AN EXPECTED HARM APPROACH TO COMPENSATING CONSUMERS FOR UNAUTHORIZED INFORMATION DISCLOSURES

by Rachel Yoo*

I. INTRODUCTION

[1] On May 22, 2007, the Executive Office of the President of the United States issued a memorandum concerned with safeguarding personal information, which first defined the term "personally identifiable information" as follows:

> [I]nformation which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[1]

[2] Since then, technological advances have enormously expanded the realm of personally identifiable information, thereby diminishing the distinction between Personally Identifiable Information and non-Personally Identifiable Information.[2] Personally Identifiable Information

* J.D., 2012, Indiana University Robert H. McKinney School of Law. Many thanks to Professor Max Huffman for the generous amount of time he devoted to reviewing this paper and for his consistent, and greatly appreciated, support and encouragement. I am so grateful for his help and truly could not have done this without him.

[1] Memorandum from John Clay III, Deputy Dir. for Mgmt., Office of Mgmt. & Budget, to the Heads of Exec. Dep'ts & Agencies 1 n.1 (May 22, 2007), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

[2] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 35-38 (2010) [hereinafter PROTECTING CONSUMER PRIVACY], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

is information that directly links to one individual, such as a name, address, or Social Security number.[3] On the other hand, non-Personally Identifiable Information is anonymous information, which by itself cannot identify an individual, such as location, web browsing history, and shopping records.[4] However, de-identified data could easily turn into identifiable data. In 2008, Netflix released certain anonymized data about its consumers' movie viewing habits so researchers could improve Netflix's algorithm for recommending films.[5] "Despite Netflix's effort to de-identify the data set, researchers using other publicly available information were able to re-identify specific Netflix customers and associate information about the films they had rented."[6] As demonstrated by this research, any information connected with an individual could constitute personally identifiable information and therefore, distinguishing Personally Identifiable Information from non-Personally Identifiable Information becomes useless.

[3] Data breaches, which involve both Personally Identifiable Information and non-Personally Identifiable Information, take place so frequently that they no longer constitute news.[7] According to the Identity Theft Resource Center, there were 414 breaches exposing 22,945,773

[3] *See id.* at 35.

[4] *See id*; *see also Privacy*, EXPRESS SCRIPTS, http://www.medcohealth.com/medco/consumer/useOfInfo.jsp?articleAppId=HelpCenterCB_Privacy&loc=GNAVHDR&accessLink=medcomedicarehome12 (last updated Sept. 20, 2012).

[5] *See* PROTECTING CONSUMER PRIVACY, *supra* note 2, at 38.

[6] *Id*; *see* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets* 8, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[7] *See generally* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTORS, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTIFY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 11-12 (2007), *available at* www.gao.gov/new.items/d07737.pdf; John Stringer, *Protecting personally identifiable information: What data is at risk and what you can do about it*, SOPHOS, 1 (2010), *available at* http://www.sophos.com/sophos/docs/eng/dst/sophos-protecting-pii-wpna.pdf.

records in 2011,[8] numbers similar to those of 2010 in which 662 breaches occurred, resulting in 16,167,542 disclosures.[9] Hacking has long become a leading cause of breaches,[10] accounting for 22.7% of the total number of breached records exposed in 2010.[11] In 2009, hacking was responsible for as much as 63% of the total amount of data exposed.[12] The 2010 Verizon security report, a leading data breach investigation report, points out that 85% of hacking attacks were "not considered highly difficult"[13] and the same has been denoted in the past.[14] The report concludes that most

[8] IDENTITY THEFT RES. CTR., 2011 BREACH LIST 1 (2011), *available at* http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf.

[9] IDENTITY THEFT RES. CTR., 2010 BREACH LIST 1 (2010), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20101229.pdf.

[10] *See* Mathew J. Schwartz, *Hacking Becomes Leading Cause of Data Breaches*, INFORMATION WEEK (Apr. 22, 2011, 12:27 PM), http://www.informationweek.com/news/security/attacks/229402094.

[11] IDENTITY THEFT RES. CTR., 2010 DATA BREACH HACKING CATEGORY SUMMARY 1 (2010), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_-_Hacking_Summary_20101229.pdf. The number of breaches and the amount of data loss is related, but they are not the same. The number of breaches means the number of incidents that resulted in a data loss and each breach carries a certain amount of data loss.

[12] IDENTITY THEFT RES. CTR., 2009 DATA BREACH HACKING CATEGORY SUMMARY 1 (2010), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_-_Hacking_Summary_20100106.pdf.

[13] WADE BAKER ET. AL, VERIZON, 2010 DATA BREACH INVESTIGATIONS REPORT 3 (2010) [hereinafter 2010 DATA BREACH REPORT], *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

[14] Both 2008 and 2009 reports indicated that 83% of attacks were not highly sophisticated. WADE H. BAKER ET. AL, VERIZON, 2009 DATA BREACH INVESTIGATIONS REPORT, 3 (2009) [hereinafter 2009 DATA BREACH REPORT], http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf; WADE H. BAKER ET. AL, VERIZON, 2008 DATA BREACH INVESTIGATIONS REPORT, 3

breaches could have been avoided without difficult or expensive controls.[15] These findings provide a clear picture of the circumstances surrounding data breaches, indicating that a majority of data loss due to hacking could have been prevented by database operators, yet they failed to do so. Nonetheless, a lack of actual damage forces victims of data breaches to bear the loss whereas database operators escape liability.

[4] When security of a database is undermined, an individual loses Personally Identifiable Information, resulting in harm ranging from negligible to destructive. However, not only is it impossible to know the ramifications of the loss until the loss causes actual harm, but it is also unreasonable to compel an individual to wait until said individual becomes injured. Therefore, the data loss itself should constitute an actionable injury and compensable harm. Therefore, the Federal Trade Commission, after conducting research, should assign values to each type of data loss and enforce compensation. To that end, this article proposes an approach that considers the expected value of harm and the benefits of disclosure to measure the harm caused by a breach. The expected value of harm and the benefits of disclosure compose the Value of Information formula. In accordance with this formula, financially sensitive information, medical information, and socially accepted disclosable information are valued in descending order.

[5] Part II categorizes Personally Identifiable Information into three groups according to its character and use: financially sensitive information, medical information, or socially accepted disclosable information. Financially sensitive information encompasses information created by financial institutions for facilitating financial transactions and a Social Security number. Medical information is information with respect to an individual's physical and mental health condition. Socially accepted disclosable information is information that is part private and part public, and is categorized into direct socially accepted disclosable information or

(2008) [hereinafter 2008 DATA BREACH REPORT], *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[15] 2010 DATA BREACH REPORT, *supra* note 13.

indirect socially accepted disclosable information. These three types of information are ranked based on their value of information, which is proportional to the extent of harm derived from disclosure. However, the benefits of disclosure offset the extent of harm.

[6] Part III analyzes how to justify compensation. Negligence tort liability fails to compensate victims of data breaches because victims have not suffered actual harm. However, courts deciding medical malpractice and environmental toxic tort claims have acknowledged future harm and an increased threat of future injury when it is reasonably linked to harm done. In situations where database operators could not have prevented breaches due to sophisticated hacking techniques, this paper proposes strict liability since collecting information constitutes an ultrahazardous activity where significant social utilities and losses coexist. Moreover, the imposition of strict liability is appropriate since it optimizes the extent of data collection and makes database operators, the least cost avoiders, bear the losses.

[7] Part IV examines how to structure a uniform compensation scheme. An examination of state and federal statutes, which penalize unlawful disclosure of Personal Identifiable Information and impose civil penalties, demonstrates that such laws fail to weigh the different values of each type of information. Ultimately, this article argues that Congress should enact a law requiring the Federal Trade Commission to collect evidence of the value of information and to establish a comprehensive civil penalty scheme. The compensation scheme should pursue deterrence and effective compensation rather than to simply punish database operators.

II. HOW TO CATEGORIZE AND RANK PERSONALLY IDENTIFIABLE INFORMATION

[8] Each form of Personally Identifiable Information is different. Some are created to serve a particular purpose, whereas others are assigned by the government. Some are designed to remain private and others are made to share with people. Since each piece of Personally Identifiable Information carries distinct information, respective

information should be weighted differently. Thus, this article categorizes each type of information based on its use, purpose, and character into financially sensitive information, medical information, or socially accepted disclosable information. Furthermore, it introduces the Value of Information equation in order to measure the value of each type of information. The equation ranks financially sensitive information, medical information, and socially accepted disclosable information in descending order.

[9] A disclosure of each form of information entails different harm and the degree of harm is proportional to the value of information. In measuring the value of information, this article takes into account two factors: first, the expected value of harm, and second, the benefits of disclosure. The most common harm is monetary loss. It is related to almost any type of information disclosure and it is the most likely outcome of disclosure. The amount of loss varies according to the type of disclosed information. The expected value of harm further increases when legal recourses, such as a private right of action or criminal prosecution, do not exist. This is because an abuse of personal information is more likely to occur when there is no imprisonment or civil penalty for misusing it. However, not all disclosure is detrimental. Certain disclosures benefit society as well as individuals and the benefits of these disclosures offset the harm derived from the disclosures.[16] Therefore, the value of information can be calculated by combining the expected value of harm less the benefits of disclosure.

Value of Information = Expected Value of Harm – Benefits of Disclosure

[16] For example, under the Health Insurance Portability and Accountability Act, certain disclosures of personal information are permitted to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. 45 C.F.R. § 164.512(j)(1)(i) (2011).

A. Financially Sensitive Information

[10] Financially sensitive information includes all information that enables people to engage in financial transactions. For example, Bank of America requires a Social Security number, debit card or bank account number, home address, current e-mail address, and if applicable, online banking ID and passcode in order for an individual to open an account.[17] Information required to carry out financial transactions involves two pieces of information, information created by financial institutions and a Social Security number.

1. Information Created by Financial Institutions

[11] Financial institutions generate information for facilitating financial transactions, and information created by financial institutions is key to these transactions. Financial institutions usually handle thousands of customers and deal with millions of dollars, making it important that they correctly identify the sources of customers' funds in addition to giving customers flexibility to control their funds. To this end, information created by financial institutions is a highly convenient tool because it is easily generated and readily destroyed.[18] Bank account numbers, credit card numbers, and bank account and credit card passwords are all typical information created by financial institutions. In addition, due to the emergence of online banking, online IDs and passwords now constitute information created by financial institutions.

[12] Information created by financial institutions is unique in the sense that customers are required to pay fees to create, maintain, use, and secure

[17] *Apply Online Frequently Asked Questions*, BANK OF AMERICA, http://www.bankofamerica.com/deposits/checksave/index.cfm?template=lc_faq_applyonline&context=&statecheck=VA&cd_bag=&sa_bag=&ch_bag= (last visited Sept. 28, 2012).

[18] *See generally Bank of America Privacy & Security*, BANK OF AMERICA, https://www.bankofamerica.com/privacy/Control.do?body=privacysecur_faqs (describing the customer information banks collect, generate and use).

their information.[19] Credit card companies often charge fees to issue credit cards and customers are required to pay annual fees to keep benefits.[20] Banks impose monthly service fees unless customers meet certain requirements.[21] Due to the sensitive nature of information created by financial institutions and the direct financial losses deriving from its misuse, financial institutions are required to establish stringent security measures.[22] However, data breaches occur often.[23] According to the 2010 Verizon Breach Report, which analyzed 141 breach cases involving 143 million data losses, 33% of breaches occurred in the financial services sector in 2010, making information created by financial institutions the most vulnerable type of information,[24] resulting in a direct monetary loss.

[13] For example, in *Shames-Yeakel v. Citizens Financial Bank,* the Shames-Yeakels, who were bank customers, sued Citizens Financial Bank when an unauthorized person gained access to their online account.[25] The thief used the customers' username and password to order a $26,500

[19] *See generally Take on Your Bank*, CONSUMER REP., Feb. 2012, at 16-19, *available at* http://www.consumerreports.org/cro/magazine/2012/02/bank-accounts/index.htm (describing different types of fees and why banks charge them).

[20] *See* Sarah Morgan, *Are Credit-Card Annual Fees Reason to Walk?*, SMARTMONEY (July 20, 2010), http://www.smartmoney.com/spend/family-money/is-a-credit-cards-annual-fee-reason-to-snub-it/.

[21] *See* Katherine Yung, *Big banks hit customers with higher fees, and more of them*, USA TODAY (May 15, 2011, 7:00 AM), http://www.usatoday.com/money/industries/banking/2011-05-15-bank-fees_n.htm.

[22] *See* 2010 DATA BREACH REPORT, *supra* note 13, at 8.

[23] *See generally* IDENTITY THEFT RESOURCE CTR., 2012 BREACH LIST (2012), *available at* http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf (listing all reported breaches).

[24] 2010 DATA BREACH REPORT, *supra* note 13, at 7-8.

[25] 677 F. Supp. 2d 994, 996 (N.D. Ill. 2009).

advance on the customers' home equity credit line.[26] The thief wired the money from Citizens Financial Bank to a bank in Hawaii and then transferred it to a bank in Austria.[27] The Austrian bank refused to return the money.[28] Despite knowing that the customers' username and password were stolen, Citizens Financial Bank billed them for $26,500.[29] After several unfruitful complaints, the customers filed suit alleging, a violation of the Fair Credit Report Act ("FCRA") and negligence in the bank's duty to secure customers' confidential information.[30] The bank moved for summary judgment.[31] The court ruled that genuine issues of material fact existed as to whether the bank breached its duty to sufficiently secure its online banking system and as to the reasonableness of the bank's decision to report the credit account as delinquent without acknowledging the disputed nature of the customers' debt.[32] The court reasoned that despite knowing that the customers contested the debt, the bank still reported the customers' account as delinquent to national credit bureaus, which would mislead a reasonable finder and have an adverse effect on the customers' credit.[33]

[14] Although the court suggested the customers might have a claim under the FCRA, the FCRA cannot accommodate a customer whose information created by financial institutions is compromised by a third

[26] *Id.* at 998.

[27] *Id.*

[28] *Id.*

[29] *Id.* 998-99.

[30] *Shames-Yeakel*, 677 F. Supp. 2d at 999-1000, 1003, 1008.

[31] *Id.* at 996.

[32] *Id.* at 1005-09.

[33] *Id*. at 1005.

party.[34] This is because the FCRA only involves the accuracy of a credit report and deals with issues regarding reporting information in dispute.[35] In other words, the court's finding was based on the bank's failure to report the nature of debt, rather than its failure to safeguard the customers' information.

[15] Another statute regulating financial institutions and the collection of financial data is the Gramm-Leach-Bliley Act ("GLBA").[36] The GLBA states, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customer and to protect the security and confidentiality of those customers' nonpublic personal information."[37] It prohibits a financial institution from disclosing "nonpublic personal information" unless the institution has provided a privacy notice to the consumer and regulates to whom the consumer's information may be disclosed.[38] In defining "nonpublic personal information," the statute focuses on the source of information, so if obtained through a non-publicly accessible source, the information is nonpublic personal information.[39] Examples given in the statute illustrate that an individual's name and address obtained through account information, which is not publicly accessible, is non-public personal information, whereas the same information supplied by a publicly available source, such as a phone book, is public personal information.[40] Such a distinction, however, renders the statute unenforceable in many instances of its application since sources of information have expanded enormously due to the Internet, making it next to impossible to detect the exact source. Even if a consumer manages to

[34] *See Shames-Yeakel*, 677 F. Supp. 2d at 1005.

[35] *See* 15 U.S.C. § 1681(a) (2006).

[36] *See id.*

[37] 15 U.S.C. § 6801(a) (2006).

[38] *Id.* § 6802(a)-(b).

[39] *See* 16 C.F.R. § 313.3(n) (2012).

[40] *See id.* § 313.3 (n), (p).

prove that his or her financial institution violates the GLBA, courts uniformly have ruled that no private right of action exists under the GLBA.[41]

[16] For instance, in *Menton v. Experian Corp*., the plaintiff alleged the defendant Experian violated the statute through its continuous sale of consumer identifying information, but the court concluded that even "assuming *arguendo*" that the allegations were true, "the GLBA does not provide for a private right of action."[42] The court found support for its holding in the statute's text, which states that it "shall be enforced by the Bureau of Consumer Financial Protection, the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction."[43] In other words, only governmental entities can bring a cause of action under the GLBA.

2. Social Security Numbers

[17] Social Security numbers were originally created to track workers' earnings for the purpose of Social Security benefits.[44] Social Security numbers have since become a commonly used personal identifier for many other reasons and a report issued by the United States General Accounting Office confirms that private sector organizations routinely obtain and use

[41] *See* C.S. v. United Bank, Inc., No. 2:08-921, 2009 WL 777643, at *5 (S.D. W. Va. Mar. 20, 2009) ("[E]very court to considered the issue has found that '[n]o private right of action exists for an alleged violation of the GLBA.'") (quoting Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007)).

[42] No. 02 Civ. 4687(NRB), 2003 WL 21692820, at *3 (S.D.N.Y. July 21, 2003).

[43] 15 U.S.C. § 6805(a) (Supp. V 2011).

[44] *See Historical Background and Development of Social Security,* U.S. SOC. SECURITY ADMIN., http://www.ssa.gov/history/briefhistory3.html (last modified May 16, 2012).

Social Security numbers for the purpose of employment screening, credit information, and criminal history.[45]

[18] A number of laws restrict the use or disclosure of a Social Security number. The Fair and Accurate Credit Transactions Act ("FACTA"), which amended the FCRA, requires consumer reporting agencies and any business that uses a consumer report to implement procedures for proper disposal of the report information, which includes a Social Security number.[46] It also stipulates that consumer reporting agencies "truncate" the first five digits of the Social Security number and, upon the consumer's request, not include it in the disclosure.[47] The GLBA protects the privacy of nonpublic personal information, such as a Social Security number, by limiting when financial institutions may disclose that information to nonaffiliated third parties.[48] The Driver's Privacy Protection Act prohibits the obtaining and disclosing of a Social Security number from a motor vehicle record except as expressly permitted.[49] The Health Insurance Portability and Accountability Act, which preserves the privacy of an individual's health information by limiting health care organizations from disclosing such information without the patient's consent, safeguards a Social Security number used in medical records.[50]

[45] U.S. GEN. ACCOUNTING OFFICE, GAO-04-11, REPORT TO THE CHAIRMAN, SUBCOMMITTEE ON SOCIAL SECUITY, COMMITTEE ON WAYS AND MEANS, HOUSE OF REPRESENTATIVES, SOCIAL SECURITY NUMBERS: PRIVATE SECTOR ENTITIES ROUTINELY OBTAIN AND USE SSNS, AND LAWS LIMIT THE DISCLOSURE OF THIS INFORMATION 2-3 (2004), *available at* http://www.gao.gov/new.items/d0411.pdf.

[46] *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952, 1985-86 (2003).

[47] *See* 117 Stat. at 1961.

[48] *See* 15 U.S.C. § 6802(a) (2006).

[49] *See* 18 U.S.C. § 2721 (2006).

[50] *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 2029 (1996) (codified in scattered sections of 42 U.S.C.).

[19] Because a Social Security number is widely used as an individual identifier, the disclosure of a Social Security number entails significant harm. One such harm is identity theft. Identity theft occurs when an impersonator acquires an individual's Social Security number and uses it to commit various illegal activities.[51] The Federal Trade Commission ("FTC")'s website illustrates various types of such fraud.[52] One of the more common fraudulent activities involves deceiving financial institutions and draining the victim's account.[53] Imposters may open new credit cards or bank accounts or even clone ATM or debit cards. Imposters often use this account information to change a victim's billing address, run up charges, or pay off the imposters' own bills, and because the bills are sent to a different address, the victim may not realize his identity is stolen.[54] Government documents fraud is also common.[55] Imposters might claim government benefits and file a fraudulent tax return.[56] They might also get a driver's license or official ID card issued in the victim's name but with an imposter's picture.[57] Imposters might get a job with a falsified identity using the victim's Social Security number.[58] Another area where imposters frequently commit identity theft is medical

[51] *See About Identity Theft*, FIGHTING BACK AGAINST IDENTITY THEFT, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Oct. 5, 2012).

[52] *See id.*

[53] *See* FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY-DECEMBER 2010, at 3 (2011) [hereinafter CONSUMER SENTINEL BOOK], *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

[54] *See About Identity Theft*, *supra* note 51.

[55] *See* CONSUMER SENTINEL BOOK, *supra* note 53.

[56] *See About Identity Theft*, *supra* note 51.

[57] *See id.*

[58] *See id.*

services.[59] Imposters might steal personal and health insurance information in order to obtain medical treatment, prescription drugs, or surgery.[60] As a result, a victim's medical records may change, he may receive bills for services he did not receive, or he may reach his insurance limits more quickly.[61]

[20] The number of complaints filed by consumers with various organizations illustrates the magnitude of consumer fraud and identity theft.[62] The Consumer Sentinel Network, the FTC-run online database, collects information about such complaints and releases an annual report.[63] According to the report, over 1.3 million complaints were filed in 2010, and 250,854 complaints involved identity theft, making it the number one complaint category.[64] What makes the threat of identity theft so alarming is the possibility of multiple identity thefts. Once an imposter succeeds in committing fraud, that success serves to prove his false identity, thereby making the second identity theft easier. Twelve percent of identity theft complaints included more then one type of identity theft.[65] A recent incident in Utah shows how a typical multiple identity theft works.[66] In May 2011, two men living in Utah were charged with using fraudulent Social Security numbers to obtain employment, driver's license renewals,

[59] *See Medical Identity Theft*, FED. TRADE COMM'N, 1 (Jan. 2010), http://ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.pdf.

[60] *See id.*

[61] *See id.* at 1-2.

[62] *See* CONSUMER SENTINEL BOOK, *supra* note 53, at 3.

[63] *See id.* at 2.

[64] *Id.* at 6.

[65] *See id.* at 11 n. 1.

[66] *See* Benjamin Wood, *Men charged with identity fraud for using false Social Security numbers*, KSL.COM (May 26, 2011, 9:45 AM), http://www.ksl.com/?nid=960&sid=15702829.

and loans.[67] They worked for several years under false Social Security numbers and obtained totaled more than $206,000.[68] Even though they were illegal immigrants, they were unrestrained once they established their identities and it took a number of years for the police to uncover their fraud.[69]

[21] Despite the seriousness and high likelihood of identity theft, a majority of courts have dismissed claims brought by persons whose Social Security number was disclosed.[70] Such incidents frequently involve a debtor who filed bankruptcy.[71] In *In re Matthys,* a debtor who filed bankruptcy brought suit against a creditor who failed to redact his Social Security number on the proof of claim that allowed anyone with a PACER (Public Access to Court Electronic Records) ID to have access to his Social Security number.[72] The debtor alleged, *inter alia,* an invasion of privacy.[73] Dismissing the claim, the Indiana court held that 'public disclosure of private facts,' one of the four elements required for the finding of invasion of privacy under Indiana law, was not established.[74]

[67] *See id.*

[68] *Id.*

[69] *Id.*

[70] *See, e.g.*, Matthys v. Green Tree Servicing LLC (*In re* Matthys), No. 09–16585–AJM–13, 2010 WL 2176086, at *2-3 (Bankr. S.D. Ind. May 26, 2010); Carter v. Checkmate, Cash Advance Ctrs., Inc. (*In re* Carter*),* No. 09–00132–TOM, 2009 WL 3425828, at *3 (Bankr. N.D. Ala. Oct. 23, 2009); Newton v. ACC of Enter., Inc. (*In re* Newton*),* No. 08–1106–DHW, 2009 WL 277437, at *3-5 (Bankr. M.D. Ala. Jan. 29, 2009); *see also* Rebecca Rose, *Disclosure of Social Security Number Does Not Give Debtors a Private Right of Action*, ST. JOHN'S UNIV. BANKR. CASE BLOG (Dec. 2010), http://stjohns.abiworld.org/node/99.

[71] *E.g.*, *In re Matthys*, 2010 WL 2176086, at *1; *In re Newton,* 2009 WL 277437, at *1.

[72] *In re Matthys*, 2010 WL 2176086, at *1.

[73] *Id*. at *1, *3.

[74] *Id*. at *3.

The court reasoned that the degree of disclosure was not large enough to make the disclosure public because only individuals with the PACER ID and password could have accessed the debtor's Social Security number, and establishing a new account with PACER would be "a far cry from leisurely surfing the net and stumbling upon private information."[75] The court viewed registering for a PACER account as an "affirmative [action] to seek out the information," and requiring such an affirmative action did not rise to the level of publicity needed to establish an invasion of privacy.[76]

[22] However, the court ignored the fact that PACER is a website designed for public access, as it stands for Public Access to Court Electronic Records, and in fact, numerous people have a PACER ID.[77] Persons with PACER ID do not need to take the affirmative action to join the site and logging into the PACER with an existing ID would hardly constitute an affirmative action.[78] Therefore, the debtor's Social Security number was available to everyone with the PACER ID, which is a sufficiently large number of people to make this disclosure public. Thus, the court's assumption that the publicity requirement was not met because a membership was required was simply wrong. Instead, the court should have based its decision on whether information was obtainable by a sufficiently large number of third parties.

[23] Rule 5.2 of the Federal Rules of Civil Procedure, titled "Privacy Protection For Filings Made With The Court," prohibits a disclosure of an individual's full Social Security number.[79] It requires that all but the last

[75] *Id*.

[76] *See id*.

[77] *See* PACER, http://www.pacer.gov/ (last visited Oct. 5, 2012).

[78] *See PACER On-Line Registration*, PACER, https://www.pacer.gov/psco/cgi-bin/regform.pl (last visited Oct. 5, 2012).

[79] FED. R. CIV. P. 5.2.

four numbers of an individual's Social Security number be redacted before filing the document electronically.[80] However, the Indiana court also dismissed this claim, reasoning that rules governing federal procedures do not give rise to a private right of action.[81] Unlike the Indiana court, a Minnesota court took a different position. In *Allstate Insurance Co. v. Linea Latina De Accidentes, Inc*., attorneys failed to redact personal information on attachments to electronic court filings and improperly disclosed birth dates, names of minors, financial account numbers, and at least one person's Social Security number.[82] The court, finding a violation of Rule 5.2, ordered the defendant to provide each individual whose information was compromised with a subscription for credit monitoring service.[83]

[24] Various federal and state governments have outlawed identity theft.[84] All fifty states have enacted identity theft statutes.[85] Most states tie penalties to the amount of money the thief steals.[86] For example, the Florida statute designates identity theft as a second-degree felony if it accompanies an injury of $5,000 or more.[87] If the injury reaches the

[80] FED. R. CIV. P. 5.2(a).

[81] *In re Matthys*, 2010 WL 2176086, at *3.

[82] No. 09-3681(JNE/JJK), 2010 WL 5014386, at *1 (D. Minn. Nov. 24, 2010).

[83] *See id.* at *3.

[84] *See Federal Laws: Criminal*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/federal-laws-criminal.html (last visited Oct. 5, 2012) (identifying federal identity theft law); *State Laws: Criminal*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-criminal.html (last visited Oct. 5, 2012) (listing all states and federal territories that classify identity theft as criminal conduct).

[85] *See State Laws: Criminal*, *supra* note 84.

[86] *See, e.g.*, FLA. STAT. ANN. § 817.568 (West 2010).

[87] *Id.* § 817.568(2)(b).

$50,000 threshold, it becomes a first-degree felony.[88] At the federal level, Congress enacted the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act").[89] The Act makes it a federal crime for anyone who "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[90] In addition, the Identity Theft Penalty Enhancement Act amends the federal criminal code to establish penalties for aggravated identity theft in addition to the existing punishments for related felonies.[91] This includes instances when identity theft has been used as one step in a process of more serious crimes, such as terrorist acts, immigration violations, and firearms offenses.[92] The Act adds two to five years to the sentences of violators.[93]

[25] However, because it does not allow a private right of action, the Act has a limited effect in remedying the harm of affected individuals.[94] In *Garay v. U.S. Bancorp*, the customer, Garay, brought an action against U.S. Bancorp alleging the aiding and abetting of identity theft under the Identity Theft Act.[95] The bank issued a credit card to an impersonator of Garay and the imposter incurred over $20,000 in charges, leaving his

[88] *Id.* § 817.568(2)(c).

[89] Pub. L. No. 105-318, 112 Stat. 3007 (1998).

[90] 18 U.S.C. § 1028(a)(7) (2006).

[91] 18 U.S.C. § 1028A (2006).

[92] 18 U.S.C. § 1028A(c).

[93] *Id.* § 1028A(a).

[94] *See generally id.* § 1028A(a) (prescribing imprisonment as punishment for violating the statute).

[95] 303 F. Supp. 2d 299, 302 (E.D.N.Y. 2004).

account delinquent.[96] Deciding for the bank, the court concluded that no private right of action exists under the Act, nor did Garay set forth any basis establishing that Congress intended to provide a private right of action under the statute.[97]

[26] Although the federal law does not allow a private right of action, some states have enacted comprehensive anti-identity theft laws.[98] For example, the state of California permits victims to obtain the fraudulent applications completed by the identify thief as well as a record of the thief's transactions carried out in the victim's name.[99] California also assists victims in stopping debt collectors from continuing to try to collect debts that the thief incurred.[100]

[27] A Social Security number is an essential piece of personal information because it is one of the most widely used individual identifiers and is necessary to engage in financial transactions.[101] Disclosure of a security number is likely to lead to an identity theft where an imposter drains a victim's account or damages the victim's credit. Despite the close connection between the disclosure of a Social Security number and

[96] *Id.* at 301.

[97] *Id.* at 302 (finding that the statute is criminal in nature and it is "'a general precept of criminal law that unless the statute specifically authorizes a private right of action, none exists'" (quoting Vasile v. Dean Witter Reynolds, Inc., 20 F. Supp. 2d 465, 477 (E.D.N.Y. 1998))).

[98] *See Identity Theft State Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/banking/identity-theft-state-statutes.aspx (last updated July 23, 2012) (noting that twenty-nine states have specific restitution provisions for identity theft).

[99] *See* CAL. PENAL CODE § 530.8(a) (2006); CAL. CIV. CODE § 1748.95(a) (2002).

[100] *See* CAL. CIV. CODE § 1788.18 (West 2008).

[101] *See generally Avoid Identity Theft: Protect Social Security Numbers*, SOC. SEC. ADMIN., http://www.socialsecurity.gov/phila/ProtectingSSNs.htm (last updated June 6, 2012) (identifying the SSN as a crucial piece of information for many organizations).

resulting financial loss, federal laws do not allow an individual to recover loss from an entity who negligently mishandled the individual's Social Security number, thereby exposing an individual to a higher degree of harm.[102]

B. Medical Information

[28] Medical information is information that exists in connection with an individual's physical and mental health condition in addition to records regarding treatments and prescriptions. Because medical information is processed by various entities, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") broadly defines "protected health information."[103]

[29] Protected health information is information created or received by a covered entity (e.g. health plans, health care clearinghouses, and health care providers) or its business associates (e.g. billing services, accountants or collection agencies) that identifies an individual and relates to that individual's health condition, receipt of health care, or payment for the provision of the individual's health care services.[104] Such information is protected health information regardless of whether it relates to a physical or mental health condition or whether that health condition existed in the past, exists in the present, or will exist in the future.[105] Similarly, protected health information includes information concerning the payment

[102] *See, e.g.*, 18 U.S.C. § 1028 (2006) (indicating that an entity must "knowingly mishandle" an individual's social security number before it is liable for damages).

[103] *See generally* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 2019, 2022. HIPAA was reformed by the Patient Protection and Affordable Care Act (PPACA) that was signed into law on March 23, 2010. Although some definitions under HIPAA were revised, this paper aims to merely illustrate exemplary definitions of medical information and finds the HIPAA's definitions appropriate for this purpose.

[104] *See* 45 C.F.R. § 160.103 (2011) (defining "business associate" and "covered entity").

[105] *See id.*

of health care services provided to an individual irrespective of when the health care was or will be provided.[106]

[30] While protected health information is an established definition under HIPAA's privacy and confidentiality provisions, for the purpose of this article, medical information is limited to pure medical records—such as history of hospital visits, drug prescription records, or health insurance claims—because certain information under protected health information falls into other categories examined in this article.

[31] Among the various types of potential harm caused by the disclosure of medical information, there is at least one situation in which such a disclosure poses a unique threat: the loss of an employment opportunity. In *Diering v. Regional West Medical Center,* the hospital's emergency room director told a potential new employer that Diering, an emergency room physician, had undergone voluntary drug and alcohol treatments without seeking Diering's consent to disclose that information.[107] As a result, the potential employer decided not to hire Diering and Diering sued the hospital for a violation of HIPAA.[108] However, the Nebraska court dismissed the case, reiterating that a wrongful disclosure in violation of HIPAA does not create a private cause of action.[109] Although this case does not concern a data breach because the director was in a position to know about Diering's health information, it involves the unauthorized use of medical information that would result from a data breach, illustrating a situation where such misuse cost the plaintiff a job, but the law failed to mitigate such harm.[110]

---

[106] *See id.*

[107] No. 7:06CV5010, 2006 U.S. Dist. LEXIS 66102, at *3-4 (D. Neb. Sept. 15, 2006).

[108] *Id.* at *3, *8.

[109] *Id.* at *8-9.

[110] *See id.* at *3.

[32] However, the likelihood of such harm is relatively low because not everyone has health issues detrimental to work performance, whereas almost everyone has financially sensitive information. In addition, fewer incentives exist for an imposter to abuse medical information. By taking advantage of an individual's financially sensitive information, an imposter could make the individual pay for services and irresponsible expenditures enjoyed by the imposter, whereas harm due to the abuse of medical information would arise only if an individual's employer becomes aware of the individual's health problems. The probability of an employer knowing and using his employee's ill health conditions against the employee is tenuous in comparison to the threat of exploiting financially sensitive information.

[33] Another harm that a disclosure of medical information implicates is emotional distress because strong negative social stigma is attached to certain medical conditions. Such conditions encompass problems range from drug and alcohol abuse to positive HIV diagnoses. Setting aside the high insurance premiums that people with these health issues have to pay, if they can get insurance, disclosures of their medical conditions would cause emotional distress, and yet again, the law fails to mitigate such harm.[111]

[34] In *Federal Aviation Administration v. Cooper*, Cooper was a recreational pilot from San Francisco who had been diagnosed as HIV-positive.[112] When he renewed his pilot license in the mid-1990s, he unlawfully withheld his diagnosis from the Federal Aviation Administration ("FAA") because he feared discrimination based on his medical condition and by implication, his sexual orientation as a homosexual man.[113] When the FAA obtained confidential information from the Social Security Administration ("SSA") that Cooper had been a

[111] *See generally* Privacy Act of 1974, 5 U.S.C. § 552a (2006) (failing to list emotional distress as a harm that calls for an award of damages).

[112] 132 S. Ct. 1441, 1446 (2012).

[113] *Id.*

long-term recipient of disability benefits because of his HIV, it launched an investigation.[114] Subsequently, Cooper's license was revoked and he was charged with making false statements to the federal government.[115] Cooper ultimately pled guilty to one count of making and delivering a false official writing.[116] He then sued the FAA for violating the Privacy Act.[117] The Act prohibits the disclosure of information maintained in systems by federal agencies absent the written consent of the subject individual and permits claims for actual damages.[118] Cooper claimed that he suffered from severe mental distress after the SSA disclosed his HIV-positive status in violation of the Act.[119] The case, after conflicting decisions from lower courts, proceeded to the Supreme Court where the Justices contemplated whether actual damages were limited to monetary loss or could include mental distress.[120] On March 28, 2012, the Supreme Court rendered its decision, holding that actual damages within the meaning of the Privacy Act do not include damages for emotional distress and are limited to out-of-pocket financial losses.[121]

[35] Disclosures of medical information can be irreparable because they could result in a loss of employment and emotional distress due to a negative social stigma. However, such disclosures are less frequent and the likelihood of disclosures is lower than that of financially sensitive information. This renders the impact of a disclosure of medical

[114] *Id.* at 1446-47.

[115] *Id.* 1447.

[116] *Id.*

[117] *Fed. Aviation Admin.*, 132 S. Ct. at 1447.

[118] *See* Privacy Act of 1974, 5 U.S.C. § 552a (2006).

[119] *See Fed. Aviation Admin.*, 132 S. Ct. at 1447.

[120] *Id.* at 1446.

[121] *Id*. at 1456.

information on an individual's financial well being less direct, thereby making medical information less valuable than financially sensitive information.

C. Socially Accepted Disclosable Information

[36] Socially accepted disclosable information concerns information that is open to the public or that is relatively easy to obtain. There are two types of socially accepted disclosable information: direct socially accepted disclosable information and indirect socially accepted disclosable information. Direct socially accepted disclosable information is information that directly leads to an individual, such as name, address, email address, date of birth, and phone number. On the other hand, indirect socially accepted disclosable information is information that shows an individual's character, traits, or preferences. It is not directly linked to an individual, but it is highly sought-after information because it is useful for advertisements. The scope of disclosures this article focuses on concerning socially accepted disclosable information does not include transferring information between affiliated parties. Although such information sharing is a sharply debated issue, it is different from disclosures due to data breaches and the dissemination of information without permission.

1. Direct Socially Accepted Disclosable Information

[37] Direct socially accepted disclosable information is more or less public. A person's name and contact information are frequently, even sometimes voluntarily, disclosed online.[122] Disclosures of direct socially accepted disclosable information might bring benefits because individuals can build and expand networks based on educational or geographical background. However, this does not mean that there is no harm created by

[122] *See* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 93, 95 (2009) (analyzing the collection and dissemination of personal identifiable information and the legal protections available concerning online privacy).

such disclosure. A disclosure of direct socially accepted disclosable information is likely, if not certain, to lead to unsolicited marketing.[123] This is demonstrated by the multitude of spam in one's emails and the continuous telephoning by automated robo-calls. Unsolicited marketing is not only annoying, but also dangerous because hackers often disguise themselves as unsolicited marketers to succeed in stealing personal information.[124] Although such harm is frequent and probable, courts have generally viewed the disclosure of direct socially accepted disclosable information as not constituting a cognizable harm.[125]

[38] In *Allison v. Aetna, Inc*., the defendant's online job application database, which stored information about 450,000 applicants, was hacked and the plaintiff who had uploaded his personal information, including his resume, sued the website.[126] An investigation revealed that unauthorized individuals had access to emails, yet it was unclear whether any other information was exposed.[127] The plaintiff contended that people "'face a significant risk of identity theft, evidenced by . . . [t]he hackers' efforts to extract personal information from [victims] via sending phishing email messages.'"[128] Nevertheless, the court dismissed the case for failure to allege actual harm, reasoning that "even assuming that the hackers

[123] *Cf.* Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1501 (2001).

[124] *See id.*

[125] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631, 637 (7th Cir. 2007); Hinton v. Heartland Payment Sys., Inc., No. 09-594, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (finding that plaintiff, who claimed that his credit information was compromised in an electronic database breach but alleging no misuse, failed to state an actual or imminent injury-in-fact).

[126] No. 09-2560, 2010 WL 3719243, at *1 (E.D. Pa. Mar. 9. 2010).

[127] *Id.*

[128] *Id.* at *5 (alterations in original) (citations omitted).

obtained Plaintiff's email address, it is highly speculative that they obtained any other information that would be necessary to commit identity theft."[129]

[39] However, one California court created an exception by allowing a case to survive a motion to dismiss. In *Claridge v. RockYou, Inc.*, the defendant company RockYou developed and published online applications for social networking sites.[130] Customers signed up by providing a valid email address and registration password, which RockYou then stored in its database.[131] Many customers were also required to provide their Facebook or MySpace usernames and passwords in order to use RockYou's applications.[132] Although RockYou promised to protect customers' information using "commercially reasonable physical, managerial, and technical safeguards," RockYou did not encrypt information and its vulnerable data security enticed hackers to break into its database.[133] The court noted that customers sufficiently alleged "the breach . . . caused [customers] to lose some ascertainable but unidentified 'value' and/or property right inherent in the [personally identifiable information],"[134] and let the case move forward based on breach of contract, breach of implied contract, and negligence claims.[135]

[40] Furthermore, a recent California Supreme Court decision points to the conclusion that a court can find value in Personally Identifiable Information. In *Pineda v. Williams-Sonoma Stores*, a customer sued

[129] *Id.*

[130] 785 F. Supp. 2d 855, 858 (N.D. Cal. 2011).

[131] *Id.*

[132] *Id.*

[133] *Id*.

[134] *Id.* at 865.

[135] *RockYou, Inc.*, 785 F. Supp. 2d at 864-66.

Williams-Sonoma Stores, alleging that its business practice of collecting customers' zip codes violated California's Song-Beverly Credit Card Act.[136] The Act prohibits requesting or requiring personally identifiable information during a credit card transaction and imposes a civil penalty of up to $1,000 per violation.[137] The court described the Act's extensive legislative history and intent, which reflected California's strong objection to retailers who acquire customers' information for their business purposes, such as to build mailing and telephone lists for in-house marketing efforts, or to sell customers' information to direct-mail or telemarketing specialists.[138] Siding with the customer, the court found that a customer's zip code constitutes Personally Identifiable Information, and thus, concluded that the stores violated the Song-Beverly Credit Card Act.[139] This decision marks a significant achievement in privacy laws in the sense that the court acknowledged, for the first time since the enactment of the Act in 1971, the inherent value in Personally Identifiable Information and the harm posed by unsolicited marketing.[140]

[41] While the court's decision in *Pindea* supports California's policy against information collection and provides a significant step toward protecting Personally Identifiable Information, the court failed to consider the commercial benefits of disclosure. By asking for zip codes instead of exact addresses, a business could develop a store in the area where many customers reside, which would invariably benefit the customers. A business could also accurately reflect preferences of a surrounding neighborhood and adequately supply products that the customers want. In addition, the court ignored that customers could falsify their information and businesses would be ill equipped to verify given information. Also,

[136] 246 P.3d 612, 614 (Cal. 2011).

[137] CAL. CIV. CODE § 1747.08 (West 2011).

[138] *See Pineda,* 246 P.3d at 619-20.

[139] *Id.* at 620.

[140] *See id.* at 618-20.

businesses cannot compel customers to provide their information when they refuse to do so, yet the court found for the plaintiff in *Pineda* who merely asserted that she furnished information, "[b]elieving it necessary to complete the transaction."[141] Hence, it is unfair to punish a business solely because it requested customers' information when the accuracy of information could be questioned and it is shortsighted not to take into account the benefits of requiring customers' information.

[42] Recognizing the severe disturbances and troubles caused by unsolicited marketing, Congress enacted several statutes to manage and control it.[142] The Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act") regulates spam mails.[143] The CAN-SPAM Act applies to all commercial e-mails, which are defined as messages with "the primary purpose of . . . the commercial advertisement or promotion of a commercial product or service,"[144] and prohibits knowingly sending commercial messages with the intent to deceive or mislead recipients.[145] The CAN-SPAM Act also requires senders of commercial emails to include clear and conspicuous explanations of how the recipients can opt out of getting emails in the future and to promptly honor opt-out requests.[146] Parties cannot avoid legal responsibilities since the Act defines a "sender" to include both the company whose product is promoted and the company that actually sends the message, thereby holding both of them legally accountable.[147] Parties who violate the Act

[141] *Id.* at 614.

[142] *See, e.g.*, Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 15 U.S.C. §§ 7701-7713 (2006); Telephone Consumer Protection Act, 47 U.S.C. § 227 (2006); Do-Not-Call Implementation Act, 15 U.S.C. §§ 6101-6108 (2006).

[143] 15 U.S.C. §§ 7701-7713 (2006).

[144] *Id*. § 7702(2)(A).

[145] *Id*. § 7705(a).

[146] *Id*. § 7704(a)(3)-(4).

[147] *Id*. § 7702(16).

may be subject to civil penalties up to $1 million[148] and criminal penalties up to five years of imprisonment.[149] The FTC vigorously enforces the CAN-SPAM Act.[150] For example, Jumpstart Technologies was fined $900,000 when the subject lines of their business's emails falsely indicated that a recipient's friend was sending free tickets and many people who tried to opt out of the promotion continued to receive similar emails for weeks afterward.[151]

[43] In addition, Congress passed the Telephone Consumer Protection Act ("TCPA") in response to the growing number of marketing calls to consumers' homes and the increasing use of automated and prerecorded messages.[152] The TCPA permits individuals to sue a telemarketer in small claims court for the actual loss incurred or up to $500, whichever is greater.[153] Further, the Federal Communications Commission ("FCC") created a national do-not-call registry in which individuals may add their phone numbers to avoid receiving telemarketing calls.[154]

[148] 15 U.S.C. § 7706(g)(3) (2006).

[149] *Id*. § 7704(d)(5).

[150] *Id.* § 7705(c); *see, e.g.*, FTC v. Cleverlink Trading Ltd., 519 F. Supp. 2d 784, 786, 800 (N.D. Ill. 2007).

[151] *See* United States v. Jumpstart Tech., LLC, No. C-06-2079 (MHP) (N.D. Cal. Mar. 22, 2006), *available at* http://www.ftc.gov/os/caselist/0423176/0423176JumpstartTechnologiesConsentDecree.pdf.

[152] 47 U.S.C. § 227 (2006); *see* H.R. REP. NO. 102-317, at 2, 5-6 (1991).

[153] 47 U.S.C. § 227(c)(5)(B) (2006).

[154] *See Do Not Call List*, FED. COMMC'NS COMM'N, http://www.fcc.gov/encyclopedia/do-not-call-list (last visited Oct. 7, 2012).

2. Indirect Socially Accepted Disclosable Information

[44] While direct socially accepted disclosable information is somewhat public in its nature, indirect socially accepted disclosable information is more private. It has emerged in the wake of the Internet. The enormous growth of data processing and storage capability enables database operators to collect consumer information and incentivizes its use because more information creates a more accurate profile, which allows more precisely targeted advertisements.[155] This is called behavioral advertising.[156] The FTC Staff Report illustrates an example of behavioral advertising as follows: a consumer living in Washington, D.C. searches for a flight ticket to New York City through a travel website, but he does not purchase a ticket.[157] Later, when the consumer visits a local newspaper website, he receives advertisements featuring tickets from Washington, D.C. to New York City.[158] This is made possible by a network advertiser. The network advertiser places a cookie, a file used to send information from a user's browser back to a website, on the consumer's computer.[159] Unbeknownst to the consumer, the cookie collects information about web pages that the consumer visited and sends it to the network adviser.[160] Then, the adviser provides such information to affiliated parties such as the newspaper website.[161] When the consumer

[155] *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[156] *Id.*

[157] *Id.* at 3.

[158] *See id.*

[159] *See id.*

[160] *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, *supra* note 155, at 3.

[161] *See id.*

visits the newspaper website, the cookie identifies the consumer and directs the newspaper website to show advertisements about a flight to New York City.[162]

[45] Behavioral advertising creates a serious privacy issue. For example, Sears and Kmart retail Internet websites disseminated cookies and collected personal information on customers' Internet activity.[163] Unlike its initial representation, the cookies collected information about the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and e-mails.[164] Another tool of behavioral advertising is selling disguised spyware. CyberSpy Software, LLC sold a spyware program called RemoteSpy.[165] The program provided detailed instructions on how to disguise the spyware as an innocuous file so that a person using a computer with the program installed would not recognize that his information was being provided to a third-party.[166] Once installed, the program recorded every website visited, captured images of the computer screen, and even obtained passwords.[167] CyberSpy's website kept the gathered information and delivered it to the purchaser of the program.[168]

[162] *See id.*

[163] Complaint at ¶ 4, *In re* Sears Holdings Mgmt. Corp., (2009) (No. C-4264), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

[164] *Id.* at ¶¶ 12-13.

[165] *See* FTC v. CyberSpy Software, LLC, No. 608-CV-1872-ORL-31GJK, 2009 WL 2386137, at *1 (M.D. Fla. July 31, 2009).

[166] *See Court Orders Halt to Sale of Spyware*, FED. TRADE COMM'N (Nov. 17, 2008), http://www.ftc.gov/opa/2008/11/cyberspy.shtm.

[167] *Id.*

[168] *Id.*

[46] Fighting this deceptive behavioral advertising, the FTC has vigorously enforced Section 5 of the Federal Trade Commission Act.[169] Enacted in 1914, the Act asserts the unlawfulness of unfair methods of competition and deceptive acts or practices.[170] Empowered by Section 5 of the Act, the FTC issues an order to cease and desist when it has reason to believe that entities have violated the Act.[171] The FTC may seek civil penalties up to $10,000 per violation of the order.[172]

[47] Two Internet giants were recently prosecuted under Section 5 of the Act. Google faced charges that its social network, Google Buzz, violated the company's own privacy policies and used deceptive tactics.[173] The FTC alleged that Google used information collected from Gmail users to generate and populate Google Buzz.[174] Google Buzz automatically enrolled users in some features of the network regardless of whether they opted out and an auto-follow option automatically added Gmail users' most-emailed contacts as publicly visible friends on the network.[175] Facebook was also charged with a similar violation.[176] It made information public that users had deemed to be private on their Facebook pages without warning its users or seeking consent.[177] Both Google and Facebook settled with the FTC, agreeing to conduct

[169] *CyberSpy Software*, 2009 WL 2386137, at *1 (citing 15 U.S.C. § 45(a)).

[170] 15 U.S.C § 45(a) (2006).

[171] *Id.* § 45(b).

[172] *Id.* § 45(m)(1)(B).

[173] *See In re* Google Inc., No. C-4336, 2011 WL 5089551, at *1-5 (F.T.C. Oct. 13, 2011).

[174] *Id.* at *2.

[175] *Id.* at *2, *4.

[176] *See In re* Facebook Inc., No. C-4365, 2012 WL 3518628, at *2-3 (F.T.C. July 27, 2012).

[177] *Id*. at *6.

independent privacy audits every other year for the next twenty years.[178] A future violation of the terms of the settlement would cost them $16,000 a day for each count.[179]

[48] Another example of a law punishing intentional and unauthorized access to a computer is the Computer Fraud and Abuse Act of 1996 ("CFAA").[180] Originally enacted in 1984 as a part of the Crime Control Act, the CFAA was the first statute to address computer crime specifically.[181] Section 1030(a) is one of the most common sources of claims under the CFAA.[182] This section prohibits (1) intentional, (2) unauthorized access to a computer or access exceeding authorization, (3) accomplished through an interstate or foreign communication, (4) that leads to the acquisition of information from a protected computer.[183] A "protected computer" is defined as a computer used by the federal government, a financial institution, or one that is used in interstate or foreign commerce or communication.[184] The CFAA allows a civil action to obtain compensatory damages or "loss," but it has a $5,000 minimum

[178] *Id.* at *81; *In re* Google Inc., 2011 WL 5089551, at *10.

[179] *In re* Facebook, Inc., 2012 WL 3518628, at *83.

[180] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

[181] *See* H. MARSHALL JARRETT ET. AL, DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1 (Feb. 2007), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf; Maxim May, *Federal Computer Crime Laws*, SANS INST. INFOSEC READING ROOM, 2 (June 1, 2004), http://www.sans.org/reading_room/whitepapers/legal/federal-computer-crime-laws_1446.

[182] *See* David W. Garland & Linda B. Katz, *Computer Fraud And Abuse Act: Another Arrow In The Quiver Of An Employer Faced With A Disloyal Employee - Part I*, METROPOLITAN CORP. COUNS., May 2006, at 5, *available at* http://www.metrocorpcounsel.com/pdf/2006/May/05.pdf.

[183] *See* 18 U.S.C. § 1030(a) (2006).

[184] *See id.* § 1030(e)(2).

damage requirement during any single year.[185] "Loss" includes costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition before the offense, and lost revenue or cost incurred because of the interruption of service.[186] However, collection of personal data is not generally prosecuted under the CFAA since it cannot meet the threshold of damage requirement.

[49] Nevertheless, disclosures of indirect socially accepted disclosable information may generate benefits. At a personal level, people find friends over social network media and build relationships with people who share a similar background or interests. Social benefits are also obtained because businesses can develop better products or services. The caller ID is a product of such efforts. Caller ID was introduced when telephone companies shifted the use of telephone numbers from mere use in completing calls to also providing identification to the recipient.[187] Now it has become one of the most convenient services, allowing recipients to selectively receive calls and avoid unwanted contact.[188] 'Amazon Recommendation' is another example of efforts to develop better products and services. Amazon uses customers' purchasing and browsing history to create recommendations and provide customized suggestions, which have made it easier for customers to locate products that they may need.[189] This has substantially increased sales as well.[190]

---

[185] *See id.* § 1030(c)(4)(A)(i)(I) (Supp. V 2010).

[186] *See id.* § 1030(e)(11).

[187] Public Comment on Preliminary FTC Staff Report from Michael Richter, Chief Privacy Counsel, Facebook, to Fed. Trade Comm'n 7 (Feb. 18, 2011) [hereinafter Facebook Comment], *available at* http://www.ftc.gov/os/comments/privacyreportframework/00413-58069.pdf.

[188] *See id*.

[189] *See id.* at 8.

[190] *See* Matt Wesson, *How to Use Your Customer Data Like Amazon*, PARDOT (Aug. 27, 2012), http://www.pardot.com/drip-campaigns/customer-data-amazon.

[50] Court judgment records are another example of indirect socially accepted disclosable information. Unless sealed, court records are public records and accessible to the public.[191] However, a private aspect of court judgments presents a privacy issue. One such example is a criminal record. Regardless of whether a person committed a felony or a misdemeanor, a person is reluctant to disclose his criminal records because it might damage his public reputation. The same applies to bankruptcy and restraining orders.

[51] Although it is true that court judgments have some private aspects, disclosures of court judgments cannot constitute harm because their benefits to society outweigh individual harm. Disclosures of criminal records serve to lawfully disqualify unfit people to carry out certain jobs. Many employers conduct pre-employment background checks. Employers conduct background checks to avoid claims of liability for negligent hiring, which allege that a hired employee with a criminal record harmed others, all of which could have been avoided by a criminal record check.[192] For example, child molesters can create liability by working at schools and persons with violent criminal records can create liability by becoming police officers.

[52] In addition to criminal records, bankruptcy also provides a legitimate reason for a private employer to refuse to hire an individual. In *Myers v. TooJay's Management Corp.*, a potential employee, who had filed for Chapter 7 bankruptcy sued an employer under the Bankruptcy Code's antidiscrimination provision because the employer rescinded an offer after finding out about the employee's bankruptcy record.[193] The court ruled in favor of the employer, relying on the plain language of the

[191] *See generally* 8 FED. PROC., LAW. EDITION § 20:240 (stating that there is both a common-law presumption of, and constitutional right to, court records).

[192] *See generally* RESTATEMENT (SECOND) OF TORTS § 317 (1965); Stacy A. Hickox, *Employer Liability for Negligent Hiring of Ex-Offenders*, 55 ST. LOUIS U. L.J. 1002 (2011) (discussing employer liability for harm caused by their employees).

[193] 640 F.3d 1278, 1281-82 (11th Cir. 2011).

provision.[194] Section 525 of the Code prescribes that a government entity may not deny employment due to bankruptcy whereas no private party may terminate employment due to bankruptcy.[195] In other words, bankruptcy has no bearing whatsoever on government related jobs, but it could serve as a reasonable basis for private companies to refuse to hire an employee although firing an employee because of bankruptcy is forbidden. Due to conspicuously different language, the court inferred Congress's intent to limit the antidiscrimination provision to a government entity and concluded that the statutes did not provide a cause of action against a private employer for an individual who was denied employment due to bankruptcy.[196]

III. HOW TO JUSTIFY COMPENSATION

[53] In the absence of statutes expressly penalizing a database operator for a security breach, the best and most probable claim that individual victims can assert is negligence. The tort negligence rule requires proof of four elements: (1) duty of care, (2) breach of duty, (3) causation, and (4) actual harm.[197] However, data breach cases usually fail to pass the threshold for negligence because they do not satisfy requirements for breach of duty and harm. Because hacking techniques continue to develop and become increasingly sophisticated, a data breach could occur no matter how diligent a database operator is in safeguarding information, with even the most attentive operator not being able to completely prevent hackers from stealing data. Without breach of duty, the database operator is not liable. To this end, this article suggests the imposition of strict liability because data collection constitutes ultrahazardous activity with substantial utility, yet with the inevitable byproduct of a data breach. Also, strict liability is appropriate because it would optimize the extent of data

[194] *Id.* at 1284-85.

[195] 11 U.S.C. § 525(a)-(b) (2006).

[196] *See Myers,* 640 F.3d at 1283-84.

[197] *See* 57A AM. JUR. 2D *Negligence* § 71 (2004).

collection since database operators, knowing they would have to bear the costs of their activities, would adjust the amount of data they store in proportion to their levels of security. In addition, it is equitable in the sense that database operators are the least cost avoiders as opposed to individual victims.

[54] With regard to the harm requirement, medical malpractice cases are illuminating. A lack of actual harm often undermines both a medical malpractice and a data breach case. Although a patient would be afraid of developing an illness, just as a victim of a data breach would be worried about a threat of future identity theft or monetary losses, both are not cognizable harm under the traditional tort analysis.[198] However, courts in medical malpractice cases have expanded the definition of actionable injury, ruling that the possibility of future damage is sufficient to warrant compensation.[199] Furthermore, courts in environmental toxic tort cases have recognized emotional distress as actionable injury, finding distress originating from a fear of future injury is reasonably related to negligent action.[200]

A. Expanding the Traditional Tort Rule: A Threat of Future Injury as Actual Harm

[55] Medical malpractice cases are similar to data breach cases in that often there is no identifiable present injury. In a medical malpractice case, a typical plaintiff suffers an increased risk of future injury, yet the court dismisses the case until the plaintiff can reasonably be diagnosed with an

[198] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) (finding no cognizable injury for threat of data breach with no damages). *See generally* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 (1992) (stating that allegations of a future injury at some indefinite time fails to qualify as an "actual or imminent injury").

[199] *See, e.g.*, Herskovits v. Grp. Health Coop. of Puget Sound, 664 P.2d 474, 478 (Wash. 1983) (concluding that claim was sufficient if negligence increased the risk of injury).

[200] *See* Hagerty v. L & L Marine Servs., Inc., 788 F.2d 315, 318 (5th Cir. 1986).

actual illness.[201] Similarly, the majority of courts in data breach cases have ruled that a threat of future injury does not satisfy the requirement for awarding damages.[202] Loss of time and money spent monitoring a victim's credit does not suffice because the victim's expenditures were "not the result of any present injury, but rather the anticipation of future injury that has not yet materialized."[203] The threat or receipt of unwanted e-mails has also been held to not constitute an injury.[204]

[56] However, some courts hearing medical malpractice cases have taken a step toward redefining actual harm. In *Herskovits v. Group Health Cooperative of Puget Sound*, the defendant physician negligently failed to diagnose the decedent's cancer.[205] This misdiagnosis resulted in a statistically demonstrable reduction in the decedent's chance of survival.[206] The Washington Supreme Court viewed the reduction of a chance of survival as a compensable injury even though the decedent

[201] *See* Herber v. Johns Manville Corp., 785 F.2d 79, 82 (3rd Cir. 1986) ("A future injury, to be compensable, must be shown to be a reasonable medical probability."); Harp v. Ill. Cent. Gulf R.R., 370 N.E.2d 826, 829 (Ill. App. Ct. 1977) (As a general rule, possible future damages are not compensable unless they are reasonably certain to occur) (citing Lauth v. Chi. Union Traction Co., 91 N.E. 431, 434 (Ill. 1977)).

[202] *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *1-2, *7 (S.D.N.Y. June 25, 2010); Key v. DSW Inc., 454 F. Supp. 2d 684, 690-91 (S.D. Ohio 2006); Giordano v. Wachovia Sec., LLC, No. 06-476 (JBS), 2006 WL 2177036, at *4 (D.N.J. July 31, 2006).

[203] Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705, 710 (S.D. Ohio 2007) (quoting Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006)).

[204] *See* Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006).

[205] 664 P.2d 474, 475 (Wash. 1983).

[206] *Id.*

already had a less than fifty percent chance of survival.[207] The court held that the plaintiff did not have to introduce evidence showing that the negligence resulted in injury or death, but "simply that the negligence increased the *risk* of injury or death."[208]

[57] Furthermore, the Connecticut Supreme Court refused to apply the traditional tort rule to a patient because it would bring about an inequitable result. In *Petriello v. Kalman*, the plaintiff was sixteen weeks pregnant when her child died *in utero*.[209] While performing a dilatation, the defendant doctor negligently punctured the plaintiff's uterus.[210] Although the scar tissue did not cause any medical problems, the plaintiff's experts testified that the presence of the scar tissue created an increased risk of future bowel obstruction.[211] The Connecticut Supreme Court held that traditional tort rule was "inconsistent with the goal of compensating tort victims for all the consequences of the injuries they have sustained,"[212] and awarded damages for increased risk of injury.[213]

[58] Moreover, applying the negligence rationale in data breach cases fails to fulfill goals of the tort system. The tort system is said to have three primary objectives: (1) compensation, (2) deterrence, and (3)

[207] *Id.* at 479 ("Damages should be awarded to the injured party or his family based only on damages caused directly by premature death, such as lost earnings and additional medical expenses, etc.").

[208] *Id.* at 478.

[209] 576 A.2d 474, 475-76 (Conn. 1990).

[210] *Id.* at 476.

[211] *Id.* at 477.

[212] *Id*. at 483.

[213] *Id.* at 481.

corrective justice.[214] "Compensation is provided to plaintiffs who can demonstrate that they were harmed by the activities of others," and "[d]eterrence is achieved through the threat of financial liability [because] economically rational actors are forced to take into account the impact of their activities on others."[215] Corrective justice demands that those responsible for harming others restore the harmed persons to their pre-injury status.[216] However, no such punishment is accomplished in data breach cases. The negligence liability tosses out data breach cases for lack of actual harm, leaving victims of data breach cases often, if not always, uncompensated. Consequently, database operators are not required to bear any costs and they have no reason to take steps to prevent future breaches. Additionally, the nature of data breach cases makes it inherently difficult to achieve corrective justice. Corrective justice for data breach cases requires the creation of new personal information for the wronged party because personally identifiable information, once disclosed, is impossible to return to a pre-disclosure status, yet creating new information is not within the tortfeasor's discretion.

[59] Just as medical malpractice cases are instructive in proving harm, environmental toxic tort cases shed light on the demonstration of actual harm in data breach cases. Albert Lin succinctly describes barriers to a plaintiff's recovery in toxic tort cases as follows:

> The characteristics of environmental toxic injuries complicate efficient liability determinations. These injuries tend to involve a large number of persons exposed to significant, albeit low, probability risks. A long latency period between exposure and illness and multiple alternate

[214] *See* DON N. DEWEES, DAVID DUFF & MICHAEL TREBILCOCK, EXPLORING THE DOMAIN OF ACCIDENT LAW: TAKING THE FACTS SERIOUSLY 5-9 (1996).

[215] Albert C. Lin, *Beyond Tort: Compensating Victims of Environmental Toxic Injury*, 78 S. CAL. L. REV. 1439, 1453 (2005).

[216] *See* Jules L. Coleman, *Tort Law and the Demands of Corrective Justice*, 67 IND. L.J. 349, 357 (1992).

> causes of illness exacerbate this causation problem. These difficulties, combined with the costs of litigation, result in the systematic undercompensation of environmental tort victims and the systematic underdeterrence of polluters.[217]

[60] Similarly, a typical data breach case involves thousands of people. The largest data breach ever reported is the Heartland Payment System breach in 2009, which resulted in 130 million records lost.[218] Last year, Sony, the electronic giant, made national news, not for its new products, but for data breaches that resulted in the hacking of seventy-seven million records.[219] These breaches compromised Sony's Play Station Network, Qriocity music, video service, and Sony's Online Entertainment service, with the expected cost of the breaches reaching at least $171 million.[220] Nonetheless, it is uncertain when this breach will result in actual harm and even if harm occurs, whether this incident caused such harm because, unbeknownst to the victims, their information could have been leaked somewhere else.

[61] In addition, victims of environmental toxic torts and data breaches tend to suffer emotional distress.[221] Intuitively, it is understandable for an

[217] Lin, *supra* note 215, at 1441-42.

[218] *See* Nathan Yau, *Largest Data Breaches of All Time*, FLOWING DATA (June 13, 2011), http://flowingdata.com/2011/06/13/largest-data-breaches-of-all-time/.

[219] *See id.*

[220] *See* Mathew J. Schwartz, *Sony Data Breach Cleanup to Cost $171 Million*, INFORMATION WEEK (May 23, 2011), http://www.informationweek.com/news/security/attacks/229625379.

[221] *See* Kahle v. Litton Loan Servicing, 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007) (acknowledging "'findings that identity theft results in more than purely pecuniary damages, including psychological or emotional distress'" (citing Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185PHXSRB, 2005 WL 2465906, at *4 (D. Ariz. Sept. 6, 2005))); Conrad G. Tuohey & Ferdinand V. Gonzalez, *Emotional Distress Issues Raised by the Release of Toxic and Other Hazardous Materials*, 41 SANTA CLARA L. REV. 661, 665-673 (2001) (discussing the development of emotional distress damages in modern toxic tort law).

individual to fear the development of an illness after exposure to toxic substances. Moreover, courts have found that such emotional distress, even without physical illness, warrants compensation.[222] For example, in *Hagerty v. L & & Marine Services, Inc.* the plaintiff was drenched with dripolene, a toxic chemical containing benzene, toluene, and xyolene.[223] The court noted that the plaintiff's present fear constituted a present fact of mental anguish that could be included in recoverable damages and concluded that "[w]ith or without physical injury or impact, a plaintiff is entitled to recover damages for serious mental distress arising from fear of developing cancer where his fear is reasonable and causally related to the defendant's negligence."[224]

[62] A fear for future harm resulting from a data breach is no less reasonable than that of an environmental toxic tort. A recent study shows that a victim of a data breach faces a chance of identity theft that is four times higher than those who were not victims of data breaches.[225] Javelin Strategy and Research, a private research institute, surveyed about 5,000 American consumers in 2009 and found that 19.5% of those who received a data breach notification were later victimized, compared to 4.3% who did not get such a letter but were victimized.[226] Logically and empirically, it is clear that a data breach increases the likelihood of harm, thereby rendering fear for future harm sufficiently reasonable to warrant compensation.

[222] *See* Tuohey & Gonzalez, *supra* note 221.

[223] 788 F.2d 315, 317 (5th Cir. 1986).

[224] *Id*. at 318.

[225] *See* Angela Moscaritolo, *Data breach alerts linked to increased risk of ID theft*, SC MAGAZINE (Oct. 23, 2009), http://www.scmagazine.com/data-breach-alerts-linked-to-increased-risk-of-id-theft/article/156376/.

[226] *See id.*

B. Beyond the Traditional Tort Approach: Data Collection as an Ultrahazardous Activity

[63] Compensating losses when a database operator is not at fault poses another problem. Rapid and innovative technologies are a double-edged sword with respect to an individual's privacy. Database operators have developed a remarkably convenient and reliable system so that individuals can engage in various transactions over the Internet, yet the very same technological advances render no security system impeccable. As one news article reports, nothing is truly secure on the Internet.[227] With ever increasing financial incentives to steal personal information, numerous data breaches have occurred and they will continue to occur no matter how database operators exercise diligence, yet the traditional negligence tort liability is ill equipped to deal with such problems.

[64] Beyond the traditional tort approach, Danielle Citron provides a noteworthy analysis.[228] She defines security breaches as "an inevitable byproduct" and a residual risk of collecting sensitive personal information because no amount of due care will prevent data breaches.[229] She argues that negligence will never deter database operators from taking adequate precautions because they need not pay for the cost and risks of their activity under the traditional negligence rule.[230] In response, she argues for strict liability for harm caused by data breaches:

> The high levels of residual risk suggest treating cyber-reservoirs as ultrahazardous activities—those with significant social utility and significant risk—that warrant

[227] Jen, *Hacking Attempts Increasing For 2011*, MOBILE INSIDER (May 30, 2011), http://mobileinsider.mobi/news/441.

[228] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 264-66 (2007).

[229] *Id.* at 264-65.

[230] *Id.* at 265.

> strict liability. As Judge Richard Posner has explained, ultrahazardous activities often involve something "new" that society has "little experience" securing, where neither the injurer nor victim can prevent the accident by taking greater care. This characterized water reservoirs in nineteenth-century England. Strict liability creates an incentive for actors engaging in ultrahazardous activities to "cut back on the scale of the activity . . . to slow its spread while more is learned about conducting it safely." Classifying database collection as an ultrahazardous activity is a logical extension of Posner's analysis. Just as no clear safety standard governing the building and maintenance of water reservoirs had emerged in the 1850s, a stable set of information-security practices has not yet materialized today. Individuals can do nothing to ensure their information remains safely inside an entity's database, especially those who have no idea that their data resides there. Database operators, too, are limited in what they can do to protect cyber-reservoirs from significant leaks given the "inevitability" of data-security breaches, even with seemingly responsible levels of precaution against such breaches.[231]

Citron's analogy to water reservoirs is legitimate and her argument for strict liability is persuasive. Both water reservoirs and databases hold enormous resources, making it possible for people to control and process these resources for the benefits of society. When they run well, considerable social utilities flow. However, they are accompanied by significant risks and destructive harm. The problem is that such damage is unavoidable, which reduces both the storage of water and collection of data to ultrahazardous activities. Strict liability is a reasonable and appropriate response to such activities.

[231] *Id.* at 265-66 (alterations in the original) (internal citations omitted).

[65] In addition, the Restatement of Torts supports the definition of data collection as an ultrahazardous activity—the factors to consider in deciding whether an activity is abnormally dangerous are as follows:

> (a) existence of a high degree of risk of some harm to the person, land, or chattels of others; (b) likelihood that the harm that results from it will be great; (c) inability to eliminate the risk by the exercise of reasonable care; (d) extent to which the activity is not a matter of common usage; (e) inappropriateness of the activity to the place where it is carried on; and (f) extent to which its value to the community is outweighed by its dangerous attributes.[232]

[66] An increasing number of data breaches and resulting data loss demonstrate a high likelihood of harm, whereas the inevitability of data breaches explains the inability to eliminate the risk. In addition, the threat of harm is substantially high enough that it is reasonable for people to feel insecure because monetary loss and identity theft are frequent. Moreover, the benefits of data breaches, if any, are negligible in comparison to the potential harm.

[67] Furthermore, strict liability is appropriate because it would optimize the amount of sensitive personal information that is stored in the database. Many database operators tend to collect every possible piece of information irrespective of how it is used because the growth of data storage technology has made cost for additional storage practically zero.[233] On the other hand, they do not allocate sufficient resources for safeguarding that information because they are rarely held liable under the negligence rule and succeed in safely externalizing their business costs.[234]

---

[232] RESTATEMENT (SECOND) OF TORTS § 520 (1977).

[233] *See* Michael Hintze, *Protecting Data: Security, Minimization and Anonymization*, *in* 2 PRACTICING LAW INST., NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW 299, 307 (June-July 2008).

[234] *See* Citron, *supra* note 228, at 265.

However, strict liability would change such tendencies. Database operators who keep marginally productive databases or those who are vulnerable to a security breach would be forced to decrease data collection in addition to bearing the cost of their activities.

[68] Moreover, strict liability is equitable in the sense that a database operator is the party who can avoid the loss at the least cost. Undoubtedly, between an individual and a database operator, the database operator is in the better position to take responsibility for data breaches because the operator has greater economic resources and is equipped with better knowledge.[235] One problem with this loss allocation rule, however, is that it may disincentivize individuals to take steps to reduce the likelihood of the loss because individuals have no reason to be cautious, knowing that the operator will take full responsibility. Modern loss allocation schemes have addressed this problem by splitting the loss between parties. For example, when a credit card is stolen, a cardholder's liability is limited to fifty dollars for unauthorized use[236] and the card issuer absorbs the remainder of the loss.[237] Imposing some liability on the cardholder makes the cardholder protect the card against loss or theft, and imposing some liability on the card issuer encourages the card issuer to develop systems that prevent the use of stolen cards.[238] The goal is to impose enough of a loss on individuals to give them an incentive to prevent the fraud without overwhelming them.[239] Because it is not only advised, but also encouraged, for individuals to take steps to secure personal information, this modified approach could serve to promote individuals' security awareness and become an alternative to pure strict liability.

[235] *See id.* at 284-85.

[236] *See* 15 U.S.C. § 1643(a)(1)(B) (2006).

[237] *See id.* § 1643.

[238] *See* Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 380 (2003).

[239] *Id.* at 379.

IV. HOW TO STRUCTURE A UNIFORM COMPENSATION SCHEME

[69] There is no law addressing data breaches nor has a uniform compensation scheme been established. Since the numerous state and federal laws preventing unauthorized disclosures of personally identifiable information were not designed to solve issues arising out of mass data losses due to data breaches, they are simply unfit and ill-equipped to deter future breaches and achieve effective compensations. Therefore, this article urges Congress to pass a law that would govern data breaches and require the FTC to create a comprehensive compensation scheme to adequately reflect the respective value of information.

[70] The value of information can be measured. According to the Value of Information formula introduced in Part III, financially sensitive information is the most valuable information because its disclosure is likely to directly affect an individual's financial resources and proves detrimental to an individual's financial well-being. Medical information comes second. The extent of harm due to the disclosure of medical information is no less than that of financially sensitive information because certain harm, such as a loss of employment and the attachment of socially stigmatized diseases, is irreparable. Nonetheless, the disclosure of medical information does not necessarily lead to monetary loss and the lower likelihood of such a disclosure makes medical information place second. The least valued information is socially accepted disclosable information. Typical harm due to the disclosure of socially accepted disclosable information includes unsolicited marketing and emotional distress. Although constant unsolicited marketing and the resulting emotional distress increase the expected value of harm, the benefits of disclosure negate the harm.

[71] Despite the disparate value associated with each type of information, laws are blind to such differences. This is because most laws were enacted without having weighed the relative value of information and ignore the importance of the differing value of each piece of information. For example, the Fair Credit Reporting Act ("FCRA"), which regulates the accuracy of credit reporting, imposes a minimum $100

and a maximum $1,000 fine for willful violations.[240] The Health Information Technology for Economic and Clinical Health ("HITECH") Act addresses the privacy and security concerns associated with the electronic transmission of health information and was designed to effectively enforce HIPAA rules.[241] The tiers in the HITECH Act categorize violations based on mental state from the least to most serious and the civil penalty, ranging from $100 to $50,000, reflects the degree of the violation.[242] Even though information on credit reports is financially sensitive information, which is more valuable than medical information, the FCRA limits the penalty to $1,000 whereas the HITECH Act allows the maximum penalty of $50,000 for each violation.[243] Thus, an individual who is denied a line of credit due to wrong information on his credit report and as a result loses his business, would receive only $1,000 whereas another individual whose medical information is intentionally uncovered, yet suffers no harm, would be compensated with $50,000.

[72] Much like all personal information, a Social Security number is undervalued. While federal laws do not impose civil penalties for the unlawful disclosure of a Social Security number, several states do.[244] For instance, Arizona prohibits the display of documents that show more than five digits of an individual's Social Security number on public websites and an entity that violates the provision is subject to a civil penalty of up to $500.[245] The state of Michigan enacted the Social Security Number

[240] *See* 15 U.S.C. §§ 1681(b), (n) (2006).

[241] *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226, 230, 242 (2009) (codified in scattered sections of 42 U.S.C.).

[242] *See id.* at 226-73.

[243] *Compare* 15 U.S.C. § 1681(n) (limiting the FCRA penalty to $1,000), *with* 123 Stat. at 273 (stating the maximum HITECH penalty is $50,000).

[244] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1373 (2007).

[245] *See id.*

Privacy Act and prohibits the use of more than four sequential digits of the Social Security number in addition to restricting the use of Social Security numbers on identification and membership cards, permits, and licenses.[246] Moreover, a person who obtains Social Security numbers in the ordinary course of business is required to create a privacy policy.[247] A violation of the Act is punishable by imprisonment for no more than ninety-three days, a fine of no more than $1,000, or both.[248] New York[249] and Texas[250] also impose up to $1,000 penalties for similar violations. According to various state statutes, an individual's Social Security number is valued up to $500 or $1,000 and it is substantially lower than the values of medical information under HITECH, which allows compensation up to $50,000.[251]

[73] The CAN-SPAM Act, which regulates commercial spam mails, exemplifies the civil penalty with respect to socially accepted disclosable information.[252] The Act stipulates civil penalties of $100 for transmitting false and misleading information and $25 for other less serious violations, such as continuously sending spam e-mails after objection.[253] In accordance with the CAN-SPAM Act, sending a deceptive email is punishable with the same dollar amount as is imposed by the FCRA for furnishing wrong information to a credit reporting agency.[254]

---

[246] *See* MICH. COMP. LAWS § 445.83 (2009).

[247] *See id.* § 445.84.

[248] *See id.* § 445.86.

[249] *See* N.Y. GEN. BUS. LAW, § 399-ddd (McKinney 2009).

[250] TEX. GOV'T CODE ANN. § 552.352 (West 2003).

[251] *See* 42 U.S.C. § 1320d-5 (2006).

[252] *See generally* 15 U.S.C. § 7706 (2006).

[253] *Id.* § 7706(g)(3).

[254] *See* 15 U.S.C. § 1681n (2006).

[74] The inadequacy of compensation in part derives from the fact that laws governing personal information are outdated. The FCRA was originally passed in 1970.[255] Although the Fair and Accurate Credit Transactions Act amended the FCRA in 2003, the amendment did not revise the civil penalties and consequently, the dollar amount of penalties is still tied to monetary values from the 1970s.[256] On the other hand, HITECH was signed into law on February 17, 2009,[257] which explains the higher amount of civil penalties.

[75] To deter future breaches and achieve effective compensations, this article argues that it is necessary to establish a uniform civil penalty scheme based on the value of information. However, assigning the exact value of each type of information is beyond the scope of this article and Congress should pass a law directing the FTC to propose a comprehensive compensation system.[258] In fact, both the White House and the FTC have called for privacy legislation. On February 23, 2012, the White House unveiled its blueprint for a Consumer Privacy Bill of Rights to protect consumers online.[259] Stressing transparency, security, and user control of

[255] *Id.*

[256] *Compare* Fair and Accurate Credit Transactions (FACT) Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952, 1953*, with* 15 U.S.C. § 1681n (2006).

[257] *See HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited Oct. 9, 2012).

[258] *See Legal Resources- Statutes Relating to Consumer Protection Mission*, FED. TRADE COMM'N, http://www.ftc.gov/ogc/stat3.shtm (last visited Oct. 9, 2012) ("Telemarketing and Consumer Fraud and Abuse Prevention Act (codified in relevant part at 15 U.S.C. §§ 6101-6108) . . . requires the FTC to promulgate regulations (1) defining and prohibiting deceptive telemarketing acts or practices; (2) prohibiting telemarketers from engaging in a pattern of unsolicited telephone calls that a reasonable consumer would consider coercive or an invasion of privacy. . . .").

[259] *See* Danny Weitzner, *We Can't Wait: Obama Administration Calls for a Consumer Privacy Bill of Rights for the Digital Age,* THE WHITE HOUSE BLOG (Feb. 23, 2012, 4:00

data, it called on Congress to pass legislation based on the Consumer Privacy Bill of Rights model.[260]

[76] Subsequently on March 26, 2012, the FTC released its final report entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers."[261] The FTC report called for the enactment of baseline privacy legislation and for legislation giving consumers the right to access personal information held by data brokers.[262] However, the effect of the Privacy Bill of Rights and the FTC's final report is questionable since both depend on industry self-regulations. The Electronic Privacy Information Center ("EPIC") criticized the FTC for "mistakenly endors[ing] self-regulation" and for not using Section 5 power to safeguard consumers' interests.[263]

[77] Self-regulation would not go a long way to protect personal information. Constructing and enforcing a uniform civil penalty scheme is imperative. Thus, this article suggests a scheme that models the HITECH Act. The Act, in determining the amount of penalties, takes into account the violator's mental state, from not knowing and exercising reasonable diligence to willfully neglectful, and whether the violation has been corrected, and sets forth four tiers of penalties.[264] If a violator did not know, and by exercising reasonable diligence would not have known, that

PM), http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age.

[260] *See id.*

[261] *See FTC Issues Final Commission Report on Protecting Consumer Privacy*, FED. TRADE COMM'N (Mar. 26, 2012), http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[262] *See* PROTECTING CONSUMER PRIVACY, *supra* note 2, at 72-73.

[263] *Federal Trade Commission Calls for Privacy Legislation*, EPIC (Mar. 26, 2012), http://epic.org/2012/03/federal-trade-commission-calls.html.

[264] *See* 45 C.F.R. § 160.404(b)(2)(i)-(iv) (2011).

he or she violated the law, each violation costs from $100 to $50,000, not exceeding $1,500,000 per year.[265] When a violation was due to reasonable cause and not willful neglect, a penalty ranges from $1,000 to $50,000, not exceeding $1,500,000 per year.[266] If a violation originated from willful neglect but was corrected, a violator is fined from $10,000 to $50,000 for each violation, not exceeding $1,500,000 per year.[267] For violations constituting willful neglect, that are uncorrected and an uncorrected, the minimal penalty is $50,000 and is limited to $1,500,000 per year.[268] Likewise, this article proposes that a penalty should be tied to the value of information, calculated by the Value of Information equation. Thus for data breaches, an entity who is obligated to secure an individual's information from an unauthorized disclosure pays the individual in the amount set below:

Tier A: Socially Accepted Disclosable Information

(1) If the disclosures involve indirect socially accepted disclosable information, $W for each disclosure.

(2) If the disclosures involve direct socially accepted disclosable information, $X for each disclosure.

Tier B: Medical Information

(1) If the disclosures involve medical information, $Y for each disclosure.

Tier C: Financially Sensitive Information

(1) If the disclosures involve financially sensitive information, $Z for each disclosure.

[78] In designing such a scheme, the FTC's aim should be deterring future breaches rather than punishing operators. Accordingly, the amount

[265] *See id.* § 160.404(b)(2)(i)(A)-(B).

[266] *See id.* § 160.404(b)(2)(ii)(A)-(B).

[267] *See id.* § 160.404(b)(2)(iii)(A)-(B).

[268] *See id.* § 160.404(b)(2)(iv)(A)-(B).

of civil penalties should not be excessive, hinder business activities, or force database operators out of business. However, effective deterrence demands multiple compensations. To put it another way, a database operator should be required to pay for a loss even if information has been previously leaked. This is because denying compensation due to a previous breach and rendering disclosed information unworthy would erode the effectiveness of deterrence. In addition, the amount of a penalty should be tied to the number of lost pieces of information so that an individual who suffers multiple losses should be entitled to multiple compensations. For example, an individual whose name, phone number, and address are disclosed is compensated for the three losses, whereas an individual who loses a single e-mail is entitled to a single damage award. It would lead the database operator to less likely collect marginally productive information.

V. CONCLUSION

[79] Data breaches have become a serious social cost. An increasing volume of personal data is stored and processed, yet no one is held liable for unauthorized disclosures and victims are forced to bear the loss. Multiple causes contribute to such an inequitable result. First, courts have uniformly held that costs for credit monitoring and emotional distress due to an increased risk of identity theft and unsolicited marketing are not actual compensable damages.[269] Consequently, victims are forced to wait until they suffer legally cognizable harm, such as monetary losses, identity theft, or even a loss of employment opportunity. Even if harm occurs, multiple causations and alternative explanations for the harm hinder victims of data breaches from being adequately compensated. This article finds a solution to such a problem in medical malpractice and toxic tort

[269] *See generally* Timothy H. Madden, *Data Breach Class Action Litigation—A Tough Road for Plaintiffs*, BOSTON B. J., Fall 2011, at 28-29 (stating that claims involving no demonstrable use of compromised information have faired poorly).

cases where courts have recognized immaterialized future harm and emotional distress due to a threat for future injury.[270]

[80] Compensation becomes more challenging because the database operator is not liable for such harm under the traditional tort rule.[271] However, strict liability resolves the issue. Imposing strict liability is appropriate because data collection, which accompanies an unavoidable risk of a breach, constitutes an ultrahazardous activity. It is also encouraged because database operators would be compelled to optimize the degree of data collection. An alternative to pure strict liability includes requiring victims to bear losses up to a certain point in order to promote the awareness in protecting personally identifiable information.

[81] Establishing a uniform compensation scheme is critical. The penalty scheme should be designed to deter future breaches and facilitate effective compensation. Thus, the amount of penalty should not be too burdensome to database operators. This should be made possible by Congress, who should order the FTC to conduct research on the values of information and tie a civil penalty to each type of information. Determining the exact value of information is beyond the scope of this article. Instead, this article formulates the Value of Information equation and categorizes information as financially sensitive information, medical information, and socially accepted disclosable information, in descending order.

[270] *See, e.g.*, Petriello v. Kalman, 215 Conn. 576 A.2d 474, 484 (Conn. 1990) (finding that increase risk of future harm entitles a plaintiff to compensation in a medical malpractice case); Donovan v. Philip Morris USA, Inc., 914 N.E.2d 891, 894-95 (Mass. 2009) (finding a cause of action for future medical expenses after the plaintiff was exposed to hazardous martial in a toxic tort case).

[271] *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 275 (2005).