ANDREWS LITIGATION REPORTER

THOMSON WEST

Privacy

COMMENTARY

REPRINTED FROM VOLUME 5, ISSUE 2 / OCTOBER 2007

Lawsuits Based on the Loss of Personal Information: Lots of Questions, Few Answers

By W. Randall Bassett, Esq., Matthew S. Harman, Esq., and Michael Weiss, Esq.

For more than a century, both statutory and common law have recognized that a cause of action may arise when a person's private information is wrongfully revealed or misused.[1] Historically, these "privacy torts," such as breach of confidence, public disclosure of private facts or false-light publicity, have arisen when a single plaintiff claims her privacy was violated because of the disclosure of her personal information.[2] While general principles of negligence may apply to such actions, more frequently, the privacy torts do not consider the reasonableness of the person's actions in disclosing the information, but instead focus on the impact of the disclosure on the affected person. These torts, moreover, were rarely encountered by most practitioners due to their unique application.

The electronic collection of personal information, however, is transforming these obscure torts and reinvigorating them in a way that all practitioners may encounter them in the future. Government agencies and businesses now maintain confidential information, including financial and medical data, concerning millions of people. Because that information may be maintained on a single storage device that could be lost, stolen or hacked into, private information about millions of citizens may find its way into the hands of a third party – instantaneously. Not only is the loss of personal information offensive to the person who entrusted it to another, the information can be used in a variety of unsavory ways to harm that individual, the most publicized being identity theft.[3]

In the past few years there have been a number of highly publicized incidents in which consumers' confidential personal information was misappropriated or misplaced. Two years ago a box of computer tapes that disappeared during shipping forced CitiFinancial to go public with the news that it had misplaced account information and Social Security numbers for nearly 4 million people.[4] Also in 2005 a laptop stolen from an unlocked office at the University of California at Berkeley led the university to warn 98,000 students and applicants that their Social Security numbers may have been compromised.[5] And earlier this year the company that runs the T.J. Maxx and Marshalls discount stores revealed that nearly 46 million credit card numbers were stolen by hackers who had been accessing the company's computer system for years.[6]

Due to the sheer numbers involved, mass data breaches present the potential for complex, protracted and expensive litigation. As traditional class actions have demonstrated, particularly those involving a state's consumer-protection law, otherwise minimal damages can be considerable when multiplied by large numbers of people, providing an incentive for plaintiffs' attorneys to litigate even when the private information was never abused by a third party.

At the same time, states seeking to protect consumers have enacted laws that limit how confidential information must be maintained. While commendable in trying to protect an individual's personal information, such laws may have the consequence of creating a "standard of care," giving plaintiffs a roadmap for arguing that a company was negligent in the loss of consumer data.

Additionally, the advent of encrypted data raises new questions about when information has been "disclosed": If a laptop loaded with credit card and Social Security numbers – and protected by 128-bit key encryption – is accidentally left in a hotel room, has the information been "disclosed" if no one can view it? If no disclosure, can a plaintiff recover for just the loss of that information?

This article will discuss the issues that have arisen and may yet arise from litigation over the mass loss or disclosure of confidential electronic information.

Possible Causes of Action Arising From Loss of Personal Data

As these kinds of mass disclosures of confidential consumer information are a relatively new phenomenon, so too is litigation arising from these incidents. Even today, many of the cases concerning personal data security breaches involve discrete populations, such as members of a local union.[7] Yet with numerous incidents garnering public attention in recent years, nearly all involving large numbers of consumers and large corporations, one would expect enterprising plaintiffs' attorneys to find ways to redress the harm (whether real or perceived) caused by the loss of personal information. Absent a contractual relationship between the entity that maintained the data and the people whose information was lost that dictates responsibility and liability, there appear to be two ways plaintiffs can assert legal claims based on traditional principles of negligence and invasion of privacy.

Simple Negligence

Perhaps the most basic cause of action that can be asserted in a case of mass disclosure of private information is simple negligence. The elements may all be present: An entity with a duty to keep information confidential has breached that duty, proximately causing injury to its customers.[8] But as described above, it is not certain that plaintiffs can prove in every situation that the defendant even had a duty to protect the information.

Present in every negligence claim is the question of foreseeability. Traditionally, a person or entity only has a duty to guard against *foreseeable* dangers. Whether the risk of identity theft is a foreseeable consequence of a security breach may depend on the nature of the breach itself. It may be foreseeable that unencrypted data stored on a keychain flash drive could easily be lost, but it may be less foreseeable that an IT consultant would sell Social Security numbers to a credit card fraud ring.

Some courts take a broad view that there is a duty whenever the outcome or harm is foreseeable; that is, because the theft or loss of information is foreseeable, a duty arises whenever such an event occurs.[9] Other courts focus more on the mechanics of the incident in question: If the particular method of accidental disclosure was not foreseeable, the entity had no duty to guard against it.

Consumer-protection laws that require companies to take certain security precautions with confidential data may be persuasive in determining foreseeability. Likewise, if a company has written information security policies that anticipate and try to prevent such a breach – and particularly if the breach occurred because of a violation of those policies – it could be difficult for the company to argue later that the breach was not reasonably foreseeable.

Along those lines, plaintiffs suing under a theory of negligence may benefit from the existence of statutory requirements for the handling of sensitive data. If a violation of a statute allegedly led to the breach that forms the basis of the lawsuit, the plaintiffs may argue that the violation constitutes negligence per se.

But there are also disadvantages to a negligence theory of recovery. One legal defense that may be available in such cases is the economic-loss doctrine, which prohibits negligence actions when the only injury is monetary loss.[10] Several states recognize this doctrine, which limits negligence claims to plaintiffs asserting personal injury or property damages.

Plaintiffs, however, may try to maintain their action under a number of exceptions to the doctrine that are recognized in some jurisdictions. Frequently an exception is made when there is an allegation of either negligent or intentional misrepresentation.[11] To take advantage of this exception, where available, the plaintiffs would have to allege the elements of a fraud claim, particularly that they provided their personal information to the corporate defendant in reliance on a representation that the information would be adequately guarded.[12]

Negligent Infliction of Emotional Distress

As described above, consumers whose information has been disclosed may not be able to allege monetary damages. In those cases, they may try to state a claim for negligent infliction of emotional distress.[13] There are a couple of potential hurdles with this approach. First, many jurisdictions impose a number of restrictions on emotional-distress claims, such as requiring physical manifestation of injury or limiting its availability as a stand-alone tort.

Second, the individual issues of proof in asserting claims of emotional distress may make it more difficult for plaintiffs to maintain their case as a mass action or class action. Still, at least one court has acknowledged the possibility, explaining that "a plaintiff may have a cause of action for negligent infliction of emotional distress if, because private information was shared, the plaintiff suffered severe emotional distress with accompanying physical manifestations."[14]

Invasion of Privacy

The torts often grouped together under the umbrella of "invasion of privacy" are unique causes of action. They are distinct from traditional negligence claims, primarily

because the disclosure of personal information renders the defendant liable to the plaintiff, without regard to whether the defendant acted reasonably in causing the disclosure. According to the Restatement (Second) of Torts:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public.[15]

Because most would agree that personal financial and medical information is something that a reasonable person would wish to keep private,[16] whether this tort applies depends on what is meant by "publicized." Traditionally, the common law contemplated that the information must be publicized to the public at large or at least broadly enough so it could become known to a large group.[17] But that law developed in more traditional privacy cases, where the information usually concerned embarrassing facts that may damage one's reputation in the community. While the same logic may apply to misplaced or stolen medical records, when the subject of the publicized information is a secret account number, disclosure to just one person could be sufficient to cause great harm to the individual and may justify loosening this requirement.

That leads to the next question: What is necessary for information to be "disclosed"? As discussed more fully below, in many cases when information is misplaced or even stolen, there is no evidence that it was viewed by anyone not authorized to do so. Is there a disclosure when a laptop loaded with thousands of Social Security numbers is left behind in a hotel room and never returned, absent evidence that whoever took the computer ever opened the file? What if the numbers on the laptop are encrypted? What if the laptop's rightful user views the file in a coffee shop in which an enterprising customer at the next table could have accessed the data via a Wi-Fi connection, though there is nothing to indicate that he did? Many state laws require that consumers be notified when their information is misplaced in at least some of these situations, but does that mean there was an actionable disclosure? These questions remain to be settled, yet they are critical to establishing the scope and applicability of this cause of action to the digital age.

Key Questions in Cases Arising From Data Breaches

When someone makes a claim arising from the mass loss of personal data, the threshold question is whether there has been an injury for which those affected may seek relief.[18] The answer is obvious when a wrongdoer actually appropriates a victim's identity to access her credit cards or bank accounts and causes measurable monetary damages. Yet many of the missing-data incidents that have garnered national attention involve personal information that has been lost but not used improperly or necessarily even accessed. For example, in 2005 a data archiving firm hired by Time Warner misplaced – and apparently never located – data tapes containing 600,000 personal employee records it had collected for storage.[19]

Indeed, even when a large volume of personal data is lost, it is quite likely that the information is never disclosed. A thief stealing a laptop from an airport may have no interest in the contents of the hard drive, just in selling the computer hardware itself. Nor may he even be aware that the laptop contains any valuable data, especially if the information is protected, whether by encryption or a simple startup password. And even if personal information is stolen by, or ends up in the hands of, someone with the ability and motivation to use it for wrongful purposes, certainly it is possible that he will not appropriate the identity of every one of the potentially thousands of people whose data he obtains.

If a breach involving confidential personal data does result in a monetary loss, such as from a thief who uses a person's exposed credit card number, it appears that there would be an actual injury. The Minnesota Supreme Court, for example, ruled that "if the unauthorized transmission of private data actually resulted in pecuniary loss due to identity theft, a plaintiff may be able to bring a negligence action."[20] It is less clear if consequential damages that may flow from the loss of personal data – costs incurred in canceling credit cards, changing account numbers, applying for new Social Security numbers and driver's licenses, and monitoring credit reports – may be sufficient to state a claim. A plaintiff may also argue that the time required to obtain new government identification or the small outlays of money associated with obtaining new identification are actual damages subject to recovery. These amounts may be minimal for each person, but substantial when aggregated into a class action or mass action.

Courts are generally in agreement, however, that a plaintiff has not suffered an injury unless she can assert that her lost or stolen personal information has actually been accessed, and even access may be insufficient if the information has not been used for an unlawful purpose.[21] A federal court in Ohio recently noted that such claims are "based on nothing more than speculation that [the plaintiff] will be a victim of wrongdoing at some unidentified point in the immediate future."[22] Unless a plaintiff can allege that the actual theft of her identity has occurred or

offer circumstantial evidence that such an unlawful use is imminent, a claim must fail for lack of standing.[23]

But when there is no financial harm, is there still an injury? Plaintiffs who cannot claim money damages, because either there is no evidence anyone used their identities or the company responsible for losing the information reimbursed any costs, still may be able to maintain a cause of action by alleging other damages. The most obvious claim is emotional distress stemming from the loss of personal information and the *possibility* that their identities may be stolen as a result. Plaintiffs may be able to allege they were afraid that their identities would be stolen, suffered anxiety that their financial information was accessible, and/or were distressed that a stranger had seen their private information, such as medical files.

State laws that require companies to notify consumers or clients about the potential loss of confidential information, now common across the United States, make it inevitable that members of the public will learn about security breaches even if they are ultimately unaffected by them.[24] Allegations of emotional injuries like these may be subject to multiple limitations in typical tort and contract actions, including actions in negligence. Yet traditional invasion-of-privacy claims are often based solely on the distress experienced by a plaintiff about whom something personal has been made public, and the lack of monetary loss would not be an obstacle to such claims.

The next question when evaluating liability for the disclosure of personal information in tort is one of duty. Centuries of tort jurisprudence have established that the question of duty often hangs on the relationship between the plaintiff and defendant. Of course, it is quite possible that the company that loses personal information, such as a bank, hospital or employer, has a fiduciary relationship with those whose information has been compromised.[25]

But it is often not nearly so clear: Does a retailer that maintains information on its customers have a legal duty to keep that information confidential? If the retailer is permitted to sell the data to another entity, does the retailer have a duty to ensure that the buyer has adequate safeguards and will not use the data wrongfully? What about a company that collects consumer data (*e.g.*, a credit reporting service) but has no relationship with the people whose information it has collected? Can it owe a duty to a member of the public with whom it has had no interaction?

It is not difficult to envision a plaintiff arguing the following: The fact that a company maintains information that a reasonable person would not wish to be publicly disclosed means that the company has an inherent duty to keep that information secure.[26] This argument may be bolstered by the growing number of state laws that impose obligations on companies that maintain such information: If the state requires data containing such information to be properly encrypted at all times, the argument goes, it follows that a company that does not do so could be civilly liable for its failure. In addition, corporate privacy policies, especially if disclosed to the public in a notice or on the Internet, may be viewed as an undertaking of a duty even if no duty previously existed.[27] Courts have only begun to wrestle with these questions, but they represent the types of issues that must be resolved as this area of the law evolves.

Conclusion

The ability to store enormous amounts of information in a way that makes it easily accessible from anywhere has been a boon to a wide range of industries. But the same technology has made that information easier to misappropriate and misuse on an unimaginable scale. This change may have opened a new avenue for people whose information is lost or stolen to seek redress in the courts. And courts are taking note. As the Michigan Supreme Court recently held:

> In the past, the risk of harm stemming from a worker taking home sensitive information may not have been great. However, with the advancements in technology, holders of such information have had to become increasingly vigilant in protecting such information and the security measures enacted to ensure such protection have become increasingly complex.[28]

So far, businesses that have inadvertently lost or disclosed confidential information have been largely able to avoid liability in civil lawsuits. But with the law so unsettled in this area, defending against such an action will require new and different legal strategies.

Notes

[1] *See, e.g., Hardin v. Hirshfield*, 12 S.W. 779 (Ky. 1890) (plaintiff claimed engagement ended because defendant spread true, but embarrassing, stories about her); N.Y. Civ. Rights Law §§ 50-51 (1903) (prohibiting use of name or likeness of living person for advertising purposes without consent).

[2] *See, e.g., Humphers v. First Interstate Bank of Or.*, 298 Or. 706, 696 P.2d 527 (1985) (birth mother sued estate of doctor who revealed her identity to daughter).

[3] *See, e.g.*, Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a)(7).

[4] Laura Smitherman, Missing Data Is Latest in Rash of Breaches; Customers Are Warned to Head Off Identity Theft, Balt. Sun, June 8, 2005, at 1A.

[5] Charles Burress, *Cal Issues Alert About Stolen Laptop Computer*, S.F. Chron., Mar. 29, 2005, at B1.

[6] Jenn Abelson, *Breach of Data at TJX Is Called the Biggest Ever*, Boston Globe, Mar. 29, 2007, at A1.

[7] *See Bell v. Mich. Council 25 of the Am. Fed'n of State, County & Mun. Employees, AFL-CIO, Local 123*, 707 N.W. 2d 597 (Mich. 2005) (members sued union after personal information was used by official's relatives in identity theft scheme).

[8] *See, e.g., id.* (recognizing potential for negligence cause of action if "unauthorized transmission of private data" leads to financial loss).

[9] See id.

[10] See, e.g., Moorman Mfg. Co. v. Nat'l Tank Co., 91 Ill. 2d 69, 435 N.E.2d 443 (1982).

[11] *See, e.g., Trans States Airlines v. Pratt & Whitney Can.*, 177 Ill. 2d 21, 26-27, 682 N.E. 2d 45, 48 (Ill. 1997).

[12] In some states the negligent-misrepresentation exception is only available when the defendant is "in the business" of supplying information. *See, e.g. Prime Leasing Inc. v. Kendig*, 332 Ill. App. 3d 300, 312, 773 N.E.2d 84, 95 (Ill. App. Ct., 1st Dist. 2002).

[13] Of course, there may be circumstances in which plaintiffs are able to state a claim for intentional infliction of emotional distress. This article, however, focuses only on possible suits against businesses for inadvertent or accidental disclosure of data.

[14] *Bodah v. Lakeville Motor Express*, 663 N.W. 2d 550, 556 n.5 (Minn. 2003).

[15] Restatement (Second) of Torts § 652D.

[16] *Id.*, cmt. b (citing tax returns as an example of information that, if made public, would constitute an invasion of privacy).

[17] *Id.*, cmt. a.

[18] This assumes, of course, that the information sought is truly private. While a number of statutes protect against disclosure of personal information from government records, for example, not all courts agree about which information is truly private. One Illinois court, for instance, determined that Social Security numbers are not private and that plaintiffs could not maintain an action against a cell phone provider that disclosed them to an epidemiological research firm without permission. *Busse v. Motorola Inc.*, 351 Ill. App. 3d 67, 813 N.E. 2d 1013 (Ill. App. Ct., 1st Dist. 2004).

[19] Hiawatha Bray, Snafu Puts 600,000 at Security Risk: Iron Mountain Loses Worker Data Tapes From Time Warner, Boston Globe, May 3, 2005, at E1.

[20] *Bodah*, 663 N.W. 2d at 556 n.5.

[21] *Kahle v. Litton Loan Servicing*, 486 F. Supp. 2d 705, 710 (S.D. Ohio 2007) (quoting *Key v. DSW Inc.*, 454 F. Supp. 2d 684, 689 [S.D. Ohio 2006] [listing cases]). In *Kahle* a plaintiff sued a mortgage lender after hard drives containing customer information were among equipment stolen from the lender's office, even though the plaintiff could not assert that her information had been accessed.

[22] *Key*, 454 F. Supp. 2d at 690.

[23] Id.

[24] *See, e.g.,* California Information Practice Act, Cal. Civ. Code § 1798.82 (2007) (requiring consumer notification).

[25] *See Bell*, 707 N.W. 2d 597 (union owes special duty to its members).

[26] See, e.g., Humphers, 696 P.2d 527.

[27] *See* Restatement of Torts § 324(i).

[28] *Bell*, 707 N.W.2d 597.

W. Randall Bassett *and* ***Matthew S. Harman*** *are partners in* ***King & Spalding*** *in Atlanta, where they practice in the firm's tort litigation and environmental group. Mr. Bassett has more than 15 years' experience representing foreign and domestic manufacturers, including those in the pharmaceutical and tobacco industries, in high-exposure product liability cases. Mr. Harman represents clients in high-exposure product liability, toxic-tort and commercial disputes and is a founding member of the firm's e-discovery practice group.* ***Michael Weiss*** *is an associate in King & Spalding's Atlanta office, where he represents manufacturers, retailers and nonprofit associations in product liability litigation.*

Mr. Bassett can be reached at (404) 572-3514 and at RBassett@KSLAW.com. Mr. Harman can be contacted at (404) 572-2807 and at MHarman@KSLAW.com. Mr. Weiss can be reached at (404) 572-2804 and at MWeiss@KSLAW.com.