No Standing

Recent Indiana Court of Appeals' Ruling May Benefit Data Breach, Class Action Defendants

By Judy Okenfuss, Stephen Reynolds, and Jenny Buchheit

Doe v. Adams, et al., 53 N.E.3d 483 (Ind. Ct. App. 2016), could be helpful to defendants involved in privacy litigation in Indiana.

The Indiana Court of Appeals recently found that a putative class action plaintiff, whose main basis for filing suit was a privacy interest in a previously taken blood sample, had no standing to maintain her lawsuit. This decision, *Doe v. Adams, et al.*, 53 N.E.3d 483 (Ind. Ct. App. 2016), *trans. denied*, could be helpful to defendants involved in privacy litigation in Indiana, including those involved in data breach and class action lawsuits.

Doe's lawsuit stems from Indiana's newborn screening program, which requires hospitals to take blood samples from every infant born under their care, and it is aimed at identifying, treating, and preventing serious conditions and diseases in infants. The sample, usually obtained by heel stick, is collected through a method referred to as "dry blog spot" (DBS), sampling, in five circles on a newborn screen card (the DBS sample), which is then transported to a designated lab for testing. The lab performs the testing by punching out small portions from the DBS sample. Often, not all of the five circles are used. From approximately 1991 to June 2013, the Indiana State Department of Health (ISDH) retained and stored the remaining portion of the newborn screen card. In June 2013, however, the ISDH changed its storage and retention policies, enabling parents or guardians of newborns either to allow the DBS sample to be used for medical research purposes for a three-year period and then destroyed, or be kept for a period of six months (to ensure further testing was not necessary) and then destroyed.

Doe, through her parents, filed a class action complaint and request for emergency



■ Judy Okenfuss is a managing partner of Ice Miller in Indianapolis and chair of the firm's Internet of Things Practice. She focuses her practice in defending manufacturers, distributers, and retailers against all types of litigation, including class actions. Stephen Reynolds, a former computer programmer and IT analyst, is a partner in Ice Miller's Litigation and Intellectual Property Group and co-chair of Ice Miller's Data Security and Privacy Practice. Jenny Buchheit is a partner in Ice Miller's Litigation and Intellectual Property Group, who represents clients at both the trial and appellate levels and focuses much of her work on defending companies in both state and national putative class actions.

declaratory and injunctive relief against ISDH. Doe sought to represent a class of "[a]ll individuals who had a blood sample taken pursuant to [Indiana's newborn blood screening program] that has been or will be stored by the [ISDH] for more than six months without any documentation of consent," asserting claims under the United States Constitution, the Indiana Constitution, and Indiana state law. The trial court dismissed Doe's complaint, finding, in part, that Doe lacked standing to maintain the lawsuit. Specifically, the trial court found that Doe lacked standing because (1) she had not sustained and was not in imminent danger of sustaining some direct injury as a result of the act of storing her DBS sample, (2) she had not made any request for destruction of her DBS sample that had been denied by ISDH, and (3) any injury is "completely speculative." On appeal, Doe argued that she had standing because "ongoing governmental violations of the Fourth, Fifth, and Fourteenth Amendments to the Constitution constitute an immediate danger of sustaining some direct injury." Doe also maintained that she had a reasonable privacy interest in her DBS sample, which contained her DNA, and the ISDH's continued storage beyond the time necessary to conduct the screening tests violated the Fourth Amendment's protections against unreasonable searches and seizure. According to Doe, "the essential question… is whether the person asserting a violation has a reasonable expectation of privacy in the material examined."

The Indiana Court of Appeals disagreed. Assuming, but not finding, that Doe had a constitutionally protected interest in her DBS sample, the court found that Doe still must show that she has suffered, or is in immediate danger of suffering, some direct injury to have standing. The Indiana Court of Appeals rejected Doe's assertion that she had a reasonable fear that her DBS sample might be misused, citing record evidence that Doe's blood was not used for medical research, nor would it be, without parental authorization. Under the facts of the case, Doe's fear was merely speculative and did not constitute the type of direct injury necessary to support a finding of standing.

This decision could be helpful to class action defendants in a number of respects. First, the Indiana Court of Appeals rejected Doe's attempts to rely on the alleged harm to the putative class to prove that her case should not be dismissed. Because the class had not yet been certified, the court found that only Doe's claims were at issue, citing *Arthur and Withered*, 11 Ind. Prac., Civil Trial Practice §18.4 (2015). *See also Alexander v. PSB Lending Corp.*, 800 N.E.2d 984, 991-92 (Ind. Ct. App. 2003) (rejecting plaintiffs' argument that standing may be determined on classwide basis), *trans. denied.*

Second, the Indiana court found that a mere privacy interest is not enough to demonstrate standing: a plaintiff must still show a direct injury, or an immediate danger of direct injury, to have standing to bring his or her claim. Such a holding could be helpful to defendants in data breach class actions. While Indiana has little case law to provide guidance in the developing data security realm, defendants could argue that data breach plaintiffs—who often claim that they have an increased risk of fraudulent charges or identity theft, but do not actually suffer such injuries—do not have standing to maintain individual or class actions under Indiana state law against companies who experience a data breach.

Given the Seventh Circuit's recent decisions in this regard, which have seemingly relaxed the standing requirement for plaintiffs, the *Doe* decision could be very useful for defendants facing data breach lawsuits in Indiana state courts. Similar to Indiana's standing requirement, a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision" to maintain a federal lawsuit. *Hollingsworth v. Perry,* ___ U.S. ___, 133 S. Ct. 2652, 2661 (2013). Defendants in the Seventh Circuit have argued that plaintiffs who were merely exposed to a data breach have not met the "concrete and particularized injury" requirement. The Seventh Circuit has repeatedly disagreed. In doing so, the Seventh Circuit has found that the increased risk of fraudulent credit card or debit charges, and the increased risk of identity theft, were "sufficiently imminent future injuries" to support standing. The Seventh Circuit also held that the time and money spent by class members resolving fraudulent charges is an injury sufficient to support standing. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015). More recently, in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), the plaintiffs contended that they suffered damages as a result of an acknowledged data breach. However, unlike the defendant in *Neiman Marcus*, P.F. Chang's determined that the data breach only affected customers of certain locations, none of which were visited by the named plaintiffs. Despite this distinction, the Seventh Circuit held there was standing for all customers. The court noted that when the data breach was first discovered, P.F. Chang's reported that it affected all locations and took steps to switch all locations to a manual procedure temporarily during its investigation. Although subsequent analysis allowed P.F. Chang's to determine that only 33 locations were involved, the restaurant's initial actions created a question of fact sufficient to support standing for customers of all locations. By allowing these actions to support standing for all customers, not just those at the affected locations, the Seventh Circuit has demonstrated an openness to expanding standing in data breach actions. This expansion would seemingly conflict with the Indiana court's holding in *Doe*, which requires a specific showing of injury on the part of the named plaintiff—separate from the injury alleged on behalf of the putative class.

Defendants in the Seventh Circuit have argued that plaintiffs who were merely exposed to a data breach have not met the "concrete and particularized injury" requirement. The Seventh Circuit has repeatedly disagreed.