I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

MICHAEL L. RUSTAD & THOMAS H. KOENIG*

Extending Learned Hand's Negligence Formula to Information Security Breaches

Abstract: Negligent security policy is at the heart of recent data theft disasters involving identity fraud and the misappropriation of electronic information. Several statutes already give the state attorneys general or federal officials the right to seek penalties against any company that fails to disclose security breaches when consumer data has been compromised. However, no state or federal security breach notification statutes give the victims of data theft a private cause of action for data theft. At present, the combination of the economic loss rule, present injury requirements, and the lack of a judicially created duty to secure data, presents an insurmountable barrier to individual recovery for negligent data handling. Companies use contractual devices such as "hold harmless" clauses and indemnification to shift the costs of data theft to users. This article argues that Learned Hand's famous risk/utility test should be extended to create a duty to secure computer systems applicable against companies that hold sensitive personal information. The victims of negligent information security should be allowed to recover damages from the data handlers whose failure to implement reasonable security enables data theft. This negligent enablement theory of tort liability will create the necessary policy incentives for companies to develop comprehensive security solutions that will prevent data intrusions.

---

* Michael L. Rustad Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts. Professor Thomas H. Koenig chairs Northeastern University's Sociology and Anthropology Department and is on the Executive Committee of its Law, Policy & Society Doctoral Program. The authors would like to thank Suffolk University Law School reference law librarian Diane D'Angelo for her assistance in locating sources and Carla Bulford of The Ohio State University Moritz College of Law for her helpful editorial suggestions.

I. INTRODUCTION

The seamless interconnectivity of cyberspace is both the Internet's greatest strength and its Achilles heel.[1] The failure of companies to anticipate and guard against security risks is a "time bomb ready to explode."[2] Inadequate computer security is already a public relations disaster and may soon become a legal disaster unless companies anticipate and protect themselves against unauthorized access.[3] In a recent survey of corporate executives, the concern over insecure corporate information systems topped the list of worries, exceeding even the fear of terrorism.[4] Current computer industry precautions are insufficient to protect confidential consumer and company data from third-party hackers or cybercriminals.

The widespread failure of information security is enabling a worldwide epidemic of cybercrime.[5] In March of 2007, TJ Maxx Companies, Inc. (TJX) disclosed that an unknown intruder compromised the security of 45.6 million credit card numbers

---

[1] *See* EDUARDO GELBSTEIN & AHMAD KAMAL, INFORMATION INSECURITY: A SURVIVAL GUIDE TO THE UNCHARTED TERRITORIES OF CYBER-THREATS & CYBER-SECURITY 2 (2d ed. 2002), *available at* http://www.itu.int/wsis/docs/background/themes/security/information_insecurity_ed.pdf ("This profound integration of computers and information technology is obviously the strength of modern life, but it is also its vulnerability. The greater the vulnerability, the greater the ease with which it can be exploited."); *see also* Michael L. Rustad & Lori Eisenschmidt, *The Commercial Law of Internet Security*, 10 J. HIGH TECH. L. 213, 216 (1995) (explaining that cybercriminals may easily exploit several vulnerabilities at the server level).

[2] *The Challenge of Electronic Data: Corporate Legal Obligations to Provide Information Security*, WALL STREET LAWYER: SECURITIES IN THE ELECTRONIC AGE, March 2006, at 1, *available at* http://www.wildman.com/index.cfm?fa=attorney.bio&bioID=3C9D1202-BDB9-4A10-5D7B92567DDF568A (last visited Nov. 5, 2007).

[3] *Id.*

[4] The Harris Interactive Survey of Crisis Situations and Extent of Worry, *Data Security Study*, Table 1 (reporting the compromise of corporate information systems to be a major worry for 61% of the 197 senior executives polled. Fifty-five percent of the respondents listed terrorism as a "major worry.").

[5] The number of high profile data thefts or losses is skyrocketing. Not a month goes by without a number of high profile data disasters. Privacy Rights Clearinghouse, *A Chronology of Data Breaches Updated*, PRIVACYRIGHTS.ORG, http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP (last visited Nov. 5, 2007). *See also*, Christopher L. Sorey, *The Hidden Risks of Outsourcing: Is Your IP Safe Abroad?*, 1 Am. U. Bus L. Brief 33 (2005), *available at* http://www.wcl.american.edu/blb/01/2sorey.pdf?rd=1.

associated with 451,000 American consumers.[6] ChoicePoint inadvertently compromised sensitive consumer data by negligently selling personal information to cybercriminals masquerading as legitimate companies.[7] Citigroup Bank and Financial Services lost computer tapes containing the personal data of 3.9 million customers.[8] MCI recently compromised the records of 16,500 current and former employees due to the theft of an employee's laptop.[9]

Thirty-seven organizations reported the loss of personally identifiable computer files containing social security numbers, account numbers, and other personal information in May of 2007 alone.[10] Public institutions such as Louisiana State University, University of Missouri and the University of California Irvine Medical Center were among these data theft victims.[11] Pillars of the corporate establishment such as J.P. Morgan, IBM, and Priority One Credit Union were also victimized.[12] While state and federal statutes require companies to provide notice of data breaches, no statute gives consumers a private cause of action for negligent security.

This article examines the duty to provide reasonable security to protect computer systems from data theft by third-party criminals. The unsettled legal issue is what duty, if any, a company owes to third-party customers with regard to the measures the company takes to protect sensitive data. We argue that companies have a duty to provide reasonable information security practices under the common law of torts.[13] Expanded legal liability is necessary to convince

---

[6] Jaikumar Vijayan, *TJX Data Breach: At 45.6 Million Card Numbers, It's the Largest Ever*, COMPUTERWORLD SECURITY, March 29, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782&source=rss_news10 (last visited Nov. 5, 2007).

[7] *Id.*

[8] MSNBC Staff, *Citi Notifies 3.9 Million Customers of Lost Data*, MSNBC.COM, June 7, 2005, http://www.msnbc.msn.com/id/8119720/ (last visited Nov. 5, 2007).

[9] Robert McMillan, *MCI Employee Data Stolen in Laptop Theft*, CNN.COM, May 23, 2005, http://www.computerworld.com/mobiletopics/ mobile/story/0,10801,101958,00.html (last visited Nov. 5, 2007).

[10] Privacy Rights Clearinghouse, *supra* note 5.

[11] *Id.*

[12] *Id.*

[13] One commentator contends that companies already have a duty to provide reasonable computer security and a duty to disclose data breaches should they occur. Thomas J.

companies to take data protection more seriously in order to address the foreseeable risks resulting from negligently designed or negligently implemented computer security systems.

The best analytical approach for crafting this new duty involves determining whether the burden of a comprehensive security solution is less than the magnitude of the damages caused by lost or stolen data, multiplied by the probability of occurrence. A major consideration in the decision to impose liability for negligent security is whether a company could have foreseen the particular harm resulting from its existing security precautions and whether cost effective measures would have significantly reduced the risk. At present, neither consumers nor companies have any meaningful remedy for cross-border breaches of data protection.[14] In a world of corporate accountability, companies should not be free to reallocate the risk of data theft to consumers or to its business customers through contractual devices such as "hold harmless" clauses and indemnification agreements. For example, companies may not use these contractual devices to bypass their duty to maintain reasonable security of financial information under the Sarbanes-Oxley Act.[15] Nor can healthcare providers side-step their duty to protect patient data under the Health Information, Portability and Accountability Act.[16] Outsourcers of products already routinely use "hold harmless" indemnity clauses in supply chain contracts to protect themselves against vendors or suppliers that violate child labor laws or

---

Smedinghoff, *Security Breach Notification—Adapting to the Regulatory Framework*, THE REVIEW OF BANKING & FINANCIAL SERVICES, Dec. 2005, at 12, *available at* http://www.asemec.org/document/document_list.asp?curPage=3&flag=all&fnd=&sfnd_y=&sfnd_m=&efnd_y=&efnd_m=&zId=2&sId=&cNo=3&cType=4&sndMenu=&sortBy=no&ccNo= (last visited Nov. 10, 2007).

[14] Erin S. Davis, *A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet*, 12 WASH. U. J.L. & POL'Y 201, 201 (2003) (stating that the difficulty of developing cyberspace remedies lies in the radically divergent legal traditions of countries connected to the Internet).

[15] 15 U.S.C. §1741, 7262 (2007).

[16] Health Information, Portability & Accountability Act, 42 U.S.C. §§ 1320d-2, 1320d-4 (2007).

environmental standards.[17] Outsourcing information or data processing "does not relieve a company" of its security obligations.[18]

This article argues for a general standard of care that requires the implementation of reasonable information security practices to protect against unauthorized access. Courts should strike down exculpatory clauses on public policy grounds because data handlers perform a necessary service of great importance to the public.[19] Exculpatory clauses are entirely appropriate for hazardous recreational activities such as skydiving but should not be enforceable for information security breaches. Recreational activities such as skydiving are wholly optional in every way. Consumers who engage in such recreational activities do so by choice and assume the attendant risk; in contrast, consumers have no ability to control or change the data flow crossing international borders. A consumer is dependent upon the ability of the company he or she contracts with to adopt reasonable information security practices. Therefore information security should not be able to be disclaimed or waived.[20] Consumers, unlike companies, are not in a position to bargain over the nature of the computer security employed in transmitting their personal data.[21]

A growing number of state and federal statutes already require companies to notify customers of data theft. The duty to disclose should be extended to a general duty to secure their computer systems and to safeguard customer data. Private consumers should be armed with a private cause of action in the event a company fails to incorporate cost-justified precautions to secure their computer systems. Similarly, companies that outsource data should be found negligent for failing to conduct reasonable security audits of any party in the distribution chain that handles consumer or company data. While there are many competing ways to set the standard of care for computer

---

[17] Howard B. Whitmore, *You've Outsourced the Operation, But Have You Outsourced the Risk*, http://www.mmc.com/knowledgecenter/MarshOutsourcing.pdf.

[18] Smedinghoff, *supra* note 13 (contending that outsourcing company has a continuing duty of care to provide adequate computer security).

[19] The Wisconsin Supreme Court defined exculpatory clauses as those "which relieve a party from liability for harm caused by his or her own negligence." Merten v. Nathan, 321 N.W.2d 173, 176 (1982).

[20] Smedinghoff, *supra* note 13 (the author reviews both state and federal law provisions that require security breach notification).

[21] Richards v. Richards, 513 N.W.2d 118, 128 (1994) (explaining that exculpatory clauses should not be enforced where there is no "opportunity to bargain").

security, the famous Learned Hand risk/utility formula is the most appropriate test of negligent computer security.[22] In order to pass the Learned Hand test, companies need to implement reasonable security to eliminate excessive, preventable dangers. Learned Hand's risk/utility test will supplement but not supplant the negligence standard used by industries which already recognize a duty to implement reasonable computer security imposed by statute or as negligence *per se*.

II: FORGING A DUTY OF CARE TO PROTECT THIRD PARTIES FROM DATA THEFT

A. LEARNED HAND'S RISK/UTILITY FORMULA

A company's failure to secure financial data, which results in injury to a consumer, will violate the Gramm-Leach-Bliley Act if the company has not implemented a comprehensive information security program.[23] In the future, consumers can use such statutes to argue that a company's actions are *negligent per se*.[24] *Negligence per se* is a particularly powerful tool in the hands of a plaintiff because the statutory violation is used to prove both the duty and the breach of the standard of care for information security. No plaintiff has successfully employed a *negligence per se* argument in a computer security case. It is arguable that Congress did not intend to provide private plaintiffs with a cause of action.[25] In the absence of a statutorily defined duty to maintain adequate computer security, injured consumers will likely turn to the common law of negligence.

The modern approach to negligence adopts the Learned Hand test, first articulated in *United States v. Carroll Towing Co.*,[26] which requires that fact finders determine whether the burden of precautions prohibitively exceed the expected costs of accidents or injuries. In

---

[22] A consumer injured by a company's failure to give notice of a security breach already has a *negligence per se* cause of action. However, no court has permitted a consumer to use federal or state statutes in a lawsuit based upon the failure to implement reasonable security.

[23] 15 U.S.C. §§ 6801, 6805 (2007).

[24] Posting of Julie Michal-Fulks to Scott & Scott, LLP, http://blawg.scottandscottllp.com/businessandtechnologylaw/2007/08 (Aug. 20, 2007, 09:03 CST).

[25] *Id.*

[26] 159 F.2d 169 (1947).

Carroll Towing, a barge named "Anna C" sunk when it was struck by a breakaway barge that escaped from its moorings due to a strong wind that exacerbated the negligence of Carroll Towing's employee in improperly securing its tethering lines.[27] The trial court found that the Anna C's owner was contributorily negligent for failing to have someone aboard to reduce the damage to other vessels if the barge broke away.

Judge Learned Hand noted that because there was no general industry rule that required having an attendant on board at all times, the barge owner's duty was a function of three variables: (1) the probability that a vessel would break away; (2) the damages or resulting injury if it did; and (3) the burden of the adequate precaution.[28] The Learned Hand formula dictates a finding of negligence, "if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether $B < P * L$."[29] If the damage could be avoided by taking precautions at very little cost, then, even if the risk is slight, the safety step is cost-justified because the burden, B, is less than the probability of the accident multiplied by the gravity of the injury.

While Judge Learned Hand did not apply either empirical data or expert testimony to quantify these variables, he nevertheless apportioned liability because the owner of the Anna C could have taken cost-justified precautions.[30] The American Law Institute adopted a modified version of the Learned Hand test in the *Restatement (Second) of Torts*, which defines negligence as an activity in which the magnitude of the risk outweighs the utility.[31] A low

---

[27] *Id.* at 171.

[28] *Id.* at 173.

[29] *Id.*

[30] In *Carroll Towing*, the court apportioned damages between the defendant and the careless plaintiff who failed to take cost-justified precautions. *Id.* As Judge Posner notes: "It is a bedrock principle of negligence law that due care is that care which is optimal given that the potential victim is himself reasonably careful; a careless person cannot by his carelessness raise the standard of care of those he encounters." McCarty v. Pheasant Run, 826 F.2d 1554, 1557-58 (7th Cir. 1987).

[31] Unreasonable risks are those of "such magnitude as to outweigh what the law regards as the utility of the act . . . ." RESTATEMENT (SECOND) OF TORTS, § 291 (1965).

probability risk that would result in limited damage does not justify costly precautions.[32]

B. EXTENDING THE LEARNED HAND FORMULA TO NEGLIGENCE THAT ENABLES DATA THEFT

The Learned Hand formula is flexible enough to set the standard of care for a broad range of negligent data handling scenarios. Learned Hand's risk/utility formula can be readily adapted to set a standard of care for computer security because the total costs and probability of computer security breaches can be compared to the cost of instituting strong security measures. The cheaper the information security precaution, the greater the risk of data theft and the greater the harm caused by the cybercriminal, the more likely it is that the failure to take the precaution was negligent.

The first step in applying a risk/utility test for data negligence is to define the radius of the risk signified by "P" in the Learned Hand formula. Two kinds of probabilities must be determined. First, there is the probability that data will be lost or stolen due to a company's failure to implement comprehensive security solutions. Second, there is the probability that data will be accessed and misused by third-party criminals. As the probabilities of both of these events increases, the duty to take precautions also increases. If the events have a low probability of occurring then the burden of an extensive precaution is not cost-justified. A company laptop stolen in the course of a routine home burglary presents a low-level probability that the information on the computer will be exploited because the common thief has no interest in misappropriating data. In contrast, an organized cybercriminal group that hacks into a company's website is likely to exploit purloined credit card numbers since the thieves are targeting information, not tangible property.

The second step is to determine the "L" in the Learned Hand formula, which is the potential loss if the company fails to invest in the precaution that would have prevented the loss. Companies are more likely to be required to enhance data security where the potential losses due to data theft are unacceptably high. The misappropriation of trade secrets due to negligently secured software, for example,

---

[32] Blyth v. Birmingham Waterworks, 11 Exch. 781 (1856) (finding that the defendant was not liable for having failed to take precautions to prevent water mains from freezing due to an unprecedented cold snap).

poses the risk of substantial and irreparable harm because these intangible assets are often a company's crown jewels.

A company is only negligent in Learned Hand's formula if the burden of precaution ("B") is less than the estimated costs of a data intrusion ("P * L"). Therefore, under the formula B < P * L, a company is negligent in failing to take cost-justified precautions when the burden of the precaution: employing encryption, enhanced employee training, or other security measures, is less than the probability of data theft multiplied by the loss that results from data theft. The Learned Hand formula is of greater analytical than operational significance because precise empirical data for "operationalizing" these variables rarely exists.[33]

Predicting the true cost of a data breach is challenging because it is difficult to accurately estimate the costs created which may include: lost employee productivity, legal fees, call centers, and the loss of future customers, before the breach takes place.[34] A recent empirical study conducted by Forrester Research Inc. concludes that the average security breach costs between $90 and $305 per lost record.[35] An earlier survey of senior executives in domestic corporations, released in 2006, provides additional data about the cost of security breaches.[36] Respondents estimated the average direct cost of a data breach to be $4.7 million; amounts ranged from $226,000 to $22 million. The direct incremental costs included $54 per lost record, which was an increase of 8% over 2005.[37] These estimates only include directly measurable costs, not the additional expenses of lost executive time,

---

[33] *McCarty*, 826 F.2d at 1557 (noting that "the parties do not give the jury the information required to quantify the variables that the Learned Hand Formula picks out as relevant. That is why the formula has greater analytic than operational significance. Conceptual as well as practical difficulties in monetizing personal injuries may continue to frustrate efforts to measure expected accident costs with the precision that is possible, in principle at least, in measuring the other side of the equation -- the cost or burden of precaution.").

[34] Sharon Gaudin, *Security Breaches Total $90 to $305 Per Lost Record*, INFORMATION WEEK, April 11, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=199000222 (last visited Nov. 6, 2007).

[35] Sharon Gaudin, *How Much Would Data Theft Cost You? Calculate it Online*, INFORMATION WEEK, April 11, 2007, http://www.informationweek.com/software/showArticle.jhtml?articleID=199000336 (last visited Nov. 6, 2007).

[36] Ponemon Institute, LLC, *2006 Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions*, 2006, at 2, *available at* http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf.

[37] *Id.*

foregone business opportunities, litigation expenditures and various other high costs.[38]

The radius of the risk of data intrusion has dramatically increased with the rise of computer-based data networks and thus, the burden of precaution can be staggering. While the cost of encrypting data may be easily cost-justified, many other measures such as enhanced employee training, outside security consultancies, data monitoring, and security audits of every party in a data transmission stream are enormously expensive.

While reliable data on the incidence of security intrusions is not available, courts can take judicial notice of the number of high profile data intrusions in recent months. A security firm recently developed a cost calculator for measuring the scope of negative financial impact in identity theft or data breach scenarios. This cost calculator can be adapted to produce the cost element in the Learned Hand formula. This calculator automatically generates "an average cost, and a plus/minus 20% range, for expenses associated with internal investigation, notification/crisis management and regulatory/ compliance if the incident at issue were to give rise to a class action claim" based on the number of affected records.[39] For a company, the foreseeable costs include attorneys fees, computer consultant costs, payments to outside security experts, fortified data security solutions, augmented data monitoring, customer support, call center monitoring, certified mail notification to victims of data loss, media management, regulatory compliance and the possibility of FTC penalties or fines from other state or federal entities.[40] The cost calculations will be more complex for outsourced data because of political uncertainties, employment policies and workplace conditions in Third World countries.[41] The next section applies the Learned Hand formula to the most common recent data intrusions which have occurred within U.S. borders.

---

[38] *Id.* at 8 (Indirect productivity costs for lost employee productivity were estimated at $30 per record or $800,000. Customer opportunity costs including brand damage and impact on new business was projected to be $98 per record or $2.6 million per company.).

[39] Tech404, *Data Loss Calculator*, http://www.tech-404.com/calculator.html (last visited Nov. 6, 2007).

[40] *Id.*

[41] Part II will explore the problems of calibrating risks when data is outsourced to Third World back office operations.

C. APPLYING THE LEARNED HAND FORMULA TO INTERNET-RELATED DATA THEFT

The first wave of computer security lawsuits stemmed from claims alleging that defective software offered inadequate security and was unreliable in protecting network perimeters.[42] California consumers filed a class action lawsuit in State superior court against CardSystems Solutions, Inc., alleging that the financial service company's lax computer security led to the wholesale misappropriation of credit and debit cards.[43] Intruders gained unauthorized access to forty million credit cards and transferred data from 200,000 individual cards in the CardSystems's computer network. The plaintiffs' complaint charged the financial services company with unreasonable data handling practices and negligent computer security, which included the company's failure to maintain properly configured firewalls and its failure to encrypt confidential customer data.[44] The complaint also charged the financial services firm with violating a California statute requiring it to inform customers of computer intrusions that compromise their personal data. In September 2005, the California Superior Court ruled against the plaintiffs in Cardsystems, holding that the credit card companies were not required to give individual notices informing customers that their credit card information had been compromised.[45]

Plaintiffs' attorneys are beginning to conceptualize and articulate a duty of care owed by data handlers when consumer's personally identifiable information is compromised. Class action suits against

---

[42] Gary H. Anthes, *The Dark Side—Looming Threats for the Future of IT*, COMPUTERWORLD, Mar. 7, 2005, *available at* http://www.computerworld.com/managementtopics/management/story/0,10801,100176,00.html?from=story_package (last visited Nov. 6, 2007).

[43] Complaint for Declaratory and Injunctive Relief and Damages, Parke v. CardSystems Solutions, Inc., No. CGC05-442624 (Cal. Super. Ct. July 5, 2005), *available at* http://www.techfirm.com/cardsystems.pdf [hereinafter CardSystems Complaint] (last visited Nov. 6, 2007).

[44] *Id.*

[45] Posting of K. M. Das to Privacy and Law Blog, http://www.privsecblog.com/archives/litigation-california-court-rules-that-personal-notification-not-required-in-cardsystems-data-breach-case.html (Sept. 26, 2005) (In "[a] San Francisco Superior Court, Judge Richard Kramer ruled that Visa and MasterCard do not have to send individual notices to thousands of their customers in California based on the CardSystems data breach that occurred between August 2004 and May of this year.").

Reed-Elsevier's LEXIS/NEXIS[46] and ChoicePoint Inc.[47] were filed for failing to implement security that might have prevented the theft of customers' personally identifiable information.[48] A growing number of federal agencies require companies to notify consumers or other users of security breaches.[49]

After computer hackers compromised the credit card information of customers of BJ's Wholesale Club Inc., BJ's entered into a consent agreement with the Federal Trade Commission in which it agreed to develop a comprehensive plan to protect the security of its customers.[50] This increase in activity by the state and federal courts and the Federal Trade Commission illustrates a growing willingness to impose on companies a duty to implement reasonable software security practices. The Gramm-Leach-Bliley Act, for example, requires companies to establish information security programs, which is the functional equivalent of a reasonable information security standard of care:

> *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and

---

[46] Jeff Ostrowski, *West Palm Bank to Pay $50 Million in Privacy Case*, PALM BEACH POST, Aug. 1, 2006 (describing potential class action against ChoicePoint, Experian, LexisNexis, First American Corporation and a number of other companies for inadequate data security).

[47] Caleb Silver, *ChoicePoint Execs Cash Out Amid Breach*, CNNMONEY.COM, Feb. 25, 2005.

[48] Dan Christensen, *Major Information Brokers Face Class Action for Invasion of Privacy*, DAILY BUSINESS REVIEW, June 24, 2003, http://www.law.com/jsp/article.jsp?id=1056139884864 (last visited Nov. 6, 2007).

[49] "Taken as a group, the state and federal security breach notification rules (as they relate to personal information) generally require that any business in possession of computerized sensitive information about an individual must disclose a breach of the security of such information to such person." Smedinghoff, *supra* note 13 (reviewing state as well as federal law provisions requiring security breach notification).

[50] Federal Trade Commission, *BJ's Wholesale Club Settles FTC Charges*, June 16, 2005, http://www.ftc.gov/opa/2005/06/bjswholesale.shtm (last visited Nov. 6, 2007) (explaining that the failure to encrypt customer data and store consumer information in secure files was an unfair and deceptive trade practice).

> complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.[51]

At present, the duty to provide adequate information security is emerging in a few sectors of the economy such as healthcare and financial services.[52] In the absence of a general duty of information security, tort lawsuits provide the only viable alternative for those victimized by inadequate security precautions. A special advisor to President Bush opined that reform would come through litigation: "We'll see [vendors] getting sued [because] so much of our infrastructure depends on computers that it's unsustainable to hold software companies blameless."[53]

In December of 2006, the TJX Companies discovered that it had been victimized by a data heist of colossal dimensions.[54] The TJX website described the unprecedented data disaster:

> The TJX Companies, Inc. suffered an unauthorized intrusion or intrusions into its computer systems that process and store information related to customer transactions. The intrusion affected the portion of TJX's computer system in Framingham, MA that handles most of our credit card, debit card, check and merchandise return transactions for most of our stores in the U.S., Puerto Rico and Canada, along with a portion of our computer system in the UK that handles credit and debit card transactions for our stores in the U.K. and Ireland. Based on our investigation to date, we believe that our computer systems were first accessed by an unauthorized intruder in July 2005, on subsequent dates in 2005 and from mid-May 2006 to mid-January 2007, but that no customer data was stolen after December 18, 2006. We do not know

---

[51] 16 C.F.R. § 314.1 (2003).

[52] *See generally* Mark Rasch, *Strict Liability for Data Breaches?*, SECURITY FOCUS, Feb. 20, 2006, http://www.securityfocus.com/columnists/387 (last visited Nov. 6, 2007) (discussing statutory standard of care in financial services industry).

[53] Neville Smith, *Insurers May be Hit by a Bad Idea Whose Time Has Come: Class Actions Over Faulty Software Could Land Insurers in a Tangle*, LLOYD'S LIST INT'L, Sept. 23, 2004.

[54] Paul F. Roberts, *Retailer TJX Reports Massive Data Breach: Credit, Debit Data Stolen, Extent of Breach Unknown*, INFOWORLD, Jan. 7, 2007, at 1, *available at* http://www.infoworld.com/article/07/01/17/HNtjxbreach1.html (last visited Nov. 6, 2007).

> who the intruder was, whether there was one or more intruder, or whether there was one or separate intrusions.[55]

The massive TJX breach, which resulted in the compromising of an estimated forty-five million credit card records, illustrates the enormous radius of the risk presented by data loss in interconnected computer systems.[56] State attorneys general are considering an action against TJX arising from state deceptive trade practices law. The action will weigh "all the factors in this breach, including when and how it was discovered and when it was reported to the authorities."[57] These state attorneys general have no jurisdiction to seek individual relief for consumers, who must sue as private plaintiffs; both banks and individuals have filed suits against TJX for the "negligent" security that enabled this far reaching cybercrime.[58] A consumers' lawsuit contends that "TJX failed to maintain adequate computer data security, which resulted in the exposure of millions of customers' personal financial information. The company's actions put customers at risk for fraud and identity theft and other damages."[59] To prevail in a negligent computer security case against TJX, the plaintiff must prove: (1) a duty of care owed by TJX to the consumer class of victims; (2) TJX's computer security fell below the applicable standard of care that amounts to a breach of that duty; (3) an injury or loss; (4) cause in fact; and (5) proximate, or legal, cause.

Plaintiffs filing a negligent computer security case against TJX will have little difficulty proving that the company owed them an obligation to take reasonable care in protecting their data. These plaintiffs may draw analogies to previous liability cases in which business owners have been held liable for reasonably foreseeable

---

[55] TJ Maxx, Frequently Asked Questions, http://www.tjx.com/tjx_faq.html (last visited Nov. 6, 2007).

[56] Ross Kerber, *TJX Differ on Scam Timeline,* BOSTON GLOBE, April 7, 2007, at E8 (Massachusetts "investigators looking into the theft of more than 45 million credit and debit card numbers from TJX Cos. are trying to determine when the Framingham retailer first learned that its computer systems were compromised.").

[57] *Id.*

[58] Robert Falertra, *Time to Reconsider Big POS Opportunity*, COMPUTER RESELLER NEWS, April 2, 2007, at 56.

[59] Bob Kievra, *Lawsuit Filed Against TJX: Company Director Resigns*, WORCESTER TELEGRAM & GAZETTE, INC., Jan. 30, 2007, at E1.

third-party crimes.[60] They will argue that TJX owes customers a duty of reasonable security to protect against unknown intruders stealing their data just as a business has a duty to protect against third-party criminal attacks on patrons. Premises liability cases, like computer security cases, predicate liability on unsafe conditions. The duty to implement security thwarting third-party cybercrimes should turn on whether the crime was foreseeable.

TJX's attorneys would favor a narrow "specific harm" rule because it would limit the company's liability to the unlikely scenario that the company was aware of specific, imminent threats to their computer system. The "specific harm" rule borrowed from premises liability would find a defender liable only upon proof that the precise crime occurred.[61] For example, a hotel owner would only be liable if the specific harm was that a guest was shot on the premises.[62] The defendant would have no liability absent proof that the precise harm has previously occurred on the premises. A landowner, for example, does not have a duty to protect customers from violent crimes unless the owner is aware of a particular threat from a third-party criminal.[63] The Tennessee Supreme Court applied the Learned Hand balancing test to a premises liability case:

> In weighing the magnitude of harm and the burden imposed upon defendant, the court must consider whether imposing a duty to take reasonable measures to protect patrons from the consequences of criminal acts of third persons would place an onerous burden – economic or otherwise – upon defendants. If it does not, then the court must consider whether the burden outweighs the foreseeability and gravity

---

[60] *See* McClung v. Delta Square Ltd. P'shp., 937 S.W.2d 891, 892 (Tenn. 2006) (reasoning that the duty to protect customers from third party attacks turns on "the foreseeability of harm and the gravity of harm . . . balanced against the commensurate burden imposed on the business to protect against that harm); *see also* Jardel Co., Inc. v. Hughes, 523 A.2d 518 (Del. 1987) (holding merchant liable for negligently failing to provide adequate security and noting that prior criminal attacks ratchets up the duty of care because of greater foreseeability); Foster v. Winston-Salem Joint Venture, 281 S.E.2d 36 (N.C. 1981) (holding mall owner liable for attack on customer because duty was based upon the greater radius of the risk proven by prior criminal attacks in the lot).

[61] Star Wealth Mgmt. Co. v. Brown, 801 N.E.2d 768, 773 (Ind. Ct. App. 2004) (discussing the specific harm test of premises liability).

[62] *Id.*

[63] MARSHALL S. SHAPO, PRINCIPLES OF TORT LAW 99 (2003).

> of the possible harm, so as to preclude the finding of a duty to take reasonable steps to protect patrons. We hasten to point out, however, that the question of duty and of whether defendants have breached that duty by taking or not taking certain actions is one for the jury to determine based upon proof presented at trial. Additionally, if properly raised as a defense, under our doctrine of comparative fault, a plaintiff's duty to exercise reasonable care for her own safety would be weighed in the balance.[64]

In the TJX case, if the Learned Hand theory is applied, the question will be whether the company could have taken cost-effective precautions to prevent the data heist. Under either the Learned Hand test or the risk/utility tests adopted in premises liability actions, a computer security risk is unreasonable and gives rise to a duty to act with due care if the foreseeable probability and gravity of harm posed by the data handler's conduct outweighs the burden upon defendant to implement security measures that would have prevented the harm. The TJX plaintiffs' burden will be to demonstrate a breach of the standard of care if the company did not implement reasonable security audits on a regular basis. The TJX data theft signals the reality that companies will face an increased risk of hackers breaking into company computers that process and store information including payment systems, trade secrets and other proprietary information.

D. APPLYING THE LEARNED HAND FORMULA TO LOST LAPTOPS

To date, most data disasters have occurred as the result of problems such as weak access controls in the terrestrial world rather than from hackers in the ethereal milieu of cyberspace.[65] Companies will need to strengthen access controls to meet industry standards in their specific sector.[66] Sony recently enhanced its computer security

---

[64] *McClung*, 937 S.W.2d at 905.

[65] Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 494 (2006) (presenting empirical findings from study of the first decade of Economic Espionage Act cases demonstrating that the greatest threat was employees or ex-employees as opposed to hackers hacking into computer systems).

[66] A wide variety of standards are evolving in the data security field. In a high security environment such as the military or banking, for example, the standard may be fingerprint recognition. Assa Abloy, *ITG Introduces Smart Card Reader with Fingerprint Recognition*, PRODUCT NEWS NETWORK, June 6, 2007, at 1. Another example of a security standard is the

procedures to comply with Sarbanes-Oxley's requirements as well as reduce the probability of a negligent security lawsuit after audit revealed weaknesses.[67]

The largest category of unacceptable peril in a corporate environment is not Internet-related cybercrime, but the mundane risk of a lost laptop or other data storage device, which accounts for one third of all data thefts.[68] The Learned Hand formula indicates that companies should implement strong encryption coupled with fortified employee training in order to minimize the costs associated with this high probability event. A company can dramatically reduce the risk of data loss from the laptop theft by implementing inexpensive security precautions.[69] The *2007 Annual Study: U.S. Enterprise Encryption Trends* found that, in the opinion of the surveyed executives, encrypting data on laptops, file servers, emails and backup tapes is the accepted standard for data risk reduction.[70] Yet, only 18 percent of the respondents required laptop encryption "most of the time."[71]

The Learned Hand formula balances the probability of lost laptops multiplied by the gravity of the resulting data loss against the burden of encrypting data in order to avoid the harm. Companies are negligent when the burden of encryption is less than the danger arising from lost or stolen laptops. The entity that entrusts data to a data handler will have potential lawsuits against the data handler as well as

---

threefold authentication system "via card, pin, and fingerprint." *Id.* Industry standards are rapidly evolving as vendors market new technologies to ensure authentication, access control and data protection. *See, e.g.*, Press Release, Trapeze Smart Mobile, Trapeze Network Joins Support Trusted Network Connect Initiative (Sept. 19, 2006).

[67] Allen Holmes, *Your Guide to Good-Enough Compliance*, CIO, April 6, 2007, http://www.cio.com/article/102751/The_ROI_of_Noncompliance (last visited Nov. 6, 2007).

[68] Ponemon Institute, *supra* note 36, at 12.

[69] J. Patrick McGregor, *Retailers Must Make Changes to Combat ID Theft*, PITTSBURGH POST-GAZETTE, April 3, 2007, at A8 (Gartner Inc. estimates that a company could encrypt data for as little as $6 per customer account, "compared with 'an expenditure of at least $90 per customer account when data is compromised or exposed during a breach.'" As the price of encryption continues to drop, the duty to implement this reasonable measure will increase.).

[70] Press Release, PGP Corporation, Sponsored U.S. Study Shows Emergence of Strategic Planning and Platform Approach to Encryption (2007), *available at* http://www.pgp.com/newsroom/mediareleases/ponemon_2007.html (last visited Nov. 6, 2007).

[71] *Id.*

any software licensor or developer who introduced code with design defects that enable cybercrime.[72]

Internet-related data thefts have not yet led to successful criminal or civil remedies. An empirical study of all Economic Espionage Act (EEA)[73] prosecutions from the federal criminal statute's enactment in 1996 to August 1, 2005 uncovered fewer than fifty economic or espionage prosecutions filed in federal courts.[74] In addition, "nearly every prosecution was for domestic rather than foreign economic espionage."[75] In a decade of EEA prosecutions, the Department of Justice did not file a single case against a hacker stealing trade secrets by "exploiting known software defects" during an Internet transmission.[76] The gross failure of the EEA to address Internet-related data theft indicates the need to strengthen private tort remedies. The negligent enablement of economic espionage threatens American competitiveness.[77] Tort law gives private litigants incentives to file negligent security lawsuits that benefit the consuming public by uncovering reckless practices.

---

[72] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553 (2005) (proposing a new tort to hold software vendors accountable for defective products and services that pave the way for third-party cybercriminals).

[73] *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839 (2000)); *see also* J. Michael Chamblee, *Validity, Construction, and Application of Title I of Economic Espionage Act of 1996*, 177 A.L.R. FED. 609, 617-18 (2005) (The EEA was enacted to fill a gap in the law. "Other federal statutes, such as the National Stolen Property Act, 18 U.S.C. § 2314, and the Mail and Wire Fraud Statutes, 18 U.S.C. § 1341 and 18 U.S.C. § 1343, were also of limited use in combating the problem of economic espionage.").

[74] Rustad, *supra* note 65, at 458.

[75] *Id.* at 494.

[76] *Id.* at 461 ("At present, the injured targets of trade secret theft have no federal civil remedy for the foreseeable consequential damages of economic espionage. Under the tort of negligent enablement, a third-party software vendor or other data intermediaries would only be civilly liable in federal court if they knew or should have known of vulnerabilities in software or network design facilitating espionage. In the first decade of EEA prosecutions, no outside hacker was prosecuted for misappropriating trade secrets by exploiting known software defects.") (Civil tort liability for the negligent enablement of trade secret theft on the Internet would supplement lax public enforcement of state-sponsored economic espionage).

[77] *Id.* at 527.

III. RISKY DATA HANDLING PRACTICES IN THIRD WORLD BPOS

A. INDIA'S UNSECURE DATA HANDLING PRACTICES

The radius of the risk of stolen data on the Internet is great because hackers can compromise any connected computer without adequate security in seconds. "They just sweep the Internet twenty-four hours a day, seven days a week, looking for vulnerabilities, and they will capture all the data they can and sort through it later."[78] Any offshore data transfer to a Business Process Outsourcer ("BPO")[79] poses potential harm. The firm that "outsources" data must carry out due diligence both through inspection and staff training in off-shore facilities in order to protect its outsourced data.

The first high profile data misappropriation incidents occurring in Third World BPOs occurred in India, the world's largest outsourcing data hub. India's data outsourcing industry continues to expand at a rapid rate and that growth has helped the Indian economy grow nine percent in a recent year.[80] India is particularly susceptible to charges of lax computer security even though its call centers have recently strengthened data safety precautions to protect against insider data theft.[81] The sun never sets on an Indian-based BPO; Indian call centers and data processors manipulate consumer data twenty-four hours a day, seven days a week. The practical result of domestic companies outsourcing call centers to India is to place unprecedented

---

[78] Richard Krantz, *Industrial Espionage Becomes Favorite Way to Achieve Gains*, VOICE OF AMERICA NEWS, April 29, 2005, at 1.

[79] BPO India.org, *BPO (Business Process Outsourcing)*, http://www.bpoindia.org/ (last visited Nov. 6, 2007) (A call center is an example of a BPO that is sometimes referred to as a back office operation. A growing number of companies are outsourcing diverse information-based activities. An Indian organization notes the list of functions outsourced is growing: "Call centres apart, functions outsourced span purchasing and disbursement, order entry, billing and collection, human resources, administration, cash and investment management, tax compliance, internal audit, pay roll . . . the list gets longer everyday.").

[80] Jared Sandberg, *It Says Press Any Key, Where's the Any Key?*, WALL ST. J., Feb. 20, 2007, at B1 *available at* http://online.wsj.com/public/article/SB117193317217413139.html (last visited Nov. 6, 2007).

[81] Pete Engardio et al., *Outsourcing: Fortress India? Call Centers and Credit-Card Processors are Tightening Security to Ease U.S. and European Fears of Identity Theft*, BUS. WK., Aug. 16, 2004, at 28.

access to confidential personal and financial data being placed in the hands of low paid, remote workers.[82]

The employee turnover in India's BPOs is extremely high, which greatly increases the possibility that insiders will exploit their trusted position.[83] Data thieves in Pune, India misappropriated $426,000 by registering false e-mail addresses in the names of their U.S. victims.[84] Call center employees based in India were able to manipulate customers "into unwittingly divulging passwords and pin numbers over the phone."[85] In 2005, a British television journalist accused "India's outsourcing industry [of being] infested with hackers and identity thieves."[86] The reporter illustrated the potential for data theft by Indian employees who allegedly purchased hundreds of UK-based banking customers' personally identifiable information.[87] In the wake of this exposé, members of Britain's Parliament called for a halt on the sending of consumer data to India because of concerns over inadequate security.[88]

British companies are beginning to withdraw their "back-end office operations from India" partly because "Indian cyberlaw, namely the Information Technology Act of 2000, has been grossly inadequate on the deal with complicated challenges concerning data protection."[89] A U.S. Trade Official contends: "India needs to have a credible data protection regime in its own interest."[90] Acme Tel Power Limited, for

---

[82] Samantha Grant, *I Just Bought a Flat Screen T.V. in Kolkata?*, 11 PGH. J. TECH. L. & POL'Y 1, 4-5(2006).

[83] Sandberg, *supra* note 80.

[84] Grant, *supra* note 82, at 1–2.

[85] *Id.* at 2.

[86] *India Weighs Tougher Cybersecurity Laws After TV Expose*, COMMWEB, Oct. 6, 2006.

[87] Andy Mukherjee, *Globalizing Law and Order*, INT'L HERALD TRIBUNE, Jan. 11, 2007, at 16.

[88] *British MPs React to Outsourcing Security Breach*, OUTSOURCING TIMES, June 24, 2005, http://www.blogsource.org/2005/06/british_mps_rea.html (last visited Nov. 6, 2007).

[89] *Need for Fast Track Action in Case of Data Security Breaches*, FINANCIAL EXPRESS, Oct. 7, 2006, at 1.

[90] *U.S. Says India Needs to Have Credible Data Protection Regime*, THE PRESS TRUST OF INDIA, Oct. 6, 2006, at 1.

example, closed its outsourcing operations in India because of the company's concern that its data was not secure.[91]

It is clearly unfair to single out India for lax data handling security. A recent empirical study concluded that India has the best information security practices of any of the top forty outsourcing destinations around the globe.[92] Indian business and government officials are sensitive to international perceptions that the country has weak data protection laws. An Indian attorney specializing in information technology argues:

> [T]he government should seriously consider enacting a special law on data protection on the lines of the OECD [Organization for Economic Co-Operation and Development] guidelines followed by major European countries and the EU Data Protection Directive. The lacunae in the Act provide fuel to the anti-outsourcing brigade in the UK and US to tarnish India's image as an outsourcing hub. It's time the government got its act together and at least implemented the proposed amendments. [The new IT law will make companies] . . . accountable for leakages caused by negligence.[93]

Under mounting pressure from Anglo-American information technology outsourcers, the Indian government "has shown a sense of urgency," proposing civil and criminal liability to make enablers liable for data security breaches for facilitating data security breaches.[94] These legal reforms would assign greater responsibility to Indian companies that fail to implement the reasonable security measures

---

[91] *BPO to Pull Out After Data Theft Case (ACME Tele Power Limited Not Satisfied With the Way the Data Theft Case is Being Handled in India)*, INDIA BUSINESS INSIGHT, Nov. 2, 2006, at 1.

[92] *Fort Knox of Data Security?*, OFFSHORING TIMES, Oct. 14, 2006, at 1 ("For example, the AT Kearney Global Services Location Index 2005 ranks India highest in a detailed analysis comparing 40 sourcing destinations across the world. The fact that India is very secure, from a data protection viewpoint, has also been confirmed by independent surveys by various credible organizations, including the Financial Services Authority and the Banking Code Standards Board, both of the UK.").

[93] Mohammed S. Waris, *Time to Get Our IT Act Together*, FINANCIAL EXPRESS, Oct. 27, 2006, at 1.

[94] *Stiff Penalty for E-Crimes*, THE TIMES OF INDIA, Oct. 18, 2006, at 1.

needed to protect sensitive data.[95] Augmented cybercrime laws, however, are not likely to curb data theft because cybercriminals can easily vanish into cyberspace. The U.S. company that "outsources" is in the best position to ensure that back offices comply with minimum security standards by investing in measures to protect customer data and to redeem trust in their back office operations.

B. THE BPO'S STAKE IN ENHANCED DATA HANDLING SECURITY

Lapses in data protection create a problem of global dimensions. Few countries have laws that are sufficiently robust to comply with European Union minimum data protection standards. India models its constitutional right to privacy on the right the United States Supreme Court has found in the American Constitution; this degree of protection does not comport with European standards because protection is limited to public sector data transmissions.[96] The United States has "only a patchwork of federal and state laws governing data protection."[97] Consistent with United States jurisprudence, in 1996, India's Supreme Court held that a constitutional privacy right exists only against the public sector.[98] Because private industry is not subject to the constitutional right of privacy, Indian civil law should bridge the enforcement gap as the civil law does in the United States.

The European Community achieved greater harmonization of data protection when the European Commission approved the Data Protection Directive, which requires each of the twenty-seven Member States to enact national legislation that protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[99] The European Union's Data Directive forbids the transfer of personal information across national borders without an "adequate level of

---

[95] *Id.*

[96] Christopher Wolf, PROSJAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE §14.5 (2006).

[97] Grant, *supra* note 82, at 5.

[98] Wolf, *supra* note 96, at 14–50.

[99] Council Directive 95/46, art. 1, 1995 O.J. (L. 281/31) (EC); *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

protection."[100] BPOs in India and around the Third World risk losing all of their European outsourcing business unless they can meet the Data Protection Directive's requirement of "adequa[te]" privacy protection standards which ensure reasonable security.[101] Negligent entrustment liability against U.S. outsourcers will help ensure that India's information companies are appropriately sensitive to the need for reasonable data security in their outsourcing activities. In the absence of liability, American firms will be tempted to award data handling contracts to the lowest bidders, which creates excessive, preventable security risks.

A company has a duty of care to prevent, deter or control the theft of data entrusted to Third World back office operations. The traditional duty of reasonable care applies equally well to outsourced data. Outsourcers know or should know that poorly paid and trained Third World data handlers pose a threat of data theft. The Federal Deposit Insurance Corporation (FDIC) released a study documenting the risks of offshoring financial services. The risk of lost data turns on the politics and socio-economics of the destination country along with the following traditional outsourcing risks:

> Operations/Transaction Risk: Weak controls may affect customer privacy.
>
> Compliance Risk: Offshore vendors may not have adequate privacy regulations.
>
> Strategic Risk: Different country laws may not protect "trade secrets."

---

[100] *See id.* at Article 25 (Article 25 addresses the adequate level of protection); *available at* http://www.cdt.org/privacy/eudirective/ EU_Directive_.html#HD_NM_45.

[101] Export.gov, *Welcome to the Safe Harbor*, http://www.export.gov/safeharbor (last visited Nov. 6, 2007) (The European Commission's Directive on Data Protection went into effect on October 1998. The Directive would have prohibited the transfer of personally identifiable data to the United States because only some sectors of the American economy complied with the European standard of reasonable security for privacy protection. "While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a 'Safe Harbor' framework." The U.S. approach is for companies individually to attest to compliance with Europe's data protection standards.).

> Credit Risk: A vendor may not be able to fulfill its contract due to financial losses.
>
> Privacy Concerns Raised by Offshoring: Few legal restrictions exist on financial service companies sending customer data to foreign countries. Financial institution customers may not opt out of these information transfers to nonaffiliated service providers if the transfer is for a purpose described in section 502(e) of the Gramm-Leach-Bliley Act (GLBA). For example, the opportunity to opt out does not apply where the information transfer is to: (1) service or process a financial product or service that the customer requested or authorized; or (2) maintain or service the customer's account.[102]

A consumer could use an outsourcer's failure to implement reasonable security in a negligence-based lawsuit. Any financial institution outsourcing data has a continuing obligation to protect the information from either internal or external threats to security, confidentiality and integrity. This affirmative obligation extends to the "monitoring of the activities of those service providers to which financial institutions transfer customer information."[103]

Privacy risks correlate directly with the job types in the back office operation. For instance, relatively low risk activities include computer source coding or application development and maintenance, whereas high risk activities include any function using personal data, such as call centers or transaction processing. At present, financial institutions are primarily offshoring low-risk IT work in addition to higher-risk, customer database type work, including mortgage servicing and customer-assistance/help-desk services.

C. APPLYING THE LEARNED HAND FORMULA TO BPO OUTSOURCING LIABILITY

Outsourcing data does not outsource liability. In order to reduce their exposure to data lawsuits, U.S. companies must either closely

---

[102] Federal Deposit Insurance Corporation, *Offshore Outsourcing of Data Services by Insured Institutions and Associated Privacy Risks*, http://www.fdic.gov/regulations/examinations/offshore (last visited Nov. 6, 2007).

[103] *Id.*

monitor BPOs or close these Third World data operations. Courts should factor security lapses such as recent thefts of data from BPOs into Learned Hand's foreseeability of danger equation. However, even if best information security practices set the floor, they do not set the ceiling of due care given the current laxity of industry standards. Compliance with a weak industry practice of entrusting confidential data to offshore BPOs without due diligence is not a good test for reasonable care.

In *The T.J. Hooper* case, Judge Learned Hand ruled that an industry custom of not having radios aboard barges was negligent even though this precaution had not been widely adopted in the late 1920s.[104] Judge Hand rejected the barge owners' argument that they were not negligent because their industry had not yet generally adopted radio receiving sets as a standard feature, finding that a "whole calling may have unduly lagged in the adoption of new and available devices."[105] Neither liability standards nor industry standards have been promulgated to compel companies to do the most elementary due diligence before transmitting data to Third World information processors. However, the lack of an industry standard should not bar recovery under Judge Learned Hand's formulation.

The *T.J. Hooper* decision stands for the proposition that mere compliance with industry custom is not a shield against negligence. An information industry may unduly lag in its adoption of new and available security solutions. Just because a software vendor complies with inadequate industry customs does not mean it escapes liability. In many sectors of the information economy, standards of security are in their infancy. The wireless computer network industry has yet to develop security standards that could serve as a surrogate for negligence.[106]

Companies can only use custom as a reliable legal defense when common prudence equals reasonable prudence. It is premature to defer to ill-formed data security standards since even a standard for encryption is not settled. Certifying organizations such as the National Institute of Standards or voluntary industry groups must step in to bridge the gap by developing consensus-based security standards to protect outsourced voice, video, fax and data traffic. Since private

---

[104] *The T. J. Hooper*, 60 F.2d 737 (2d Cir. 1932).

[105] *Id.* at 740.

[106] Drew Clark, *Cyber Security: White House Aide Criticizes Progress Toward Internet Security*, NAT'L J.'S TECH. DAILY, July 30, 2002, at 1.

industry standards are relatively undeveloped for the data handling industry, best practices are not an effective shield against negligence claims.

High profile disasters have led to two varieties of negligent data handling claims: negligent enablement and negligent entrustment actions. In a negligent enablement case, the defendant's act or omission in failing to protect customer data results in data theft. These data disasters generally are attributable to some combination of lax laptop policies, encryption failures, misplaced disks and data stolen by dishonest employees. In contrast, in a negligent entrustment case, the data handler has outsourced handling functions to thirds parties, frequently to back office operations in Third World countries.

A BPO located in Bangladesh or Beijing will typically be beyond the reach of the American legal process but plaintiffs can file "negligent entrustment" claims against the outsourcer that failed to supervise off-shore entities. Whether the case is a negligent enablement or a negligent entrustment claim, the required elements are the same: duty, breach, causation and damages. A court will enter summary judgment or dismiss the plaintiff's claim in a negligent data handling case unless the claimant proves: (1) the data handler owed the plaintiff a duty of care, (2) the data handler breached that duty, (3) the plaintiff sustained tangible, present damages and (4) the breach of the duty proximately caused the damage.

IV. EMERGENT NEGLIGENT DATA CAUSES OF ACTION

A. NEGLIGENT ENABLEMENT FACT PATTERN

To date, the victims of data theft have been unsuccessful in pursuing claims against data handlers for failure to secure personal or company information. In *Guin v. Brazos Higher Education Services*, a company negligently permitted one of its employees to store unencrypted private customer data on a laptop computer that was later stolen.[107] Brazos sent a notification letter warning about the laptop theft to all of its approximately 550,000 customers.[108] One of Brazos' customers filed suit based upon breach of contract, breach of fiduciary duty and negligence. The aggrieved customer produced no evidence that a third party had accessed his personal information; much less that

---

[107] Guin v. Brazos Higher Educ. Serv. Corp., 2006 U.S. Dist. LEXIS 4846 (D. Minn. 2006).

[108] *Id.* at *4.

he was a victim of fraud, identity theft or any other damages.[109] The court granted the defendant's summary judgment motion because of the plaintiff's failure to trace cognizable damages arising from the defendant's breach of the standard of care. The negligence formula requires the plaintiff to demonstrate a present and actual injury that resulted from the negligent security practices, which the plaintiff in *Brazos* failed to do.

Plaintiffs do not satisfy the injury requirement by pointing to the possibility that their personal data might be exploited by an identity theft in the future. Anticipated injury or fear of a future cybercrime is insufficient to meet the injury requirement. "A plaintiff may recover damages for an increased risk of harm in the future [only] if such risk results from a present injury and indicates a reasonably certain future harm."[110] As the Minnesota federal court stated, "future harm, not yet realized, will not satisfy the damage requirement."[111]

B. NEGLIGENT ENTRUSTMENT FACT PATTERN

Forbes v. Wells Fargo Bank, N.A is a typical negligent entrustment case.[112] Subsidiaries of Wells Fargo hired a third-party service provider to print monthly statements for home equity mortgage and student loan customers. Computers containing Wells Fargo's customers' unencrypted names, addresses, Social Security numbers and account numbers were stolen from the contractor.[113] Two customers filed suit against Wells Fargo, although there was no evidence that the purloined information was either accessed or used. The plaintiffs' principal theory was that Wells Fargo's contractor negligently failed to implement adequate security to protect their account information.[114] The court granted summary judgment in favor of Wells Fargo because the plaintiffs were unable to demonstrate a present injury, which is a requirement of a negligence claim. A

---

[109] *Id.* at *5.

[110] Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006).

[111] *Guin*, 2006 U.S. Dist. LEXIS at *13 (citing Reliance Ins. Co. v. Anderson, 332 N.W.2d 604, 607 (Minn. 1982)).

[112] *Wells Fargo*, 420 F. Supp. 2d at 1018.

[113] *Id.* at 1019.

[114] *Id.* at 1021.

plaintiff must suffer some actual loss or damage in order to bring an action for negligence.

C. NO HARM, NO FOUL

In both the negligent enablement and entrustment examples, the court granted the defendants' summary judgment because of the plaintiffs' failure to prove present damages. Plaintiffs' attorneys have unsuccessfully attempted to overcome the "present injury" barrier by arguing that consumers may be identity theft victims in the future. No plaintiff has been successful in receiving an award to compensate for lost data where identity theft has not yet occurred.

Perhaps this area of law will continue to develop along the lines of toxic torts law. In toxic torts cases, plaintiffs who have no present injury but only suffer the threat of a future injury cannot meet the injury requirement necessary in negligence-based actions.[115] Courts are split on the issue of whether a plaintiff must demonstrate a "present injury" as a predicate for a medical monitoring claim.[116] Courts may be reluctant to recognize negligent computer security claims where a consumer's data has been stolen until there is empirical or objective evidence of an economic or other loss under the "present injury" requirement. The victims of data theft will not have a viable claim unless courts recognize that the mere compromise of data constitutes a present injury. In medical monitoring cases, the victim of a toxic exposure may not have a full-blown injury but nevertheless has the financial burden of frequent testing and medical examinations. Every right has a remedy and therefore a consumer whose personal data is compromised incurs costs to mitigate identity theft. A consumer, for example, would incur costs in closely monitoring credit reports and taking other steps to mitigate losses. The victims of a widespread data theft such as the TJX case could form a "monitoring class" roughly

---

[115] Metro-North Commuter R.R. v. Buckley, 521 U.S. 424 (1997) (holding that a railroad worker negligently exposed to asbestos, but without symptoms of any disease, cannot recover under the Federal Employers' Liability Act for negligently inflicted emotional distress unless he manifests symptoms of a disease).

[116] Paul A. Locke & Patricia I. Elliott, *Caveat Broker: What Can Real Estate Licensees Do About Their Potentially Expanding Liability for Failure to Disclose Radon Risks in Home Purchase and Sale Transactions?*, 25 Colum. J. Envtl. L. 71, 108 (2000) (noting that "the courts are split on whether a present injury must accompany a medical monitoring claim").

paralleling consumers implanted with a defective medical device that has not yet injured them.[117]

Several other courts also have found that plaintiffs had no basis for using criminal statutes as a surrogate for negligence.[118] For example, in *Stollenwerk v. Tri-West Healthcare Alliance*, a health care company's corporate office was burglarized and a number of items were stolen, including computer hard drives containing the personal information of the defendant's customers.[119] The Arizona court rejected the plaintiffs' tort claims on the grounds that the plaintiff was unable to prove a cognizable injury.[120] The *Stollenwerk* court noted that "an increased risk of experiencing identity fraud for the next seven years" was not enough to satisfy the injury requirement for negligence.[121] The speculative threat of future harm, not yet materialized, will not satisfy the damage requirement of negligence in either enablement or entrustment cases.[122]

Most recently, in *Randolph v. ING Life Ins. & Annuity Co.*, employees filed a class action lawsuit after a company representative's computer, which contained private personal information, was stolen in a home burglary.[123] The plaintiffs' class action suit asserted claims for invasion of privacy, gross negligence and ordinary negligence.[124] The D.C. District Court found that the plaintiffs lacked standing because they could not prove an injury in fact.[125] The plaintiffs were unable to overcome the present injury requirement pleading that the data breach

---

[117] *See, e.g.*, Grovatt v. St. Jude Med. Inc., 425 F.3d 1116 (5th Cir. 2005) (describing "medical monitoring class" of consumers implanted with prosthetic heart valves which have not yet failed).

[118] *Id.*

[119] Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. 2005).

[120] *Id.* at *4.

[121] *Id.* at *5.

[122] Plaintiffs have failed to demonstrate a cognizable injury in a number of other cases in which data was lost or stolen. *See, e.g.*, Giordano v. Wachovia Sec., LLC, 2006 U.S. Dist. LEXIS 52266 (D.N.J. 2006); Bell v. Acxiom Corp., 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. 2006); Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).

[123] Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 2–3 (D.C. Cir. 2007).

[124] *Id.* at 2.

[125] *Id.* at 10.

constituted an invasion of privacy and breach of fiduciary duty. The court dismissed these causes of action on the grounds that they were not in the plaintiffs' original complaint depriving the defendant of notice. It is unclear whether privacy-based torts or fiduciary duty claims can be a way to side-step the present injury problem. The court ruled that the plaintiff's complaint did not comply with the notice requirements of the Federal Rules of Civil Procedure, but noted that it was of "no consequence" because they failed to allege an "actual or imminent" injury in fact.[126] To date, no plaintiff has been successful in a data theft case because courts do not consider the possibility of identity theft a legally cognizable injury.

D. ECONOMIC LOSS RULE

In *East River S.S. Corp. v. Transamerica Delaval, Inc.*, the Court held that a plaintiff could not recover for tort damages in admiralty for losses resulting from the defective design of main propulsion units used in four oil-transporting supertankers.[127] The Court stated, "[c]ontract law, and the law of warranty in particular, is well suited to commercial controversies of the sort involved in this case because the parties may set the terms of their own agreements setting the responsibilities of a seller of a product that fails to perform the function for which it was intended."[128] The Court precluded the plaintiffs from suing in tort since the only damages were economic loss, from harm to the malfunctioning turbines, rather than harm to collateral property or an individual.[129]

In the wake of *East River*, courts have stretched this economic loss rule (ELR) beyond products liability to a wide variety of cases where there is no collateral property damage or personal injury.[130] The

---

[126] *Id.* at 9.

[127] E. River S.S. Corp. v. Transamerica Delaval, 476 U.S. 858, 872–73 (1986).

[128] *Id.*

[129] *Id.* at 876.

[130] *See, e.g.*, Coastal Conduit & Ditching, Inc. v. Noram Energy Corp., 29 S.W.3d 282, 290 (Tex. App. 2000) (that a contractor's claim for increased costs because of a gas company's failure to properly mark or install pipelines was barred by the economic loss rule); Transport Corp. of Am. Inc. v. IBM Corp., 30 F.3d 953, 957 (8th Cir. 1994) (extending the economic loss rule to bar a tort claim where a defective electronic disk drive was integrated into a computer system); *see also* Anita Bernstein, *Keep It Simple: An Explanation of the Rule of No Recovery for Economic Loss*, 48 ARIZ. L. REV. 773 (2006); Jane Stapleton, *Comparative*

Nevada Supreme Court described the path of the economic loss rule in a case extending the doctrine to home construction cases:

> [T]he economic loss doctrine arose, in large part, from the development of products liability, but its application is broader and serves to maintain a distinction between contract and tort principles . . . . We conclude that damages sought in tort for economic losses from a defective building are just as offensive to tort law as damages sought from economic losses stemming from a defective product.[131]

The economic loss rule has created a Maginot Line separating expectation-based contract remedies from tort law arising out of breaches of the standard of care.[132] The underlying jurisprudence supporting the ELR is the concern of liability out of proportion to the defendant's fault.[133] In a typical computer breach case, the economic losses are likely to take the form of consequential damages such as lost profits, the loss of electronic funds or stolen personal identity information.[134]

The rule barring economic loss in tort law precludes both negligent enablement and data entrustment cases where there is a direct contractual relationship between the parties. Even if the plaintiff can prove the elements of negligent entrustment or enablement, courts typically bar the action because there is no loss of life or resulting property damage. The ELR will prevent most companies from recovering for lost proprietary data, trade secrets and lost profits where there is a contractual nexus between the data handler and "entruster."

Economic Loss: Lessons from Case-Law-Focused "Middle Theory," 50 U.C.L.A. L. REV. 531 (2002).

[131] Calloway v. City of Reno, 993 P.2d 1259, 1265-66 (Nev. 2000).

[132] Sidney R. Barrett, Jr., *Recovery of Economic Loss in Tort for Construction Defects: A Critical Analysis*, 40 S.C. L. Rev. 891, 894-95 (1989) ("The economic loss doctrine marks the fundamental boundary between contract law, which is designed to enforce the expectancy interests of the parties, and tort law, which imposes a duty of reasonable care and thereby encourages citizens to avoid causing physical harm to others.").

[133] People Express Airlines v. Consolidated Rail Corp., 495 A.2d 107, 109-110 (N.J. 1985) (explaining how a virtually *per se* rule bars recovery for economic loss unless the negligent conduct also causes physical harm).

[134] Pavlovich v. Nat'l City Bank, 435 F.3d 560, 569 (6th Cir. 2006).

The New Jersey Supreme Court rejected the ELR where the plaintiff class was easily identifiable and the causal connection between the defendant's breach and economic loss was clear-cut.[135] In *People Express v. Consolidated Rail*, the New Jersey Supreme Court permitted an airline to recover for purely economic losses in a case where the railroad negligently caused a chemical fire resulting in the shutting down of the terminal and the cancellation of flights.[136] In *J'Aire Corp. v. Gregory*, the California Supreme Court allowed an airport restaurant operator to recover in tort for purely economic losses arising out of delays in remodeling of an airport due to a contractor's negligence.[137] However, few courts have followed the "highly foreseeable" plaintiffs' exception forged by the *People Express* and *J'Aire Corp* courts.[138]

Even assuming that the plaintiffs can prove a present injury in a data interception case, courts permit no recovery for purely economic losses.[139] However, plaintiffs may be able to file a tort action such as fraudulent inducement. In a data entrustment claim, for example, a Fortune 500 company may have misrepresented its security measures to a prospective customer when the company had not audited a BPO operation. If plaintiffs can prove that they were fraudulently induced to enter into a data-handling contract, they will be able to overcome the ELR since fraud in the inducement is an independent tort.

In *HGI Assocs. v. Wetmore Printing Co.*, the Texas Supreme Court held that tort damages for a fraudulent inducement claim are recoverable even if the misrepresentations are "later subsumed in a contract or whether the plaintiff only suffers an economic loss related

---

[135] *People Express Airlines*, 495 A.2d at 112 (explaining that "the extent to which the defendant knew or should have known the particular consequences of his negligence, including the economic loss of a particularly foreseeable plaintiff, is dispositive of the issues of duty and fault").

[136] *Id.* at 118.

[137] J'Aire Corp. v. Gregory, 598 P.2d 60 (Cal. 1979).

[138] *See* Bernstein, *supra* note 130 at 791.

[139] To date, plaintiffs have not been successful in side-stepping the ELR in negligent data handling cases. *See, e.g.*, Trans States Airlines v. Pratt & Whitney Can., 682 N.E.2d 45, 48 (Ill. 1997) (citing In re Chicago Flood Litigation, 680 N.E.2d 265, 275 (Ill. 1997) (stating, "The event, by itself, does not constitute an exception to the economic loss rule. Rather, the exception is composed of a sudden, dangerous, or calamitous event coupled with personal injury or property damage.").

to the subject matter of the contract."[140] The Court in *HGI Assocs.* further stated that a decision restricting fraud damages to situations in which a plaintiff suffers an injury that is distinct from the economic losses recoverable under a breach of contract claim is inconsistent with Texas law.[141]

Courts have also posited a second exception to the ELR "when the sudden occurrence is highly dangerous and presents the likelihood of personal injury or injury to other property."[142] The ELR would not bar consumer actions for negligent security cases where they have no contractual privity with third-party negligent or reckless data handlers such as Indian BPOs. Nevertheless, third-party actions against offshore data handlers will generally be impractical due to the problems with cross-border jurisdiction, enforcement of judgments and costs.

E. OVERCOMING THE NEGLIGENT ENABLEMENT BARRIER

Courts will need to be innovative to overcome the present injury and ELR barriers to recovery given the increasing radius of the risk of data misuse or misappropriation. In a wrongful death case, the New Hampshire Supreme Court broke new ground when it held a data broker potentially liable for negligent handling of personally identifiable information of a victim killed by a stalker. In *Remsburg v. Docusearch, Inc.*, the representative of the decedent, a young female murder victim, filed a lawsuit against an Internet-based investigative service, which sold information allowing the murderer to locate his victim.[143]

Courts need to revisit both the injury requirement and the ELR to advance the practical goal of providing a remedy for the significant losses posed by data theft despite the absolute bar to recovery currently posed by the ELR. The traditional justification for the ELR is that a plaintiff should not have a negligence-based action where they already have a contract remedy.[144] This policy consideration is simply

---

[140] HGI Assocs. v. Wetmore Printing Co., 427 F.3d 867, 876 (11th Cir. 2005) (citing Formosa Plastics Corp. v. Presidio Engineers & Contractors, Inc., 960 S.W.2d 41, 46 (Tex. 1998)).

[141] *Id.*

[142] Stepan Co. v. Winter Panel Corp., 948 F. Supp. 802, 808 (N.D. Ill. 1996).

[143] Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005-06 (N.H. 2003).

[144] Southwestern Bell Tel. Co. v. Delanney, 809 S.W.2d 493, 495 (Tex. 1991).

not applicable to negligent enablement or entrustment cases because the claimants have no other remedy. In data handling claims, for example, the customer has no contractual remedy against third-party handlers, particularly when the negligent handler is located offshore. Any contractual remedy that a consumer will have against the data handler has often been, in effect, an anti-remedy because of warranty and remedy limitations.[145]

Courts should also be more open-minded when considering the injury of having personal or company data intercepted because of negligent data handling. At a minimum, courts should recognize special damages arising from the need to monitor credit reports and implement augmented security to mitigate the potential costs of identity fraud. Companies should also be able to recoup the costs of informing customers or implementing employee education where they are the victims of data theft.

V. CONCLUSION

Groundbreaking social transformations have always required the reworking of legal doctrine.[146] This article has examined the collision of interests between a consumer and a company's right to data security and the company's obligation to implement reasonable security measures to prevent third-party cybercrimes as well as data theft from laptops and other terrestrial storage devices. At present, consumers and companies have no meaningful remedy for injuries such as the theft of personal data, computer viruses or Internet fraud enabled by software failure.

Courts and legislatures need to be bolder in carving out tort duties to compensate the victims of negligent security because data handlers are in the best position to avoid the peril. In the absence of liability for the negligent enablement of data theft, "immunity breeds irresponsibility while liability induces the taking of preventive

---

[145] Rustad & Koenig, *supra* note 72, at 1611 (contending that consumers have no meaningful warranties and remedies in cyberspace contracts); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1241 (1995) (describing one-sided adhesive contracts in cyberspace).

[146] Courts have reworked the doctrine of premises liability to reflect societal changes. Until the last three decades, courts denied recovery to the victims of third-party criminal attacks on the grounds of no duty owed. *See, e.g.*, Nigido v. First Nat'l Bank, 288 A.2d 127 (Md. 1972). Courts overcame this "no duty" rule on public policy grounds of fairness and the law and economics principle of placing the burden of precaution on the least cost avoider.

vigilance."[147] The extension of Learned Hand's negligence test to computer and Internet security will help to establish the courts' recognition that in order to protect consumers and companies from data theft, it is necessary to increase tort liability.

Data handlers who fail to implement reasonable security or effective perimeter defenses provide an invitation for cybercriminals in distant venues. Despite the fact that companies have a large theoretical negligence exposure under the Learned Hand formula, plaintiffs have not successfully obtained awards against companies or their data handlers.[148] The social and economic costs associated with negligent data handling will not decrease until a stronger liability rule emerges and the courts hold the industry accountable for failing to implement reasonable security.

---

[147] Thomas F. Lambert, Jr., *Suing for Safety*, TRIAL, Nov. 1983, at 48.

[148] Davis, *supra* note 14, at 207 (stating that the difficulty of developing cyberspace remedies is the radically divergent legal traditions of countries connected to the Internet).