2008

Data Security and Tort Liability

Vincent R. Johnson
St. Mary's University School of Law, vjohnson@stmarytx.edu

Data Security and Tort Liability

By Vincent R. Johnson

Numerous lawsuits have recently been filed against data possessors (such as banks and universities) by data subjects (such as customers and alumni) seeking damages for harm caused by breaches of data security.[1] Some of these claims have been successful. Courts have held, for example, that a union has a duty to safeguard its members' information[2] and have imposed liability for improper disposal of educational records.[3] However, other claims have failed.[4]

Whether and to what extent courts hold database possessors liable for damages caused by improper data access are questions of huge importance. Unless courts impose some form of liability, the persons often in the best position to prevent the losses caused by identity theft may have insufficient incentive to exercise care to avoid unnecessary harm. However, if liability is too readily assessed, it may bankrupt valuable enterprises because of the vast numbers of potential plaintiffs and extensive resulting damages.

Despite the recent enactment of security breach notification statutes in 35 states,[5] the law governing database possessor liability is unsettled. In considering this field of tort law, it is useful to differentiate three questions. The first issue is whether database possessors have a legal duty to safeguard data subjects' personal information from unauthorized access by hackers or others. Such obligations may be imposed by statutes, ordinary tort principles, or fiduciary duty law. The second issue concerns not whether there is a duty to protect computerized information from intruders, but whether a database possessor has a legal obligation to disclose evidence of a security breach to data subjects once an intrusion occurs. The third issue is how far liability should extend when the database possessor has failed to exercise reasonable care to protect data or to disclose information about an intrusion.

Vincent R. Johnson is Visiting Professor of Law, George Washington University, and Professor of Law, St. Mary's University, San Antonio, TX. He earned a BA from St. Vincent College (Pa.), a JD from the University of Notre Dame, and an LLM from Yale University. He is a Member, American Law Institute and co-author, Studies in American Tort Law (3d ed. 2005) (with Alan Gunn). This article has been adapted from an earlier work by the author, "Cybersecurity, Identity Theft, and the Limits of Tort Liability," 57 S.C. L. Rev. 255-311 (2005), which should be consulted for a more extensive treatment of the subject.

STATUTORY DUTIES TO PROTECT DATA

A statute may impose a duty to exercise care to protect data from intruders. An important example is California's Security Breach Information Act (SBIA).[6] The SBIA has served as a model for legislation subsequently adopted in numerous other jurisdictions. Mutual concerns animate the various state laws, which often share a common language and structure. However, the statutes sometimes differ in important respects. One key difference concerns whether a breach of the duties imposed by the act is expressly actionable in a private lawsuit.

The California SBIA imposes a data protection obligation and expressly authorizes maintenance of a suit for damages caused by a breach of that duty. The relevant language, which became effective July 1, 2003, states: "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[7] The legislation further provides that "Any customer injured by a violation of this title may institute a civil action to recover damages."[8]

The SBIA leaves no doubt that businesses owe a duty under California law to protect customers' personal information and that customers may recover damages if businesses breach that duty. The civil actions that the California legislature has instructed the courts to entertain are rooted in principles of negligence. Only unreasonable (*i.e.*, negligent) conduct violates the California SBIA. However, beyond offering clear guidance regarding the existence of duty and the liability regime, the SBIA leaves many matters unsettled. The SBIA makes no attempt to define what constitutes "reasonable security procedures and practices." More importantly, the SBIA gives no indication as to what types of damages plaintiffs can recover.

In some states security breach notification laws require database possessors to protect personal information from unauthorized access but make no provision for civil liability.[9] Many of those laws nevertheless leave room for judicial recognition of a civil cause of action. Under a traditional negligence *per se* analysis, a court may, in its

discretion, embrace a statute not expressly providing for a civil cause of action as the standard of care for a tort suit. If the legislature intended the enactment to protect the class of persons of which the plaintiff is a member from the type of harm that occurred, a court may determine that violation of the statute defines the appropriate terms for imposing civil liability.[10] Many state laws satisfy these requirements. However, in some cases, the language of a statute suggests that the legislation should not be deemed to set the standard of care.

For example, the Arkansas Personal Information Protection Act,[11] which provides for enforcement by the attorney general, states that it "does not relieve a person or business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information."[12] The absence of any provision for private enforcement and the second usage of the word "other" seem to suggest that a court should not embrace the security breach notification law, by itself, as the basis for a civil cause of action.

Similarly, it is difficult to envision that the Texas security breach statute[13] could be a predicate for a negligence *per se* claim. Unlike the California SBIA, the Texas act does not create a civil cause of action against a database possessor that fails to exercise reasonable care. In addition, the act expressly provides for a deceptive trade practices action against hackers and others who "obtain, possess, transfer, or use [the] personal identifying information of another" without authorization.[14] It would be reasonable to interpret the Texas statute as an expression that civil liability should extend only to hackers and other unauthorized persons and not to database possessors.

COMMON LAW DUTIES TO PROTECT DATA

Aside from statutes, common law principles support judicial recognition of a database possessor's duty to safeguard information from intruders. Two landmark cases offer guidance: *Palsgraf v. Long Island Railroad Co.*[15] and *Kline v. 1500 Massachusetts Avenue Apartment Corp.*[16]

In *Palsgraf*, Chief Judge Benjamin Cardozo set down the basic rule on duty for the New York Court of Appeals: "The risk reasonably to be perceived defines the duty to be obeyed, and risk imports relation; it is risk to another or to others within the range of apprehension."[17] In *Palsgraf*, nothing in the appearance of a newspaper-wrapped package carried by a man trying to board a moving train gave notice that the parcel contained explosives. Therefore, nothing warned the trainmen that Helen Palsgraf, a patron waiting across the platform, was in danger. There was as to her no "risk reasonably to be perceived" and thus no "duty to be obeyed." As she was concerned, the railroad had no legal obligation not to carelessly dislodge the package while trying to assist the man who was running for the train.

Courts today continue to apply the *Palsgraf* duty rule. Thus, it is useful to ask whether, from the standpoint of database possessors, there is a "risk reasonably to be perceived" to data subjects if data is not protected from unauthorized intrusion. Obviously, in many situations (such as when hackers can access data via the Internet), the answer is yes. At least on its face, the basic rule in *Palsgraf* suggests that database possessors should often have a duty to exercise reasonable care to protect data from intruders.

Palsgraf did not involve the threat of criminal intervention, but *Kline* did. In *Kline*, a landlord was on notice that "an increasing number of assaults, larcenies, and robberies [were] being perpetrated against the tenants in and from the common" areas of a large apartment building.[18] In holding the landlord responsible for a subsequent attack on the plaintiff, the court said that a landlord is by no "means an insurer of the safety of his tenants" and is not obliged "to provide protection commonly owed by a municipal police department."[19] However, a landlord is under a duty to take such precautions as "are within his power and capacity to take" in order to prevent harm by criminal intruders.[20] In writing for the District of Columbia Circuit, Judge Malcolm Richard Wilkey emphasized the fact that the landlord was the only party in a position to secure the common areas:

> No individual tenant had it within his power to take measures to guard the garage entranceways, to provide scrutiny at the main entrance of the building, to patrol the common hallways and elevators, to set up any kind of a security alarm system in the building, to provide additional locking devices on the main doors, to provide a system of announcement for authorized visitors only, to close the garage doors at appropriate hours, and to see that the entrance was manned at all times.[21]

The court added:

> The landlord is entirely justified in passing on the cost of increased protective measures to his tenants, but the rationale of compelling the landlord to do it in the first place is that he is the only one who is in a position to take the necessary protective measures for overall protection of the premises . . . .[22]

A similar analysis is equally applicable to cases involving database security. Individual data subjects are in a poor position to protect database information from intruders. The database possessor, in contrast, is the only

one with the ability to mitigate the risk that intruders may cause harm. As in *Kline*, the database possessor can spread the cost of providing database security to a broader class of data subjects, at least when there is customer relationship between the plaintiff and defendant. *Kline*, like *Palsgraf*, suggests that, at least in some circumstances, database possessors should owe data subjects a duty to exercise reasonable care to protect data from intruders.

In both *Palsgraf* and *Kline*, there was a relationship between the plaintiff and the defendant. *Palsgraf* was a ticket purchaser of the defendant railroad; *Kline* was a tenant of the defendant corporation. Those relational ties are important, for other cases teach that duty often depends upon more than foreseeability of harm and opportunity to take precautions; it depends, sometimes, on a special linkage between the party who owes the duty and the one who receives its benefit. In this regard, recent cases involving allegedly negligent enablement of imposter fraud are instructive.

In *Huggins v. Citibank, N.A.*,[23] for example, the plaintiff sued various banks on the ground that they "negligently issued credit cards" in the plaintiff's name to an "unknown imposter." The plaintiff alleged, among other things, that the banks issued "credit cards without any investigation, verification, or corroboration" of the applicant's identity. In response, "the [b]anks asserted they owed no duty to [the plaintiff] because he was not their customer." The court agreed with the defendants and wrote:

> In order for negligence liability to attach, the parties must have a relationship recognized by law as the foundation of a duty of care. In the absence of a duty to prevent an injury, foreseeability of that injury is an insufficient basis on which to rest liability. . . . The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.[24]

Other courts have reached similar conclusions.[25]

Together, *Palsgraf*, *Kline*, and *Huggins* indicate that the strongest cases for imposing a common law duty to guard data from intruders will be those in which there is a business relationship between the defendant database possessor and the plaintiff data subject. This conclusion makes sense on economic as well as doctrinal grounds. Imposing a duty of care in these cases will force the database possessor, which benefits from the use of computerized information, to internalize losses relating to improperly accessed data as a cost of doing business. That duty will in turn create an incentive for database possessors to scrutinize whether their business methods are really worth the costs that they entail. At the same time, the imposition of a duty in a business context gives the database possessor a means for distributing the loss by adjusting the price of the goods or services that it sells to the class of persons that ultimately benefits from the defendant's business methods. That reallocation of losses will help ensure that the costs relating to improperly accessed data will not fall with crushing weight on either the data subject or the database possessor.

Placing a burden on database possessors to protect data from unauthorized access would tend to reduce intruder-related losses by encouraging investment in database security. That investment would be consistent with the possessors' own interests because unauthorized access entails huge costs, in terms of public relations and otherwise, for those who maintain databases.

VOLUNTARY ASSUMPTION OF A DUTY TO PROTECT DATA

Even if courts decline to impose a tort duty to safeguard data on database possessors generally (or at least on businesses), voluntary-assumption-of-duty principles may create a legally enforceable data-protection obligation.[26] A person not otherwise under a duty to exercise reasonable care may voluntarily assume the responsibility to do so. One way of assuming this duty is by promising to exercise care and thereby inducing detrimental reliance.[27] Another way is by "undertak[ing] to render services" and consequently increasing the risk of harm to the plaintiff.[28] Either way, the party that undertook the duty of reasonable care will be subject to liability if it breaches the voluntarily assumed duty and causes damages.

These well-established principles may apply when consumers reveal personal information to financial institutions in reliance on financial institutions' stated privacy policies. For example, the policy of one major banking institution, which is not atypical, states in reassuring terms:

> The law gives you certain privacy rights. Bank of America gives you more. . . . Keeping financial information secure is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect Customer Information. . . . All companies that act on our behalf are contractually obligated to keep the information we provide to them confidential . . . .[29]

A customer reading this information would conclude, at a minimum, that in exchange for entrusting the bank with personal information, the bank agreed (1) to protect the data by means of physical, electronic, and procedural safeguards and (2) to keep it confidential. Other language in the privacy policy reinforces those sensible conclusions by stressing the importance of precautions on the part of the customer to guard against disclosure or unauthorized

use of account and personal information. The same is true of statements in the bank's advertising and on its Web site emphasizing the dangers of identity theft and assuring the customer that "[y]our checking account statements are always protected in Online Banking."[30] A court might reasonably interpret such a privacy policy as an undertaking to exercise reasonable care and might conclude that a breach of that duty would support a tort cause of action.

Similarly, even if the plaintiff never read or relied on the institution's privacy policy, a court might impose a duty of care under the other prong of the undertaking rule, which says that, when services provided for the protection of another increase the risk of harm "beyond that which existed without the undertaking," there is a duty to exercise reasonable care.[31] Depending on the facts, the measures taken to protect computerized data (*e.g.*, use of passwords and firewalls) may contain flaws that increase the risk of unauthorized data access. An increased risk of harm might also result when data protection practices allow transmission of unencrypted data, which is especially vulnerable to hacking.

FIDUCIARY OBLIGATIONS TO PROTECT DATA

If a database possessor owes fiduciary obligations to a data subject, it is reasonable to argue that regardless of whether general tort principles would impose a duty, the fiduciary is obliged to protect computerized information relating to the data subject from unauthorized access by third parties. For example, the relationship between an attorney and client is fiduciary as a matter of law. Accordingly, lawyers have a special obligation to protect confidential client information, aside from any demands imposed by ordinary tort principles. A lawyer's broad fiduciary obligation of confidentiality extends to all forms of information about the client, including computerized data,[32] for the existence of the duty turns on the content, not the form, of the information. In light of the fiduciary-duty rules on confidentiality (and the related obligations requiring safekeeping of client property), a lawyer or law firm could not plausibly argue that there is no duty to safeguard computerized client data from intruders. Indeed, the duty of safekeeping may even impose an obligation to encrypt sensitive information.[33]

The same analysis should apply to all fiduciary relationships.[34] However, ordinary business relationships are not fiduciary. In business, parties normally deal with one another at arm's length. The "mere acceptance of confidential information" does not create a fiduciary relationship,[35] nor does the fact that one party "trusts another and relies on a promise to carry out a contract."[36] Consequently, while fiduciary-duty law may play an important role in determining whether professionals, such as lawyers, physicians, or trustees, have a duty to protect the information of clients, patients, and beneficiaries from intruders, it will not set the standard of care in most commercial settings.

STATUTORY DUTIES TO REVEAL SECURITY BREACHES

There are at least four ways of imposing on potential defendants a duty to reveal a compromise in database security. First, a statute may impose a duty, either as a result of the statute's express terms or as a result of judicial reliance on the statute as the proper expression of the standard of care. Second, a duty may arise from common law principles governing negligence liability generally. Third, there may be a duty under the law of misrepresentation, which imposes a general duty to update previously accurate statements (*e.g.*, statements relating to data security) that are the basis for pending or continuing reliance by the recipient of the statements. Finally, failure-to-act rules may require the exercise of reasonable care to avoid or minimize damages if a database possessor's conduct created a continuing risk of physical harm.

Many state security breach information acts require certain types of database possessors (typically businesses, but sometimes governmental agencies or other persons or entities, such as non-profit organizations) to notify data subjects of violations (or possible violations) of their information's security. Several of the states that impose notification obligations expressly authorize a civil action for damages.[37] In addition, Illinois allows a deceptive trade practices action,[38] which permits a "person who suffers actual damage . . . [to recover] actual economic damages or any other relief which the court deems proper,"[39] including "reasonable attorney's fees and costs."[40] In other states, a variety of means are used to enforce the notification obligation, such as administrative or civil fines or an action by the attorney general to recover "direct economic damages" or to remedy deceptive trade practices.

Some state notification statutes not expressly providing for civil liability, such as the Maine Notice of Risk to Personal Data Act,[41] leave room for courts to entertain negligence *per se* actions by ruling out arguments that legislatures intended the statutorily created penalties to be the sole measure of a database possessor's obligations. The Maine law states that "rights and remedies available under [the statute] are cumulative and do not affect or prevent rights and remedies available under federal or state law."[42]

COMMON LAW DUTIES TO REVEAL SECURITY BREACHES

A key question in determining whether common law principles should require notification is whether disclosure of the breach would be useful or futile. If a data subject could not do anything to protect his or her own interests following an intrusion into data security, there would be little reason to require notification. However, individuals can act to protect themselves from financial and physical harm that persons with unauthorized access to their data may cause. The federal Fair and Accurate Credit Transactions Act of 2003 (FACTA)[43] allows consumers to place a "fraud alert" in their files with credit reporting agencies. Certain state laws also enable consumers to place a "security freeze" on their credit report, which "prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer."[44] Some state laws permit victims of information security breaches to obtain a court order declaring the individual a victim of identity theft.[45] That declaration can aid the data subject in dealing with law enforcement authorities or with businesses. Consumers can also monitor their credit card and bank accounts more closely for evidence of unauthorized transactions or pay monthly service fees to a company that tracks three national credit reporting companies on a daily basis and advises subscribers of key changes to their data (such as new applications for credit by someone using the subscriber's name and identity).

In many circumstances, US tort law has imposed liability for failure to warn. Indeed, courts have sometimes held that there is a duty to warn even when there is no duty to do anything else. Consequently, it might reasonably follow that, even if a state holds that there is no duty to protect databases from intrusion, there should at least be a duty to provide notice of a security breach of the database.

There is a duty to update previous statements that were intended to induce reliance and that, though true when made, have become false or misleading as a result of subsequent developments.[46] The duty extends until recipients of the information are no longer able to protect their own interests by foregoing reliance on the now-erroneous representation of the fact. Thus, if businesses tell their customers, through advertisements, Web sites, or published privacy policies, that their personal data is secure, but then learn information to the contrary, the businesses may have a duty to disclose those developments to their customers. The customers have a choice whether to continue their relationships with the businesses in question. There has been no irrevocable reliance by a customer, even though a business-customer relationship is already in progress. The customers may act to protect their interests by terminating the relationship and doing business elsewhere.

It is also well established that when a person's prior conduct creates a continuing risk of physical harm there is a duty to render assistance to keep the harm from occurring or mitigate adverse consequences.[47] This duty exists even if the prior conduct was not tortious. Thus, a driver who is involved in an auto accident must stop to render aid, regardless of whether he was at fault for the collision.[48] The harm caused by intrusions into computerized personal data is typically more economic than physical in nature. Yet, misuse of improperly accessed personal data can result in a physical attack on a data subject or physical harm to property. Hacking of a newspaper's records, for example, may reveal when a customer's paper will be on vacation hold and thereby lead to a burglary while the customer is away on vacation. Thus, on appropriate facts, this rule may impose a duty to disclose information about a data security breach.

Finally, a fiduciary relationship imposes a duty of candor. The fiduciary must exercise reasonable care to reveal all material information to the person to whom the fiduciary owes a duty. Indeed, when the interests of the fiduciary and the beneficiary are adversely aligned, fiduciary principles may require something more than reasonable care, perhaps a degree of forthcomingness that approximates "absolute and perfect candor."[49] If a database possessor owes fiduciary obligations to a data subject (as in the case of an attorney and client), the possessor must disclose information relating to a breach of database security. The interests of the fiduciary and the data subject are in potential conflict because there are important questions as to whether the possessor may be held responsible for the loss of the data. The law requires the fiduciary to subordinate personal interests to the interests of the data subject. Non-disclosure would ordinarily be inconsistent with those heavy obligations.

THE ECONOMIC LOSS RULE

The economic-loss rule is an obscure, but important, legal doctrine, which holds that a plaintiff may not recover economic losses resulting from the defendant's negligence without corresponding physical damage to the plaintiff's person or property. Obviously, if the economic-loss rule applies to cybersecurity cases, it has the potential to greatly limit the scope of recoverable damages. Consequently, it is important to understand the policies underlying the rule and the nature of its restrictions. Viewed from the standpoint of public policy, the economic-loss rule serves

three different functions: avoidance of too broad a scope of liability; insistence that damages be proved with certainty; and definition of the doctrinal boundary between contract law and torts.

First, somewhat crudely, the economic-loss rule protects potential defendants from the risk of a disproportionately wide range of liability.[50] This is an important function, for acts of negligence often have broad adverse economic consequences. Without this protection, there would be no sensible stopping point to tort liability. For example, a referee who negligently made a bad call that eliminated a team from the playoffs could be liable for the lost profits of merchants who sell team-related items, or a person who caused an auto accident could be responsible for the economic losses that resulted from the delays of persons tied up in traffic. Not surprisingly, the Restatement provides, as a general rule, that there is no liability for negligent interference with contracts or economically promising relations.[51]

Second, lost economic opportunities are often not readily susceptible to precise calculation.[52] Yet, the law insists that damages must be proved with reasonable certainty. By ruling out litigation in a huge range of cases (suits involving no personal injury or property damage), the economic-loss rule helps to ensure (again somewhat crudely) that compensation is not awarded for amounts that are speculative. In the process, the economic-loss rule promotes judicious use of limited judicial resources, ensuring that those scarce assets are not squandered on the burdensome, and perhaps dubious, task of trying to quantify endless economic losses that may, in truth, not be provable with reasonable precision.

Third and most importantly, the economic-loss rule marks the boundary between contract law and tort law. Delineating these two bodies of law is vital, for otherwise there is a risk that "contract law would drown in a sea of tort."[53] The law of contracts has meaning only because entering into an agreement has legal consequences. One of those consequences is that, if a person makes a bad deal, he usually must suffer the result. This reality creates an incentive for contracting parties to exercise diligence to protect their own interests. It would render superfluous a great part of contract law if parties who strike disadvantageous bargains could successfully complain that they should recover damages because the other side failed to exercise reasonable care to protect their interests.

With these three policy considerations in mind—scope of liability, certainty of damages, and delineation of the boundary between contract law and torts—the questions are whether the economic-loss rule should apply to cybersecurity cases, and if so, what claims for damages the rule might bar. Answering those questions involves consideration of the types of economic losses that may arise in these cases, as well as the efficacy of contract law and the insurance market in addressing such losses. Unauthorized use of personal information can result in many types of harm. In cybersecurity cases where breaches of security result in identity theft, the losses include, but are not limited to: (1) out-of-pocket expenses incurred to restore a good credit rating; (2) personal time spent on that task; and (3) lost opportunities resulting from bad credit.

Focusing first on out-of-pocket losses, there is little policy justification for denying recovery. Various estimates currently peg out-of-pocket costs in a typical case between $800 and $1,400. Although the amount of out-of-pocket damages may vary, this element of damages is susceptible to proof with a high degree of certainty. The plaintiff can gather receipts, make a list, and total the sum. There is no reason to deny compensation for amounts actually and reasonably spent on restoring a good credit rating on the ground that out-of-pocket damages are speculative.

Nor does recovery of out-of-pocket costs present a case that requires a tightly circumscribed circle of liability to prevent an over extension of legal responsibility. In many cases, there will be a business relationship between the database possessor and the damaged data subject, and in other cases the relationship (presumably) is sufficiently close enough that the defendant had some legitimate reason to maintain a database containing personal information about the plaintiff. These are not situations where some stranger in the community (*e.g.*, the vendor of the losing team's products or the person tied up in traffic) is seeking to recover damages. If a database possessor wishes to constrict the scope of potential liability, it can always do so by removing the personal information of data subjects from its database. But if it fails to do so, courts should be reluctant to deny recovery of out-of-pocket losses to data subjects. The database possessor chose to maintain personal information in a form where one of the risks was unauthorized access.

If the scope of liability and uncertainty of damages are not significant considerations, the only question is whether the boundary between contracts and torts is a good reason for a court to say that this type of loss should be compensated only if a contractual obligation exists. The answer to that question is no.

An emerging consensus, reflected in the recently passed state security breach notification statutes, suggests that rights relating to protection of personal data and notification of security breaches are not proper subjects for bargaining between the parties. Many state laws, such as the Rhode Island Identity Theft Protection Act of 2005,[54] provide that a waiver of a data subject's rights is against

public policy and therefore void and unenforceable. If that is true, it makes little sense that consumers should bargain and pay for the level of cybersecurity protection—and the right to sue for out-of-pocket damages—that they desire. Moreover, it is simply unrealistic to expect bargaining to occur between individual consumers and the large corporations that play a pervasive role in modern life. Individuals often lack both the commercial leverage and the information necessary to assess the risks that they face. In light of the ubiquity of computerized databases, ordinary persons would have to devote a huge amount of energy to negotiating the parameters of data protection with every potential defendant if contract law were the only solution to these types of problems.

As an alternative to this sort of David-versus-an-army-of-Goliaths contractual model, a better paradigm would routinely permit recovery of foreseeable and necessary out-of-pocket losses from the tortfeasor. Compensation of out-of-pocket losses should not depend on whether the data subject read the fine print in the defendant's privacy policy or bargained for a specific level of protection. Instead, compensation should depend on the reasonableness of the amount spent to restore a good credit rating. Tort law can perform this function better than contract law.

A different analysis is required with respect to requests for recovery of compensation for time spent restoring one's good credit or for opportunities lost as a result of a bad credit rating. Victims of identity theft spend 600 hours on average to restore their credit. The harm suffered by these victims is tremendous, but valuing these lost hours would be difficult. If damages amounted to compensation for the plaintiffs' time measured at their usual hourly rates of earnings, the awards to professionals, minimum wage workers, and unemployed homemakers would vary widely. Similarly, if every victim received the same amount for the value of lost time, how would that amount be set? Ensuring uniformity in valuing damages for lost time is a task better committed to legislatures than to the multitude of fact-finders who will preside over numerous tort claims.

The problems of compensating for the value of lost opportunities, such as the lost chance to buy a house, obtain a car loan, or open a cell phone account, are also obvious. How does one prove precisely which opportunities the plaintiff lost and what those opportunities meant in economic terms to the plaintiff? In addition, there is a clear risk of imposing an excessively wide range of liability. Negligence requires only a momentary misstep. To say that a negligent database possessor should be liable to a broad class of persons for all of their lost opportunities, as well as out-of-pocket and perhaps other damages, would quickly pose a serious risk of liability disproportionate to fault. These issues suggest that courts have a greater reason to apply the economic-loss rule to bar claims for lost time and lost opportunities than to hold that a plaintiff cannot recover out-of-pocket losses.[55]

The economic-loss rule, as defined in most states, has important limits. First, it bars only claims for economic harm caused by negligence.[56] A plaintiff may thus be able to avoid the rule by proving more culpable conduct, such as recklessness or intentional wrong-doing. Second, the economic-loss rule is a common law doctrine that does not preempt legislative provisions to the contrary. Liability for negligently caused economic harm may be actionable pursuant to statute. At least one state, Illinois, expressly allows for recovery of economic losses in cybersecurity cases.[57] Third, many types of harm caused by intrusion are not purely economic. Thus, the rule does not bar recovery of damages for personal injury, property damage, and, perhaps, emotional distress. Fourth, some states show little enthusiasm for the economic-loss rule[58] and may determine that it does not apply to cybersecurity cases. Finally, virtually all states that embrace the economic-loss rule recognize exceptions. For example, economic damages are routinely recoverable in negligent misrepresentation actions.[59] Many states also allow persons whose legacies are lost due to negligent preparation of a will to sue to recover those economic damages.[60] A court might determine that the relationship between a database possessor and data subject is sufficiently special to warrant recovery of out-of-pocket losses resulting from identity theft, notwithstanding the economic-loss rule.

EMOTIONAL-DISTRESS DAMAGES

States differ tremendously over whether negligently caused emotional-distress claims are actionable. Some jurisdictions hold that emotional-distress damages are almost never recoverable,[61] but others seem quite willing to entertain claims for psychic suffering caused by a tortfeasor's failure to exercise due care.

One arena in which a consensus of sorts has emerged is the fear-of-disease cases. In these suits, the plaintiff alleges that the defendant's tortious conduct subjected the plaintiff to emotional distress based on fear of contracting a contagious disease. Many of these cases have involved HIV or AIDS, but the precedent extends somewhat further to fear of cancer and other diseases. In addressing these claims, courts generally hold that a plaintiff may recover emotional-distress damages only if the plaintiff was actually exposed to the disease.[62] Courts deem fear of disease in the absence of exposure to be unreasonable and therefore not compensable.

The precedent that has emerged in these cases provides a logical starting point for determining whether a

data subject should be able to recover for emotional-distress losses resulting from unauthorized database intrusion and fear of identity theft or other harm. If there is no evidence that an intruder actually accessed the plaintiff's data, and the evidence proves only a risk of unauthorized access, courts ordinarily should deny emotional-distress damages, which are inherently difficult to quantify. However, some cases will warrant a presumption of unauthorized access. If the defendant has allowed or caused the best evidence of exposure to be lost or destroyed, courts reasonably may assume that exposure occurred absent proof to the contrary. Some fear-of-disease cases take this approach.[63]

In cases involving intentional infliction of emotional distress, courts have assiduously required that the distress be severe before it is compensable.[64] This severity requirement is all the more applicable when the distress results from mere alleged negligence. Presumably, in only rare cases will it be possible for a data subject who does not suffer physical harm to recover emotional-distress damages relating to data intrusion.[65]

CREDIT-MONITORING DAMAGES

Database possessors who suffer a security breach are often reluctant to discover and report those developments for fear of triggering adverse publicity, legal liability, or increased attacks by hackers. As a result, there can be an undesirable lag between the occurrence of an intrusion, discovery of that breach, and revelation of the events to data subjects. Yet, prompt revelation of a breach is important because it enables data subjects to protect their interests through increased vigilance against identity theft and other types of harm.

State security breach notification laws currently provide only a limited incentive for database possessors to discover intrusion because legislatures ordinarily base notification obligations on actual discovery or notification of the intrusion rather than when the database possessor should have discovered the breach. In addition, legislatures typically impose a low cap on the civil fines that apply to a breach of a general statutory duty to protect customer information, which may provide insufficient inducement for best practices.[66]

Legislatures should give database possessors a legal incentive to discover and report unauthorized database intrusions. That incentive could take the form of a limitation on liability. One reasonable option would be to cap the database possessor's exposure to liability at the moment that the database possessor reveals the breach to the data subject. Notification could serve as the pivotal factor in shifting further responsibility (beyond the damages cap) from the database possessor to the data subject. Once the database possessor provides notice of the security breach, the data subject is in a better position than the database possessor to monitor the risk of harm and to take action against threats to the data subject's credit and personal security.

The cap on damages could take the form of limiting liability to an amount equivalent to the out-of-pocket costs of monitoring credit ratings and taking other reasonably necessary steps to prevent identity theft and related losses. "Credit-monitoring damages" would be similar in concept to the medical monitoring damages that some state[67] and federal[68] courts allow victims of toxic exposure to recover. The analogy is apt. A data subject who loses personal data due to a security breach, like a person who suffers exposure to a toxic substance, is at risk of further harm. The harm (*e.g.*, identity theft in the case of the data subject or cancer in the case of the toxic-exposure victim) may or may not later occur. However, the reasonable and prudent course is to incur the expenses necessary to monitor the risk that harm may develop. The victim of the exposure is thereby in a better position to take prompt action; in one case, to combat the risk of financial harm from data misuse, and in the other to secure medical care to address the risk of developing an illness.

The bargain of capping a cybersecurity plaintiff's damages at the cost of monitoring credit if the database possessor provides notification of a security breach is not a bad one. From the standpoint of the data subject, the plaintiff may be better off with a warning and reimbursement for the out-of-pocket costs of vigilance than gambling on a tort action against the database possessor. A tort suit would be fraught with many obstacles: a possibly short statute of limitations; a risk that the court will not find the database possessor's negligence to be a proximate cause of resulting criminal conduct; a likelihood that the economic-loss or exposure rules may bar key portions of the damages; and a possibility that the court might find that the database possessor had no duty at all.

Nor is the bargain bad for database possessors. Capping damages at the cost of credit monitoring would avoid the risk of catastrophic liability for personal injuries that sometimes occur, the possibility of exposure to property-damage claims, and the chance that a court might narrowly construe the applicability of the economic-loss rule. Some companies faced with the risk of liability from loss of personal data have voluntarily provided affected persons with credit-monitoring protection.[69] However, courts have been reluctant to award credit monitoring damages.[70]

Moreover, society would be better off if the law capped damages at the cost of credit monitoring in

exchange for victim notification whenever there is a security breach. The only ways to minimize the losses stemming from database intrusions (aside from criminal penalties, which seem ineffective) are to spur investment in data security, to discover when intrusions occur, and to warn persons whose interests are at risk. A cap on damages in exchange for notification of security breaches would not undercut the database possessors' incentives to invest in data security. Database possessors would still be subject to state and federal laws that impose various sanctions relating to cybersecurity; they would still face the threats of bad publicity and consumer disaffection resulting from disclosure of security breaches; and at least some possessors (*e.g.*, credit card companies) would still stand to lose millions of dollars as a result of unauthorized use of personal information. However, capping damages at credit-monitoring costs would help to ensure that database possessors are not subject to ruinous tort judgments. The cap would create incentives to discover security breaches and to internalize the resulting credit-monitoring costs that those intrusions entail. In addition, the cap on damages might also reduce the threat of overburdening already overworked federal and state courts. The cap would greatly simplify damages issues in cybersecurity cases and guidance from the courts would quickly define the average costs of security monitoring, thereby promoting the settlement of cases. Indeed, limiting liability to security-monitoring damages is also likely to promote insurance coverage of intruder-related losses by making the extent of liability more certain, thereby facilitating the pricing of insurance coverage.

A damages cap should not apply to cases involving egregious conduct. A plaintiff who can establish that the defendant acted with reckless indifference or intentional disregard in failing to protect data should be able to avoid the limitation on liability. Similarly, if the defendant did not disclose a security breach, liability for a breach of the notification duty or of the duty to protect data should extend as far as the usual rules of tort law allow.

A cap on database possessor liability at the costs of credit-monitoring damages can be legislatively enacted. However, in the absence of legislation to the contrary, questions relating to duty, proximate causation (including shifting responsibility), and damages have traditionally been within the province of the courts. State law may permit courts to determine that, if a database possessor negligently fails to protect computerized personal information, the database possessor has no legal obligation other than to pay for credit-monitoring damages if the database possessor revealed the breach to the data subject.

SECURITY IN INSECURE TIMES

Modern society is built on fragile foundations of computerized personal data. If this society is to endure and prosper, then it must vigilantly safeguard those foundations. Tort law offers an appropriate legal regime for allocating the risks and spreading the costs of database intrusion-related losses. Tort law can also create incentives, on the part of both database possessors and data subjects, to minimize the harm associated with breaches of database security. Courts and legislatures must consider carefully the role of tort liability in protecting computerized data. If those who make and interpret the laws too hastily conclude that database possessors are not liable for losses occasioned by unauthorized data access, whether because there is no duty, no proximate causation, or no recoverable damages, important opportunities to reduce and distribute the costs of computerized technology will be lost. If liability is too readily assessed, important institutions will be adversely affected and with them the prosperity of modern society. Security in insecure times requires a sensitive balancing of competing interests. Established tort principles carefully applied to the contemporary problems of cybersecurity and identity theft can perform a key role in protecting the economic foundations of modern life.

NOTES

1. *See* Sheri Qualters, "Data-Breach Class Actions Abound," *Nat'l L.J.*, Aug. 6, 2007.
2. *See* Bell v. Michigan Council 25, 2005 WL 356306 (Mich. App. 2005).
3. *See* Scott v. Minneapolis Public Schools, Special Dist. No. 1, 2006 WL 997721 (Minn. Ct. App. 2006).
4. *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 639 (7th Cir. 2007); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, *4 (D. Ariz. 2005); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 779 (W.D. Mich. 2006); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712-713 (S.D. Ohio 2007); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690-691 (S.D. Ohio 2006). *See also* Assoc. Press, "Data Breach Suit Against Ohio U. Tossed," *Balt. Sun*, Aug. 30, 2007.
5. *See* David L. Silverman, "Data Security Breaches: The State of Notification Laws," 19 No. 7 *Intell. Prop. & Tech. L.J.* 5 (2007); Catherine M. Bump, Expedia, Inc., Julie O'Neill, Alysa N. Zeltzer, Kelley Drye Collier Shannon, "Summary of State Data Security Laws as of March 2006," 865 PLI/Pat 39 (2006).
6. SBIA effective July 1, 2003, ch. 915, 2002 Cal. Legis. Serv. (West), *available at* CA LEGIS 915 (2002) (Westlaw).
7. Cal. Civ. Code § 1798.81.5 (Westlaw 2007).
8. Cal. Civ. Code § 1798.84(b) (Westlaw 2007).
9. *See, e.g.*, Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, § 11-49.2-2(2) to § 11-49.2-6 (Westlaw 2007).
10. *See generally* Restatement (Third) of Torts: Liab. for Physical Harm § 14 (Proposed Final Draft No. 1, 2005).
11. Personal Information Protection Act, Ark. Code Ann. §§ 4-110-101 to -108 (Westlaw 2007).
12. *Id.* § 4-110-106(b).
13. Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code § 48.001, *et seq.* (Westlaw 2007).

14. *See id.* § 48.101 and § 48.203.
15. Palsgraf v. Long Island Railroad Co., 162 N.E. 99 (N.Y. 1928).
16. Kline v. 1500 Massachusetts Avenue Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).
17. *Palsgraf*, 162 N.E. at 100.
18. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 479 (D.C. Cir. 1970).
19. *Id.* at 486-488.
20. *Id.* at 487.
21. *Id.* at 480.
22. *Id.* at 488.
23. Huggins v. Citibank, N.A., 355 S.C. 329, 585 S.E.2d 275 (2003).
24. *Id.* at 333-334, 585 S.E.2d at 277.
25. *See, e.g.*, Smith v. Citibank, N.A., No. 00-0587-CV-W-1-ECF, 2001 WL 34079057, at *2-4 (W.D. Mo. Oct. 3, 2001); Polzer v. TRW, Inc., 682 N.Y.S.2d 194, 195 (N.Y. App. Div. 1998).
26. *See generally* Restatement (Third) of Torts: Liab. for Physical Harm § 42 (Proposed Final Draft No. 1, 2005).
27. *See id.* § 42 cmt. e.
28. *See id.* § 42.
29. Bank of America, Privacy Policy for Consumers 2005, *http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr* (last visited Nov. 15, 2005).
30. Bank of America, Online Banking, *http://www.bankofamerica.com/privacy/index.cfm?template=privacysecure_olb* (last visited Oct. 30, 2005).
31. Restatement (Third) of Torts: Liab. for Physical Harm § 42(a) (Proposed Final Draft No. 1, 2005).
32. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. No. 782 (2004). *See generally* David Hricik, "The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age," 10 *Computer L. Rev. & Tech. J.* 73 (2005).
33. *See* David J. Ferrell, "Avoid the Shame and Liability of Lost Data–Encrypt!," *Tex. B.J.* 580 (2007).
34. *See* Bell v. Michigan Council 25, 2005 WL 356306, *3 (Mich. App. 2005) (holding a union liable to its members).
35. PulseCard, Inc. v. Discover Card Servs., Inc., 917 F. Supp. 1478, 1485 (D. Kan. 1996).
36. Navistar Int'l Transp. Corp. v. Crim Truck & Tractor Co., 791 S.W.2d 241, 243 (Tex. Ct. App. 1990).
37. *See, e.g.*, Cal. Civ. Code § 1798.84(b) (Westlaw 2007); La. Stat. Ann § 51:3075 (Westlaw 2007); Tenn. Code Ann., § 47-18-2107(h) (Westlaw 2007).
38. 815 Ill. Comp. Stat. Ann. 530/5, *et seq.* (Westlaw 2007).
39. *Id.* at 505/10a(a).
40. *Id.* at 505/10a(c).
41. 10 Me. Rev. Stat. Ann. § 1346 (Westlaw 2007).
42. *Id.* at § 1349(3).
43. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended in scattered sections of Titles 15 and 20 of the US Code).
44. *See, e.g.*, Wash. Rev. Code 19.182.170 (Westlaw 2007).
45. *See* Texas Bus. & Com. Code § 48.202 (Westlaw 2007).
46. *See* Sharff v. Pioneer Fin. Servs., Inc., No. 92 C 20034, 1993 WL 87718, *6-7 (N.D. Ill Mar. 22, 1993); Stevens v. Marco, 305 P.2d 669, 683 (Cal. Dist. Ct. App. 1957); St. Joseph Hosp. v. Corbetta Constr. Co., 316 N.E.2d 51, 71 (Ill. App. Ct. 1974); McMahan v. Greenwood, 108 S.W.3d 467, 494 (Tex. App. 2003).
47. *See* Restatement (Third) of Torts: Liab. for Physical Harm§ 39 (Proposed Final Draft No. 1, 2005).
48. *Cf.* Restatement (Second) of Torts § 321 illus. 3 (1965).
49. *See* Vincent R. Johnson, "Absolute and Perfect Candor to Clients," 34 *St. Mary's L.J.* 737, 792 (2003).
50. *See* Jay M. Feinman, Economic Negligence: Liability of Professionals and Businesses to Third Parties for Economic Loss § 1.2, 1.3.2 (1995).
51. *See* Restatement (Second) of Torts § 766C (1977).
52. *Cf.* J'Aire Corp. v. Gregory, 598 P.2d 60, 65 (Cal. 1979).
53. E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 866 (1986).
54. R.I. Gen. Laws § 11-49.2-6(b) (Westlaw 2007).
55. *See also* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).
56. *Cf.* People v. Ware, No. H025167, 2003 WL 22120898, *1-2 (Cal. Ct. App. Sept. 11, 2003).
57. 815 Ill. Comp. Stat. Ann. 505/10a(a) (Westlaw 2007).
58. People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 118 (N.J. 1985).
59. *See* Restatement (Second) of Torts § 552B cmt. a (1977).
60. *See, e.g.*, Heyer v. Flaig, 449 P.2d 161, 163 (Cal. 1969).
61. *Cf.* Charles E. Cantu, "An Essay on the Tort of Negligent Infliction of Emotional Distress in Texas: Stop Saying It Does Not Exist," 33 *St. Mary's L.J.* 455, 465-468 (2002).
62. *See, e.g.*, Majca v. Beekil, 701 N.E.2d 1084, 1090 (Ill. 1998).
63. *See* S. Cent. Reg'l Med. Ctr. v. Pickering, 749 So. 2d 95, 102 (Miss. 1999).
64. *See, e.g.*, Russo v. White, 400 S.E.2d 160, 163 (Va. 1991).
65. *But see* Bell v. Michigan Council 25, 2005 WL 356306, *6-7 (Mich. App. 2005) (allowing recovery of emotional distress damages). *See also* Scott v. Minneapolis Public Schools, Special Dist. No. 1, 2006 WL 997721 (Minn. Ct. App. 2006) (allowing recovery for emotional distress caused by revelation of educational records).
66. *See, e.g.*, Tex. Bus. & Com. Code §§ 48.201(a), (e) (Westlaw 2007) (holding violators "liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation").
67. *See, e.g.*, Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824-825 (Cal. 1993).
68. *See, e.g.*, Carey v. Kerr-McGee Chem. Corp., 999 F. Supp. 1109, 1119 (N.D. Ill. 1998); Witherspoon v. Philip Morris, Inc., 964 F. Supp. 455, 467 (D.D.C. 1997).
69. *See* Daniel Wolfe, "Security Watch," *Am. Banker*, Apr. 28, 2006, at 5; David Colker & John Spano, "Hackers Steal Data on 300,000 or More," *Kan. City Star*, Apr. 13, 2005. *See also* Sara Semelka, "UM Tries Salving Security Breach," *Colum. (Mo.) Daily Trib.*, June 23, 2007 (discussing a university that arranged discounted rates for affected individuals). *But see* Hope Yen, "Government Withdraws Credit Monitoring After Veterans' Data Theft, VA Originally Promised to Offer Program for One Year," *Charleston Gazette & Daily Mail*, July 19, 2006).
70. *See* n.3, *supra*.