawsuit against the business that collected and stored his or her private, personal information, which was then exposed in a subsequent breach.

Although most states have enacted data-breach notification statutes, such laws only speak to notice obligations towards the victims of a data breach; they do not yet provide remedies for consumers who allege that a company's security was too lax or who fault the company for its breach-response or loss-mitigation strategies.

For those potential plaintiffs, the primary causes of action are the very same ones familiar to product liability lawyers — negligence, breach of warranty or violation of a state consumer protection statute. And that means the defenses, too, are ones that have been well-honed and refined by a generation of product liability lawyers.

Contesting the "Duty" Element in a Data Breach Case

Negligence is the primary, and most frequently asserted, cause of action in the majority of data breach cases, which means that one of the first questions any data breach lawyer will confront is the familiar question of "is there a duty?" The answer will vary from jurisdiction to jurisdiction, and while it is

reasonable to assume courts will be more likely to recognize a duty to protect against breaches of consumer privacy as hacks become more common, many courts are not yet there.

For example, the Northern District of Georgia in 2013 refused to recognize negligence claims premised on a 2012 hack of an electronic transaction processing service, which compromised some consumers' credit card information, reasoning that "courts have found that no duty of care exists in the data breach context where, as here, there is no direct relationship between the plaintiff and the defendant." Willingham v. Global Payments Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013).

And as recently as January 2017, the Superior Court of Pennsylvania affirmed dismissal of negligence claims premised on the exposure of some 62,000 University of Pittsburgh Medical Center employees' personal information, including Social Security numbers and bank information, after concluding that several factors, including social utility and the public interest, weigh against recognizing a "duty of reasonable care in its collection and storage of the employees' information and data." Dittman v. UPMC, 154 A.3d 318, 322-23 (Sup. Ct. Pa. 2017).

Those who believe that the news cycle and public awareness over data breaches may affect the evolution of a data breach-related "duty" will be particularly interested by the Supreme Court of Pennsylvania's decision to allow an appeal from the Dittman decision on Sept. 12, 2017 — only five days after Equifaxannounced a breach potentially impacting more than 143 million U.S. consumers.

Even where a duty exists, the inquiry may not stop there. As product liability lawyers know, courts have recognized numerous defenses and exceptions to negligence claims even where the defendant did owe a duty of reasonable care. One such example is the economic loss doctrine, which precludes a plaintiff from recovering in negligence when the alleged damages are purely economic, unaccompanied by physical or property damage.

In 2008, the Third Circuit applied this doctrine to bar negligence claims in data breach litigation, concluding that the costs incurred by a credit card issuer to issue new cards and reimburse cardholders for fraudulent charges after a merchant's computer system had been hacked were not "loss of property." Sovereign Bank v. BJ's Wholesale Club Inc., 533 F.3d 162, 176 (3rd Cir. 2008).

Other courts, however, have recognized that the economic loss doctrine varies from state to state, and may not bar negligence claims based on purely economic damages where a "special relationship" of confidentiality or fiduciary responsibility exists. See In re Target Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1172-76 (D. Minn. 2014).

The Summers v. Tice Causation Problem Revisited

Another lesson straight from the world of product liability that may prove useful for data breach lawyers is the issue of alternative causation. Many product liability lawyers remember Summers v. Tice, 33 Cal. 2d 80 (1948) — the "hunting mishap" case — from their earliest days of law school.

Three companions went on a quail hunting excursion gone suddenly awry when two of the hunters shot at the same bird, missed and injured the third hunter. The court famously acknowledged that it was impossible for the plaintiff to prove which of his companions was responsible, and so shifted the burden onto the defendants to absolve themselves from joint liability. See id. at 88.

In the world of product liability, courts have long accepted the doctrine of alternative liability in cases "where the precise identification of a wrongdoer is impossible." Girau v. Europower Inc., No. 10 Civ. 4320 (NSR), 2017 WL 4124340, at *5 (S.D.N.Y. Sept. 14, 2017) (internal quotation omitted).

To date, causation questions in data breach litigation have been primarily confined to the pleadings stage. Many such cases have been resolved on motions to dismiss, where the defendants have successfully argued that a consumer whose information may have been exposed in a data breach, but has not incurred any pecuniary harm, lacks the requisite "injury in fact" needed to establish Article III standing to sue. See, e.g., Whalen v. Michaels Stores Inc., 689 F. App'x 89 (2d Cir. 2017).

Other courts, like the Eleventh Circuit in Resnick v. AvMed Inc., 693 F.3d 1317 (11th Cir. 2012) have held a data breach plaintiff's allegations sufficient where they "include allegations of a nexus between the two instances beyond allegations of time and sequence." Id. at 1326-27.

This "nexus test" is representative of a trend that appears increasingly forgiving of the "injury in fact" requirement as data breaches become more and more common. See, e.g., Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (2015) ("It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level.").

But as data breach litigation matures, alternative causation issues are certain to play a critical role in resolution of these cases at the merits stage. In reality, most consumers have had at least some of their personal information exposed in numerous data breaches, and so causation issues may require a comprehensive review of the plaintiff's own financial history.

Even under the Eleventh Circuit's "nexus" test for establishing standing, courts have recognized that "proving this nexus may require a review of any prior thefts of each class member's identity." Smith v. Triad of Alabama LLC, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *14 (M.D. Ala. Mar. 17, 2012) (emphasis added).

Defendants may argue that plaintiffs must "show that their injuries are traceable to the data incursion at the company rather than to one of several other large-scale breaches that took place around the same time" — an argument that the Seventh Circuit noted was "reminiscent of Summers v. Tice." Remijas, 794 F.3d at 696. Just so, it would not be surprising if courts apply the alternative causation rules in cases where multiple companies may have exposed the plaintiff's private information to a breach. Id.

Strict Liability and the Internet of Things

While this article focuses on lessons that data breach lawyers may apply from the world of product liability, it is worth considering that the intersection of these two fields may be closer than anyone thinks.

This holiday season more consumers than ever brought "smart" devices into their homes — from televisions to appliances to baby monitors. This rapidly expanding network of devices intended to streamline and automate our lives have led many to conclude that we are living in an era referred to as the "Internet of Things." The concept, simply, focuses on how computers, sensors and objects interact with each other and collect information relating to their surroundings, including a wide array of private personal information.

When smart devices are hacked or controlled by third parties, damage can extend beyond just the exposure of private information; a hacked electronic thermostat, for example, could lead to frozen or burst pipes and water damage. The still nascent law surrounding data breaches is ill-equipped to remedy such harms, but product liability law is well-positioned to fill in the gaps.

For example, many smart devices may be vulnerable because they are configured to be administered with default credentials, which can in turn be identified and accessed by malicious hackers. See Zach Wikholm, "When Vulnerabilities Travel Downstream," FLASHPOINT BLOG (Oct. 7, 2016), https://www.flashpoint-intel.com/blog/cybercrime/when-vulnerabilities-travel-downstream/.

Aware of this, a manufacturer who fails to take basic precautions to change these settings could be deemed liable for selling a product with a "defective design," which is actionable in strict liability in many jurisdictions. This approach too has its challenges — among others, courts would need to consider what sort of test ("consumer expectations" or "risk-utility" for example) to apply. But the point is that as the "Internet of Things" expands data breach lawyers will have much to learn from product liability litigators.

Michael J. Ruttinger is of counsel at Tucker Ellis LLP in Cleveland, Ohio, and handles appellate, class action, commercial and complex litigation in state and federal courts across the country.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.