BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Damages

Privacy Litigation

In the absence of actual identity theft or other quantifiable harms, courts have declined to recognize amorphous emotional or dignitary harms from privacy violations as being sufficient to support standing or prove damages as a necessary element of a cause of action. This article by attorneys at Sidley Austin LLP assesses the impact of conflicting cases and observes that the majority trend has focused on compensation of concrete harms for privacy violations.

Damages for the Harm of Data Breaches and Other Privacy Claims

BY ALAN CHARLES RAUL, EDWARD MCNICHOLAS AND JENNIFER TATEL

Alan Charles Raul and Edward McNicholas are partners and Jennifer Tatel is an associate in the information law and privacy practice of the Washington office of Sidley Austin LLP. This article is published for informational purpose only and is not legal advice. Readers should not act upon this article without seeking advice from professional advisers. The views expressly herein are those of the authors personally and do not necessarily reflect the views of any governmental or private entity, client, or association.

Quantifying the value of privacy has proved a difficult task for the law. Sometimes this issue is clear—a job has been lost, costs incurred, or a contract breached. Particularly in the context of data breaches, however, the harm of a violation of privacy is often solely the public disclosure of some private piece of information. Repeatedly, in the absence of actual identity theft or other quantifiable harms, courts have declined to recognize amorphous emotional or dignitary harms from privacy violations as being sufficient to support standing or prove damages as a necessary element of a tort cause of action. This article assesses the impact of conflicting cases on this crucial question for the future of privacy litigation, and it observes that the majority trend has focused on compensation of concrete harms for privacy violations. Accordingly, courts have generally required proof of special or actual, eco-

 ISSN 1538-3423

nomic damages in data breach litigation, as opposed to allowing general damages to be presumed for nebulous harms to privacy interests.

Just recently, in August 2008, the U.S. District Court for the Northern District of California provided a clear example of this trend of requiring what are essentially special (i.e., economic) damages when it denied damages under the Privacy Act to a man who suffered mental distress from a federal agency's disclosure of his HIV status. *See Cooper v. Federal Aviation Admin.*, No. 07-1383 (N.D. Cal. Aug. 22, 2008) (7 PVLR 1309, 9/8/08). In doing so, the court addressed a key issue that the U.S. Supreme Court left open in *Doe v. Chao*, 540 U.S. 614 (2004) (3 PVLR 235, 3/1/04), namely, what constitutes ''actual damages'' that are compensable under the Privacy Act. In reaching this issue, the district court observed that the courts of appeals have split over the issue of whether the emotional harm occasioned by a breach of the Privacy Act constitutes compensable ''actual damages.'' *Compare Fitzpatrick v. IRS*, 665 F.2d 327 (11th Cir. 1982) (holding ''actual damages'' to include only ''proven pecuniary losses and not for generalized mental injuries, loss of reputation, embarrassment or other non-quantifiable injuries.'') with *Johnson v. Department of Treasury*, 700 F.2d 971 (5th Cir. 1983) (holding that ''actual damages'' include mental injuries); *see also Albright v. United States*, 732 F.2d 181, 186 (D.C. Cir. 1984)), ''emotional trauma alone is sufficient to qualify as an 'adverse effect' under Section 552a(g)(1)(D) of the [Privacy] Act.'').

In *Cooper*, the district court noted that the Ninth Circuit considers emotional distress and humiliation as ''actual damages'' under other statutes, particularly the Fair Credit Reporting Act, 15 U.S.C. § 1681 (citing *Guimond v. Trans Union Credit Information Co.*, 45 F.3d 1329, 1332-33 (9th Cir 1995)). Nonetheless, the court felt compelled to deny legal recognition to the mental anguish of having one's HIV status disclosed because it did not constitute ''actual damages'' under the court's reading of the Privacy Act, in part based on the principle that waivers of sovereign immunity should be construed narrowly.

Common Law Damages for Privacy Harms

In reaching this result, however, the district court reflected the larger debate about whether special or general damages should be compensable for privacy harms, and whether, if general damages are to be awarded, some special harm must first be demonstrated. This rejection of qualitative, general damages contrasts with the historical, common law development of privacy torts.

In Warren and Brandeis' seminal article on the subject, for example, the authors observed that

> [t]he remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely: 1. An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel. 2. An injunction, in perhaps a very limited class of cases.

Samuel D. Warren & Louis D. Brandeis, ''The Right to Privacy,'' 4 *Harv. L. Rev.* 193, 219 (1890) (footnote omitted). Significantly, the availability of a damages remedy for harms to privacy—compensation for ''injury to feelings as in the action of slander or libel''—was indeed preferred to equitable relief, such as injunctions, which were to be available in ''a very limited class of cases.''

The measure of such damages was ill-defined even then, however, and Warren and Brandeis were left to reference literary and artistic property, which we now consider to be covered by the much more well-developed protections of copyright law. As the Supreme Court noted in *Doe v. Chao*, privacy torts have traditionally involved presumed, general damages that are ''a monetary award calculated without reference to specific harm'' (citing *inter alia Restatement of Torts* § 621, Comment d (1939) (damages are available for privacy torts ''in the same way in which general damages are given for defamation,'' without proof of ''pecuniary loss [or] physical harm' '').

Consistent with this common law approach, some U.S. courts have recognized that the harms of misuse of personal information are themselves worthy of compensation in certain circumstances. The New Hampshire Supreme Court, for example, reflected this tradition by observing that the long-standing common law privacy torts do not require evidence of harm beyond the bare invasion of privacy itself. *Preferred Nat'l Ins. Co. v. Docusearch, Inc.*, 829 A.2d 1068, 1075 (N.H. 2003). Indeed, in the Restatement formulation, an ''action for intrusion upon seclusion does not require a claimant to prove any harm beyond the intrusion itself.'' *Id.* (*citing* Restatement (Second) of Torts § 652H cmt. a at 402 (1977) (''[O]ne who suffers an intrusion upon his solitude or seclusion . . . may recover damages for the deprivation of his seclusion'')).

More recently, a New York appellate court upheld a substantial damages award to a woman whose parents had been accidentally told of her abortion. *See Randi A.J. v. Long Island Surgi-Center*, 842 N.Y.S.2d 558, 566-67 (N.Y. App. Div. 2007) (6 PVLR 1592, 10/15/07) (holding that a medical center's releasing of confidential information regarding an abortion to a patient's mother after the patient specifically requested not to be contacted at home supports a punitive damages award under various tort theories); *see also Pulla v. Amoco Oil Co.*, 882 F. Supp. 836 (S.D. Iowa 1995) (awarding $2 in actual damages and $500,000 in punitive damages based on improper credit card access under invasion of privacy).

The Absence of a Damages Remedy for Data Breaches

The Supreme Court in *Doe v. Chao*, also noted that, even at common law, general damages were available for certain dignitary torts, such as defamation, ''only when a plaintiff first proved some 'special harm,' *i.e.*, 'harm of a material and generally of a pecuniary nature.' '' Accordingly, it is also accurate to characterize the common law as allowing presumed, general damages to redress amorphous dignitary injuries, as *Chao* opined, ''only if they [the plaintiffs] could demonstrate some actual, quantifiable pecuniary loss.''

In an era of substantial computer data breaches, the majority trend has decidedly turned away from finding damages based upon the ''mere'' exposure of personal information when proof of quantifiable pecuniary loss is absent. The data breach privacy cases of the last several years have rejected any analogy to medical monitoring or environmental contamination cases, where the mere risk or fear of increased harm is often considered sufficient ''damage'' to support a cause of action.

  PVLR ISSN 1538-3423

See, e.g., *Theer v. Philip Carey Co.*, 628 A.2d 724, 733 (N.J. 1993) (allowing monitoring damages based on an increased risk of illness directly related to an exposure). Instead, numerous data breach cases have held that a mere risk of harm occasioned, for instance, by having information on a lost backup tape, is too speculative to support a cause of action.

The data breach privacy cases of the last several years have rejected any analogy to medical monitoring or environmental contamination cases, where the mere risk or fear of increased harm is often considered sufficient "damage" to support a cause of action.

Unless a statute provides for liquidated damages, it is entirely unclear whether any plaintiff would be able to demonstrate any independent quantifiable harm in the absence of actual identity theft. Ethereal fears have not been considered concrete enough to support legal relief. Emblematic of this trend is the decision in *Conboy* v. *AT&T Corp.*, 241 F.3d 242 (2d Cir. 2001), in which the U.S. Court of Appeals for the Second Circuit held that transfers of personal information collected by a company do not necessarily cause injury or give rise to cognizable damages. The court entertained no presumption of emotional distress or other similar damages from the disclosure of personally identifiable information, absent some concrete evidence of demonstrable harm. Thus, the corporate defendant prevailed over plaintiffs who claimed it had improperly distributed their customer proprietary network information to a credit card affiliate in order to assist in debt collection.

Other courts have followed the trend of *Conboy*, holding that mere dignitary harm of intrusion is insufficient to establish an injury in fact. *In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp.2d 299, 326-28 (E.D.N.Y. 2005), the court held that the passengers' alleged loss of privacy as result of the airline's transfer of their personal information to a data mining company was not a damage available in a breach of contract action, and passengers did not otherwise establish an actual injury sufficient to sustain a claim against the airline for trespass to chattels. In *Smith v. Chase Manhattan Bank*, 293 A.D.2d 598 (N.Y. App. 2002) (1 PVLR 490, 4/29/02), the court rejected several common law causes of action after a bank promised its customers that it would not sell their personal information to third parties, but then did so, including to a telemarketing firm. The court's rejection was based on the lack of purported 'harm' in the offering of products and services that plaintiffs were free to decline. *Id.*

In the data breach context, several courts have held that the mere risk of harm due to loss of personal information is not actionable injury sufficient to confer standing. *See, e.g.*, *Randolph v. ING Life Insurance & Annuity Co.*, 486 F. Supp.2d. 1 (D.D.C. 2007) ; *Bell v. Acxiom Corp.*, No. 06-485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (5 PVLR 1431, 10/16/06); *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006) (5 PVLR 1470, 10/23/06); *Giordano v. Wachovia Sec., LLC*, No. 06-476, 2006 WL 2177036 (D.N.J. July 31, 2006). Other ''lost data'' cases have been decided at the summary judgment stage, again because the mere risk of identity theft as a result of lost or stolen data is not a recognized ''injury.'' *See, e.g., Stollenwerk v. Tri-West Healthcare Alliance,* 254 Fed.Appx. 664 (9th Cir. 2007) (6 PVLR 1825, 12/3/07) (finding no standing for plaintiffs who offered no proof of identity theft or other pecuniary harm); *Guin v. Brazos Higher Ed. Serv. Corp.*, No. 05-668, 2006 WL 288483 (D. Minn. 2006) (5 PVLR 233, 2/20/06); *Forbes* v. *Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018 (D. Minn. 2006) (5 PVLR 628, 5/1/06).

The Possible Resurgence of General Dignitary Damages in Data Breach Cases

Two more recent cases, including the first published federal appellate decision on the issue in the context of a data breach, may suggest a reversion to the minority trend of presuming general damages. Most significantly, in *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (6 PVLR 1374, 9/3/07), a bank operated a marketing Web site on which potential customers can complete online applications, some of which required the submission of personal information. This information was stored on the bank Web site and was maintained by a hosting facility, which in 2005 experienced a ''sophisticated, intentional, and malicious'' security breach. Plaintiffs claimed that the bank and its processor were negligent in the maintenance of personal information on the Web site, which caused them to suffer ''substantial potential economic damages and emotional distress and worry'' about an enhanced possibility of identity theft. Plaintiffs alleged no ''direct financial loss to their accounts as a result of the breach, nor did they claim that they or any other member of the putative class already had been the victim of identity theft as a result of the breach.'' Rather, plaintiffs alleged that they ''incurred expenses in order to prevent their confidential personal information from being used and will continue to incur expenses in the future.'' The district court concluded that plaintiffs' claims failed as a matter of law, in part because the credit monitoring and other costs incurred by the plaintiffs to prevent ''a future injury'' are not ''damages.'' Without a concrete, cognizable damages claim, the district court was compelled to dismiss the negligence claims because, as a matter of Indiana law, plaintiffs could not state a claim for ''potential damages.''

Although the U.S. Court of Appeals for the Seventh Circuit ultimately affirmed the district court, in doing so, the Court disagreed with several district courts and considered the mere fear of future identity theft to be consequential enough to establish an injury-in-fact for Article III standing. The Court of Appeals held that a threat of future harm is sufficient to give plaintiffs standing to bring their claims, noting without much analysis that this conclusion was in conflict with the ''no standing'' decisions of a number of district courts (several of which are mentioned above).

The Court then looked to the negligence standard under applicable Indiana state law, asking the threshold question of whether Indiana ''would consider that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing compensable injury and conse-

quent damages required to state a claim for negligence or for breach of contract.'' The Court answered that question in the negative, finding no statute or case law precedent to support a cause of action for such alleged injuries.

Under its analysis, the Indiana data breach notification statute requires mere notice, and, therefore, provided no support for the conclusion that monitoring expenses constitute a compensable injury. Moreover, the data breach notification provides that only the state's attorney general may bring suit in the event that statute is not followed; no cause of action exists for affected customers. Absent a clear statement of legislative intent, the Court determined that consumers' monitoring costs associated with a data breach are alone not a compensable injury. Although primarily grounding its ruling in Indiana law, the Court also emphasized that its holding is consistent with the refusal of other federal courts to recognize credit monitoring costs as a compensable injury. The Court reviewed the existing data breach case law and found that all of the cases ''rely on the same basic premise: Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.''

The logic of *Pisciotta* was later followed in *Ruiz v. Gap, Inc.*, No. 07-5739 (N.D. Cal. Mar. 24, 2008) (7 PVLR 634, 4/28/08), in which a district court held that a mere increased risk of identity theft as a result of a security breach, without any allegation of actual or imminent harm, is sufficient to confer at least preliminary standing on a plaintiff. In 2007, laptop computers containing the unencrypted personal information of approximately 800,000 Gap job applicants were stolen from a third-party recruiting contractor. Upon learning of this breach, Ruiz, who had submitted an online application for employment at one of Gap's retail stores in late 2006, filed a class action complaint asserting several privacy-related causes of action. In an order that contained little analysis and did not address any analogous security breach cases, the court ruled that Ruiz had preliminary standing to maintain certain of his claims.

At the outset of its standing analysis, the court noted that the only harm alleged in the complaint was that the security breach increased Ruiz's risk of identity theft; Ruiz did not claim that his identity was in fact stolen. The court observed that, to possess standing, a plaintiff must allege an ''injury in fact'' that is '' 'actual or imminent, not conjectural or hypothetical.' '' *Ruiz*, No. 07-5739, slip op. at 5 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). While acknowledging that Ruiz's claim that he was at increased risk for being a victim of identity theft at some unspecified future point ''seem[ed], at first blush, conjectural or hypothetical, rather than actual or imminent,'' *id*. at 6, the court nonetheless felt bound to ''presume 'that general allegations embrace those specific facts that are necessary to support the claim,' '' *id*. (quoting *Lujan*, 504 U.S. at 561). The court therefore concluded that, for purposes of a motion for judgment on the pleadings, Ruiz possessed sufficient standing to pursue his claims. Although the court also did not specify what specific standing requirements would apply on a motion for summary judgment, the court did, however, preserve the possibility that Ruiz may be found to lack standing in a later phase of the proceedings, should his alleged injury ultimately appear ''too speculative or hypothetical.'' *Id*. Having resolved the issue of standing in Ruiz's favor, the court went on to rule that Ruiz could maintain his claim that Gap was negligent in failing to protect job applicants' personal data as well as other claims.

The Future of Damages for Privacy Violations

At present, it appears that courts will continue to require proof of special damages or injury in data breach cases. Merely being a part of the group exposed to a data breach has not normally been deemed adequate to establish a case of action, but a reversion to presumed, general damages is certainly possible. Resolution of the issue will no doubt be significant for corporations assessing the overall risks of vexatious litigation based on the loss of personal data under circumstances where actual harm is highly unlikely. Similarly, the potential for substantial damages when there are real harms should continue to provide robust incentives to corporations while designing privacy compliance programs.

  PVLR ISSN 1538-3423