PRIVACY COSTS AND PERSONAL DATA PROTECTION: ECONOMIC AND LEGAL PERSPECTIVES

Sasha Romanosky & Alessandro Acquisti†

TABLE OF CONTENTS

---

† Sasha Romanosky is a PhD student at the Heinz College at Carnegie Mellon University. Alessandro Acquisti is an Associate Professor of Information Systems and Public Policy also at the Heinz College at Carnegie Mellon University. We can be reached at [sromanos, acquisti]@andrew.cmu.edu. We would like to thank the following people for their insightful comments and feedback: John Bagby, Fred Cate, Ben Edelman, Mark Melodia, and Alana Maurushat. We would like to acknowledge CyLab at Carnegie Mellon for their generous support. We would also like to thank Charlotte Chang, Varty Defterderian, Kristin Kemnitzer, and Peter Nagle for their excellent editing.

I. INTRODUCTION

In 1994, the U.S. Congress enacted the Drivers Privacy Protection Act (DPPA)[1] to protect the privacy of personal data collected by states' Departments of Motor Vehicles (DMVs). The Act made parties such as data brokers or DMVs liable to individuals whose personal information had been wrongfully used or released. The DPPA allowed offended individuals to bring a civil action in a United States district court against violators, permitting courts to award "*actual damages*, but not less than liquidated damages in the amount of $2,500."[2] However, obtaining compensation by proving *actual* damage proved elusive: after all, what constitutes an actual damage when an individual's personal information assembled by a state's DMV is simply passed to third parties—such as data aggregators and data brokers? In 2005 the Eleventh Circuit resolved that under the DPPA, individuals did not have to prove actual damages in order to get liquidated damages.[3] But this has not translated to other privacy legislation, particularly in the area of consumer data breaches:[4] obtaining compensation for the loss or theft of personal information held by another entity has not, generally, proved viable.[5]

Economic and legal theories seem to assess differently what constitutes consumer harm resulting from a breach of personal data: economic theory may recognize privacy costs that legal jurisprudence does not.[6] For an economist, the potential damages from the dissemination of consumer informa-

1. 18 U.S.C. §§ 2721-2725 (2006).
2. 18 U.S.C. § 2724(b)(1) (2006) (emphasis added).
3. Kehoe v. Fid. Fed. Bank & Trust, 421 F.3d 1209, 1210 (11th Cir. 2005).
4. We generally refer to "breaches" as the loss or theft of personal consumer information. For instance, the California data breach disclosure law defines a breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." *See* CAL. CIV. CODE §§ 1798.29, 1798.82 (2002).
5. For example, in a 2004 case involving the wrongful disclosure of a Social Security Number, the Supreme Court ruled that the Privacy Act of 1974 requires an individual to prove actual harm before he can receive the minimum statutory award. Doe v. Chao, 540 U.S. 614, 617-18 (2004).
6. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 115-16 (Anupam Chander et al., eds., 2007).

tion may be various: from the increased probability of receiving spam or being subject to identity theft (which elevates the individual's expected, though not necessarily realized, costs), to the decrease in market value of their personal data, given its wider availability and lower scarcity. For the economist, the difference between an actual and a possible cost is a matter of probabilities and uncertainty; in either case, the breach of a consumer's data has heightened the *expected* costs—be they tangible or intangible—that the consumer will suffer when (and if) his data is abused. However, while other areas of law have accepted the concept of probabilistic damage,[7] such ambiguity is, most of the time, unacceptable to personal data protection legislation: under the law, a person may not be able to sue a data broker for *future* or *potential* identity theft, which *may* have originated from the disclosure of his personal data. Under tort law, compensation for losses requires plaintiffs to demonstrate harm to one's person or property. While additional pecuniary awards can be granted for economic loss, they are predicated on actual or physical harm. As a result, courts (and juries) have often rejected attempts to award damages for breaches of personal information,[8] challenging the very effectiveness of policy initiatives aimed at protecting consumer data.[9] The goal of this Article, therefore, is to examine U.S. personal data protection laws using the lens of economic theory. We focus on consumer data breaches resulting from the loss or theft of personal information held by another entity.

Personal information flows are necessary for the functioning of modern economies and are often beneficial to consumers (data subjects), first parties (data holders), and third party companies (data brokers). Consumers benefit from transactions involving their personal data due to easier access to credit and insurance,[10] customization,[11] and personalization.[12] However, they may

7. *See generally* Glen O. Robinson, *Probabilistic Causation and Compensation for Tortuous Risk*, 14 J. LEGAL STUD. 779 (1985); Richard W. Wright, *Actual Causation vs. Probabilistic Linkage: The Bane of Economic Analysis*, 14 J. LEGAL STUD. 435 (1985). *See also* Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. (2008), 223-47 *available at* http://ssrn.com/abstract=998305, discussed *infra* in the Article, on the comparison between harm following data breaches and medical cases that allow for damages for monitoring one's health after being exposed to toxic chemicals.

8. *See infra* Section III.B.

9. P. H. RUBIN & T. M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 16 (2002).

10. *See generally* NICOLA JENTZSCH, THE REGULATION OF FINANCIAL PRIVACY: THE UNITED STATES VS. EUROPE (ECRI, Research Report, No. 5) (2003); Nicola Jentzsch & San José Riestra, *Consumer Credit Markets in the United States and Europe*, *in* THE ECONOMICS OF CONSUMER CREDIT 27 (Giuseppe Bertola et al., eds., 2006).

11. *See* Robert C. Blattberg, & John Deighton, *Interactive Marketing: Exploiting the Age of Addressability*, 33 SLOAN MGMT. REV. 5, 5 (1991).

also be harmed by abusive treatment of their data; they may suffer from identity theft, discrimination, or social stigma;[13] they may witness degraded value of their personal data publicly disclosed, or suffer other psychological, intangible costs. Companies also bear costs when they misuse—or, specifically, lose because of negligence or criminal attacks—consumers' personal data: they may sustain negative publicity, embarrassment, lost sales, or suffer fines or other sanctions.[14] Technological solutions such as data security and privacy enhancing technologies[15] can help balance the interests and needs of data subjects and data holders.[16] However, they are not always spontaneously adopted by individuals or companies,[17] which drives the motivation for policy intervention: in the U.S. there exists a patchwork of state and federal legislative initiatives that attempt, in coordination with self-regulatory approaches, to reduce data breaches, protect personal information, and mitigate the harm to disparate parties due to these breaches.

In this Article, we undertake an economic analysis and comparison of such legal mechanisms for consumer data protection. Our goal is not to establish the value of privacy legislation using economic theory: the vast and complex array of U.S. legislative initiatives meant to protect personal information is clear proof of an interest in protecting consumer data while maintaining beneficial flows of personal information. Rather, we investigate the effectiveness of those initiatives. We focus on data breaches and the resulting

---

12. *See* Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MARKETING SCI. 367, 374 (2005).

13. *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21 (2004).

14. *See* David Streifield, *On The Web, Price Tags Blur; What You Pay Could Depend On Who You Are*, WASH. POST, Sept. 27, 2000, at A1. *See also* Alessandro Acquisti et al., *Is There a Cost to Privacy Breaches? An Event Study*, ICIS 2006 PROCEEDINGS 1563 (2006). For further discussion regarding sanctions imposed by the FTC on firms that violate privacy policies and engage in deceptive practices using consumer data, see *infra* Section III.A.

15. *See generally* Ian Goldberg, *Privacy-Enhancing Technologies for the Internet III: Ten Years Later*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES (Alessandro Acquisti et al. eds., Auerbach, 2008).

16. Data subjects (consumers) may want stronger protection of their personal information, while data holders (ecommerce, marketing, data brokers, etc.) benefit from less stringent regulations.

17. *See generally* Benjamin D. Brunk, *Understanding the Privacy Space*, 7 FIRST MONDAY 10 (Oct. 2002), http://131.193.153.231/www/issues/issue7_10/brunk/index.html (discussing investments in privacy enhancing technologies). Naturally, companies have incentives to invest in information security to protect their information systems and assets. *See generally* Lawrence Gordon & Martin Loeb, *The economics of information security investment*, 5 ACM TRANSACTIONS ON INFO. & SYS. SECURITY, 438 (2002). However, it is an unresolved issue how much the consideration of consumer data privacy affects those incentives.

consumer costs of such violations.[18] Specifically, we present an economic analysis of three legislative approaches used to reduce the potential privacy harm from a firm's activity: ex ante safety regulation, ex post liability, and information disclosure. In addition, we discuss the means by which legal and economic frameworks calculate and compensate for consumer loss. Ex post liability, ex ante regulation, and information disclosure laws have had only mixed success in preventing consumer data breaches. Some of the causes for such lukewarm results relate to challenges that each of these mechanisms face in the marketplace—challenges that economic theory (in particular, behavioral economics and transaction costs economics) help explain.

The rest of the Article is structured as follows: first, we introduce the general mechanisms of regulation, liability, and information disclosure. We next present examples of these approaches in the area of personal information protection and analyze their impact, showing a gap between the legislature's intentions and marketplace reaction. Finally, we provide a formal economic analysis of regulation, liability, and information disclosure, and contrast conditions under which they may be socially efficient or inefficient.[19]

II. CONSUMER DATA PROTECTION LAWS

Despite, or perhaps because of, the adoption of more U.S. state laws requiring firms to notify consumers of data breaches, breaches appear to be occurring more frequently. For example, the identity theft resource center (ITRC)—which maintains a detailed catalog of reported data breaches—recently announced a surge in breaches in 2008 to 656, up 47% from the previous year.[20] Such breaches can have a tremendous range of impacts for the individuals whose data are affected. In cases where the breach is caused by simple loss of a backup tape, or theft of a device with intention to wipe the contents and sell the hardware, the financial impact to consumers may be negligible—in fact, there may be none. However, breaches can also result in various types of identity theft (ranging from fraudulent unemployment

18. In this article, we focus on data breaches in which the data of individuals (such as consumers, employers, or third parties) held by a company was exposed because of poor security practices, obtained by unauthorized parties (such as cyber-criminals), lost (in computers or data storages went missing), sold, or otherwise traded in manners that generate suspicion of illegality in the victims.

19. We refer to whether these methods succeed or fail to minimize total firm and consumer costs. A level of care that minimizes the sum of these costs is known by familiar economic terms as the socially optimal level.

20. Identity Theft Resource Center, *2008 Data Breach Totals Soar*, http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml (last visited July 18, 2009).

claims[21] to fraudulent tax returns,[22] fraudulent loans,[23] home equity fraud,[24] and payment card fraud[25]) which can impose financial, psychological, and other costs on the victims.[26] Consumer costs can be indirect, too. For instance, in response to a breach notification, consumers must process the information and decide a course of action. This imposes cognitive costs and can represent a significant burden.

In addition to losses inflicted to others, the breached institutions can also incur significant costs as a result of incident investigations—whether they are schools, retail stores, hospitals, or government agencies. Such costs include fines paid to federal agencies, legal fees, and consumer redress. For example, the Department of Veterans Affairs paid $20 million to veterans and current military personnel after the theft of a laptop that contained personal information of 26 million veterans, even though officials maintain that no information was accessed.[27] Choicepoint incurred at least $26 million in fines and fees from a breach in 2005,[28] and as of fall 2007 the retailer TJX reported losses of $256 million from its massive data breach in 2005.[29] Heartland Payment Systems, one of the largest credit card processing companies in the United States, incurred $12.6 million in fines and fees from a breach in 2008

---

21. *See* Dan Goodin, *IT Contractor Caught Stealing Shell Oil Employee Info*, THE REGISTER, Oct. 7, 2008.

22. *See* Robert McMillan, *United Healthcare Data Breach Leads to ID Theft*, NETWORK WORLD, June 3, 2008.

23. *See* Mary Hogan, *Arrests Made in ID Theft Case*, SEALY NEWS, Aug. 9, 2008.

24. *See* Brian Krebs, *Thieves Stole Identities to Tap Home Equity*, WASH. POST, Nov. 28, 2008, at E10.

25. *See* Mark Jewell, *TJX Breach Could Top 94 Million Accounts*, MSNBC, Oct. 24, 2007, http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml (reporting that payment fraud from the TJX breach reached $83 million); Ross Kerber, *Grocer Hannaford Hit by Computer Breach*, BOSTON GLOBE, Mar. 18, 2008, http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer_breach/ (reporting 1,800 cases of fraudulent payment card use); *Data-Breach Lawsuit Follows $9 Million Heist*, SECURITY FOCUS, Feb. 6, 2009 (reporting fraudulent losses of $9 million from RBS Worldpay breach).

26. A particularly nefarious example of the consequences of the theft of personal information occurred in *Remsburg v. Docusearch*: the defendant sold personal information about the plaintiff's daughter to Liam Youens, who stalked and killed her. Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

27. Terry Frieden, *VA Will Pay $20 Million to Settle Lawsuit Over Stolen Laptop's Data*, CNN, Jan 27, 2009, http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html.

28. Jaikumar Vijayan, *ChoicePoint To Pay $10M To Settle Last Breach-Related Lawsuit*, COMPUTER WORLD, Jan. 28, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9059659.

29. Ross Kerber, *Cost of Data Breach at TJX Soars to $256m; Suits – Computer Fix Add to Expenses*, BOSTON GLOBE, Aug. 15, 2007, at A1.

that has affected, as of this writing, more than 665 financial institutions.[30] In fact, a recent study revealed an increase in costs to companies because of data breaches every year since 2005.[31]

As a result of data breaches and their costs, U.S. policymakers have produced a patchwork of legislation that creates incentives for companies to protect personal information, and decrease the harm to disparate parties as a result of breaches of this information. This Part presents an overview of the legal approaches adopted to protect personal information, borrowing a classification of legislative initiatives found in the economic theory of law.

A long tradition of scholarship has investigated the relationship between economics and the law, and has applied economic modeling to the analysis of various legislative approaches designed to reduce accident costs.[32] Some literature directly compares ex ante safety regulation with ex post liability,[33] whereas other literature separately discusses the economics of information disclosure.[34]

Ex ante safety regulation is a common way to control or limit an externality caused by a firm's harmful activity. This is an ex ante mechanism, in the sense that it is meant to prevent harm from occurring through the enforcement of minimum standards or operating (compliance) restrictions. It is considered "public" in nature because enforcement is promulgated by sta-

---

30. Linda McGlasson, *Heartland Data Breach Update: Now More Than 665 Institutions Impacted*, BANK INFO SECURITY, Feb 12, 2009, http://www.bankinfosecurity.com/articles.php?art_id=1200.

31. PONEMON INSTITUTE, LLC, 2008 ANNUAL STUDY: COST OF A DATA BREACH 10 (2009).

32. *See generally* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW (2004); WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW (1987); John Prather Brown, *Toward an Economic Theory of Liability*, 2 J. LEGAL STUD. 323 (1973); A. Mitchell Polinsky & Steven Shavell, *Economic Analysis of Law* (Stanford Law Sch., John M. Olin Program in Law & Econ., Olin Working Paper No. 316, 2005), *available at* http://ssrn.com/abstract=859406; Cento Veljanovski, *The Economics of Law* 151 (Inst. of Econ. Affairs, Hobart Paper No. 157, 2006), *available at* http://ssrn.com/abstract=935952.

33. *See generally* Steven Shavell, *Liability for Harm Versus Regulation of Safety* (Nat'l Bureau of Econ. Research, Working Paper Series No. 1218, 1983), *available at* http://ssrn.com/abstract=227549; Steven Shavell, *A Model of the Optimal Use of Liability and Safety Regulation*, 15 RAND J. ECON. 271, 271-80 (1984) [hereinafter *Model*]; Charles D. Kolstad et al., *Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?*, 80 AM. ECON. REV. 888 (1990); Patrick W. Schmitz, *On the Joint Use of Liability and Safety Regulation*, 20 INT'L REV. L. & ECON. 371 (2000).

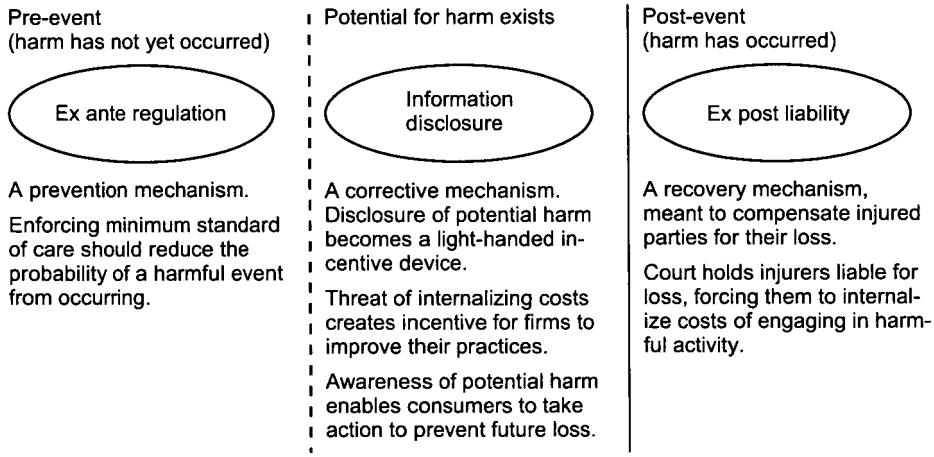
34. *See generally* Steven Shavell, *A Note on the Incentive to Reveal Information*, 14 GENEVA PAPERS ON RISK & INS. 66 (1989); Boyan Jovanovic, *Truthful Disclosure of Information*, 13 BELL J. ECON. 36 (1982); A. Mitchell Polinsky & Steven Shavell, *Mandatory Versus Voluntary Disclosure of Product Risks* (Stanford Law & Econ., Olin Working Paper No. 327, 2006), *available at* http://ssrn.com/abstract=939546.

tutes and government agencies,[35] though safety standards can also be created through self-regulation by firms. An important characteristic is that sanctions can be imposed simply as soon as standards have been violated, even though no harm has yet occurred.

Ex post liability, instead, is exercised after harm has occurred. It is a legal device that enables victims to sue for damages, forcing firms to internalize part of the harm they cause. It is "private" in nature because suits are initiated by private entities such as consumers and corporations.

Finally, information disclosure forces firms to reveal information about the risks of their products or services. The intent is to allow consumers to take action to mitigate potential loss, and create a strong incentive for firms to improve their practices—in order to avoid negative publicity and customer backlash. This approach is a lighter form of intervention in that it does not mandate specific technologies or precautions, and therefore allows market forces to respond freely. Figure 1 illustrates these three mechanisms.

Figure 1: Three Policy Approaches



The dashed vertical line represents an event that could lead to harm, such as a data breach, while the solid vertical line represents the actual harmful consequence, such as identity theft. Below, we discuss how these three legislative approaches have been implemented in the area of consumer data protection as mechanisms to help prevent data breaches. Indeed, the scope of laws and regulations relating to consumer privacy is broad and it is not the purpose of this paper to summarize them all. Instead, we focus our attention on personal consumer data that are the subject of many data breaches, and

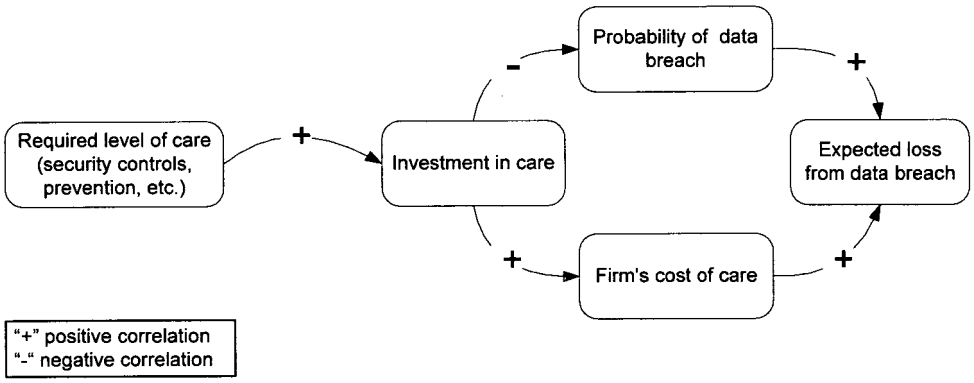
35. Susan Rose-Ackerman, *Regulation and the Law of Torts*, 81 AM. ECON. REV. 54, 54 (1991).

note that the three approaches can (and certainly have been) used in combination.

A. EX ANTE REGULATION

Consumer data protection and compliance regulations require firms to invest in a minimum level of security controls in the hopes of reducing the probability of a data breach and resulting harm. Figure 2 illustrates this mechanism: as the required level of care increases, the investment in security protections also increases, reducing the probability of a breach, which in turn is expected to decrease the loss caused by the firm's activity (such as those cause by a data breach).[36] However, increased investment in care also increases a firm's total expected cost.[37]

Figure 2: Ex Ante Safety Regulation



While a number of U.S. federal and state laws currently mandate only "reasonable" security controls, some states have recently adopted more specific and proscriptive standards.[38] For example, Connecticut law (HB5658),

36. The signs on the arrows in the diagram reflect the correlation between two adjacent stages. E.g., an increase in the probability of a breach increases the expected loss from a data breach. Similarly, because the correlation is positive ("+"), a decrease in the probability of a breach decreases the expected loss.

37. This causality diagram foreshadows an interesting policy problem: while spending more on security lowers the probability of a breach (and resulting harm), it also increases the firm's costs. And so, it is no longer obvious whether the net effect is higher or lower overall costs.

38. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006) (requiring financial institutions to provide "adequate" security controls for consumer information); Sarbanes-Oxley Act 15 U.S.C. § 7262 (2002) (requiring firms to implement reasonable security controls for material computing systems); Health Insurance Portability and Accountability Act Pub L. No. 104–191, § 110 Stat. 1936 (1996) (requiring covered entities to establish reasonable controls protecting personal health information).

An Act Concerning the Confidentiality of Social Security Numbers, requires any person or business that collects or possesses Social Security Numbers to create and publicly display a privacy policy.[39] It also requires, more generally, anyone who possesses personal information to protect it while in use, and destroy it before disposal.[40] Michigan, Rhode Island, and Texas also require similar kinds of data protection and disposal measures.[41]

Both Massachusetts[42] and Nevada,[43] on the other hand, enforce stricter standards through data encryption. For example, in Massachusetts, businesses must encrypt all personal information sent across public (wired or wireless) networks or stored on portable devices (laptops, USB drives, etc). The law "establish[es] minimum standards . . . to safeguard personal information" which apply to every person or business that owns, licenses, or stores personal information of Massachusetts residents.[44] Similarly, the encryption provision of Nevada's data security law prohibits businesses from transferring unencrypted personal information beyond the "secure system of the business."[45]

Federal administrative agencies have also tried to enforce similar standards on entities under their jurisdiction. For example, the SEC proposed an amendment to Regulation S–P as Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information where they propose "more specific requirements for safeguarding information and responding to information security breaches, and broaden the scope of the information covered by Regulation S–P's safeguarding and disposal provisions."[46] Specifically, the proposal would require stricter "administrative, technical and physical information safeguards" for the protection of personal customer data, an increase in the scope of information covered, proper guidelines for

39. H.B. No. 5658 (Conn. 2008), *available at* http://www.cga.ct.gov/2008/ACT/PA/2008PA-00167-R00HB-05658-PA.htm (requiring that policies must "protect the confidentiality of, prohibit unlawful disclosure of, and limit access to SSN").

40. *Id.*

41. *See* MICH. COMP. LAWS ANN. § 445.84 (West 2005); R.I. GEN. LAWS § 11-49.2-2 (2005); TEX. BUS. & COM. CODE ANN. § 48.102(a) (2005).

42. 201 MASS. CODE REGS. 17.01 (2009). Most components become effective May 1, 2009 while the requirement to encrypt data stored on portable devices has been extended to Jan. 1, 2010. *See generally* Kris D. Meade & Robin B. Campbell, *Massachusetts Sets the New Standard, But Delays Implementation*, PRIVACY LAW ALERT (2008), *available at* http://www.crowell.com/NewsEvents/Newsletter.aspx?id=1096.

43. NEV. REV. STAT. § 597.970 (2008).

44. 201 MASS. CODE REGS. 17.01 (2009).

45. NEV. REV. STAT. § 597.970 (2008).

46. Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information; Proposed Rule, 73 Fed. Reg. 13,692 (Mar. 13, 2008) (to be codified at 17 C.F.R. pt. 248), *available at* http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf.

the disposal of personal information, and require that these security policies be formalized in writing.[47]

The FTC employs Section 5 of the FTC Act[48] to impose sanctions on firms that exhibit unfair or deceptive practices—practices that they feel would likely result in the disclosure of personal information or a privacy invasion. The FTC has also created the *Red Flag Rules* which define specialized guidelines for financial institutions and creditors to implement controls that would detect potentially fraudulent activity leading to identity theft.[49]

The enforcement of minimum protection standards can also be achieved through self-regulation. For instance, VISA, MasterCard, and other credit card companies have created a set of guidelines for the protection of payment (debit and credit) card data. Formally know as the Payment Card Industry Data Security Standard (PCI DSS),[50] these rules are mandated by the credit card companies and are ostensibly a prerequisite for any merchant that wants to process payment card transactions. VISA also imposes a requirement that strong encryption be enabled on U.S. gas pumps in order to prevent unauthorized disclosure of personal financial information.[51]

B. EX POST LIABILITY

Negligence liability claims in the context of breaches of personal information generally allow compensation to victims who successfully demonstrate four conditions: (1) that a firm had a duty of care to protect the plaintiff's information, (2) that the firm breached this duty, (3) that actual harm was suffered, and (4) that this harm was a direct result of the firm's breach of duty.[52]

---

47. *Id.*

48. 15 U.S.C. §§ 41-58 (2000). The FTC also imposed sanctions on firms that already incurred breaches, though had not necessarily demonstrated actual harm.

49. *See generally* FEDERAL TRADE COMMISSION, *Fighting Fraud with the Red Flags Rule*, http://www.ftc.gov/redflagsrule (a website developed by the FTC to assist organizations in developing the proper procedures).

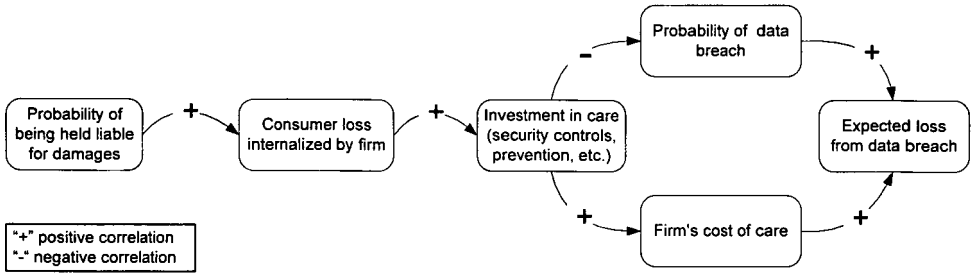
50. PCI SECURITY STANDARDS COUNCIL, *About the PCI Data Security Standard (PCI DSS)*, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited May 1, 2009).

51. Jaikumar Vijayan, *Clock Ticking for Gas Stations to Pump Up Data Security*, COMPUTERWORLD, Jan. 7, 2009, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125261.

52. *See* Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668, 2006 U.S. Dist. LEXIS 4846, at 6 (D. Minn. Feb. 7, 2006); Kahle vs. Litton Loan Serv., 486 F. Supp. 2d 705, 708 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006); Pisciotta v. Old Nat'l. Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *see also* Chandler, *supra* note 6, at 223; John Hutchins, A New Frontier in Privacy Litigation: The Advent of Private

Ex post liability serves as a deterrent for firms by raising their expected costs of engaging in some harmful activity and compensating injured parties for their loss. In the context of consumer losses due to breaches, this causality is illustrated in Figure 3: as the probability of being held liable for damages due to breaches increases, so does the amount of consumer loss internalized by the firm. This, in turn, increases the firm's incentive to further invest in security controls, reducing the probability of a data breach, and finally, reducing the expected harm. Just as with ex ante regulation, higher investment in care also increases the firm's cost of care, increasing the total expected cost of a data breach.

Figure 3: Ex Post Liability



The strongest push towards assigning liability for data breaches has emerged from state legislation that shifts liability for breaches of a specific type of personal information—credit card numbers—from the financial institution to the merchant.[53] While consumers are responsible for a maximum of fifty dollars from a fraudulent charge on their credit card,[54] there are still tangible costs associated with providing the consumer with a new credit card, which represents a social loss.[55] Specifically, such legislative efforts are created to make retailers liable to card-issuing banks for the costs of reissuing payment cards.[56]

For example, while only contractually binding, under the PCI DSS, merchants may be held liable to card-issuing banks if they (or their service providers or business partners) fail to maintain minimum security controls on

---

Lawsuits Over Data Security Breaches at the ABA Annual Meeting, Section of Litigation, Remarks at the ABA Annual Meeting (Aug. 8, 2008).

53. Tracy B. Gray et al., *Privacy & Data Security Briefing: Issue 2*, HOGAN AND HARTSON LLP, at 8 (2008), *available at* http://www.hhlaw.com/pressroom/newspubs/PubDetail.aspx?publication=3628.

54. 15 U.S.C. § 1693(g) (2006).

55. The concept and implication of social loss will be discussed further in this Article.

56. Gray, *supra* note 53, at 9.

computing systems that store, process or transmit payment card information.[57] In addition to minimum standards of care, the PCI DSS effort holds a merchant's acquiring bank liable for breaches suffered by the merchant.

Moreover, in some instances PCI DSS has evolved into a legal standard through the adoption of certain components as state law. For example, Minnesota's Plastic Card Security Act (HF1758) allows financial institutions to bring action against merchants who suffer a breach of a payment card's magnetic stripe information.[58] The act "essentially imposes strict liability on merchants" by requiring them to reimburse financial institutions for issuing new payment cards.[59] Nevada also legalizes PCI DSS by requiring data collectors who accept payment card information from a sale to comply with the PCI DSS standards.[60] Moreover, Nevada law creates a standard of care by absolving any data collector of liability for damages from a data breach if the data collector is in compliance with PCI DSS and if the breach was not caused by gross negligence.[61]

In addition, Connecticut amended its data breach disclosure law (SB1089) to include provisions for liability to the merchant.[62] Specifically, a merchant that suffers a data breach "shall be liable to a bank . . . for the costs of any reasonable action undertaken by the bank . . . on behalf of its customers as a direct result of the breach."[63] The related costs include cancellation or reissuance of cards, and costs associated with stop payments and refunds.[64]

---

57. The relationships involved in PCI DSS compliance are unusual. While it is the merchant that must demonstrate compliance with the PCI DSS standard, it is the merchant's acquiring bank (the entity that settles credit card transactions on behalf of the merchant) that is subject to a fine by a credit card company. This is because only the acquiring bank has a direct relationship with the credit card company, not the merchant. *See* Benjamin Wright, *New Merchant Liability for Losing Credit Card Data,* SANS TECHNOLOGY INSTITUTE, June 14, 2007, http://www.sans.edu/resources/leadershiplab/cc_data_mn_law_bw1.php; David Navetta, *The Legal Implications, Risks and Problems of the PCI Data Security Standard*, THE SCI-TECH LAWYER, Volume 5, Number 1, Summer, 2008, http://www.abanet.org/scitech/scitechlawyer/pdfs/data.pdf.

58. H.F. 1758, 85th (Minn. 2007-2008).

59. Michael P. Carlson & Laura E. Meyer, *Minnesota's New 'Plastic Card Security Act': A Harbinger of Things to Come?*, TRENDS, March/April 2008, at 7, *available at* http://www.faegre.com/files/12645_Trends%20March%20and%20April%202008.pdf.

60. *See* S.B. No. 227 (Nev. 2009), https://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf (repealing NRS 597,970).

61. *Id.*

62. S.B. 1089, Gen Assem., Reg. Sess. (Conn. 2007).

63. *Id.*

64. *Id.*

Other states have tried to pass similar liability bills, including Texas, Illinois, Iowa, Washington, Wisconsin, Alabama, Michigan, and New Jersey. A Massachusetts bill (HB 213)[65] was defeated despite the fact that Massachusetts hosts the head office of TJX Cos., the company that suffered a breach of some 45 million credit card records in 2005.[66] Governor Schwarzenegger vetoed the California bill (AB 779), citing that it would unfairly harm small businesses.[67] The Governor claimed that "the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers" and that "the Payment Card Industry has already established minimum data security standards."[68] The New Jersey law was more robust in that it "could potentially impose liability on any business or government agency that experienced a data security breach involving personal information."[69]

Finally, some data breach disclosure laws allow for a private right of action against an institution in the event of a data breach, as we discuss further below.

C. INFORMATION DISCLOSURE

Information disclosure policies, specifically data breach disclosure laws, work in indirect ways. The force of public notification, a form of light-handed paternalism, enables both consumers and firms to change their behavior and reduce losses. However, information disclosure competes with the stricter, more direct forms of legislation such as ex ante regulation and ex post liability.

Information disclosure as it relates to consumer privacy and data breaches is mainly achieved with the body of state data breach disclosure (or, security breach notification) laws. Currently, at least forty-five states require firms to disclose to consumers when their personal information has been lost or stolen.[70] These laws leverage two important principles, *sunlight as a disinfectant*[71]

---

65. *See* H.B. 213, 185th Gen. Court, Reg. Sess. (Mass. 2007).

66. Grant Gross, *U.S. Authorities Settle with TJX*, TECHWORLD, Mar. 31, 2008, http://www.techworld.com/security/news/index.cfm?newsid=11844. Other reports, however, identify the number of compromised accounts at over 100 million. Privacy Rights Clearing House, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 13, 2009).

67. Letter from California governor, Arnold Schwarzenegger, to the members of the California State Assembly, *available at* http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf.

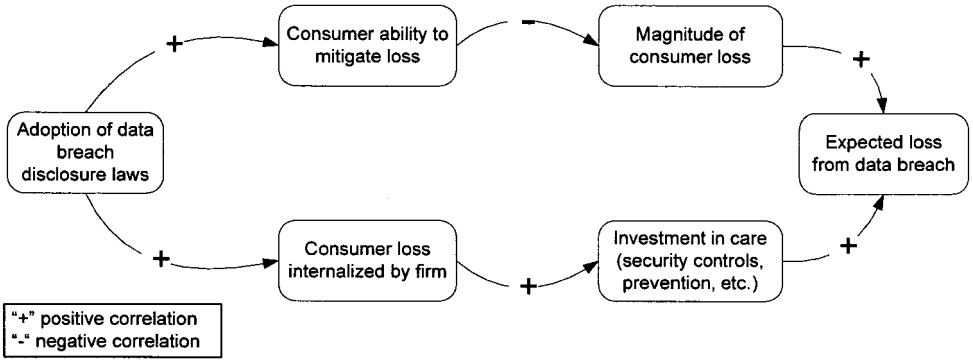
68. *Id.*

69. Gray, *supra* note 53, at 9.

70. *See* Posting to Perkins Coie Internet Case Digest, Missouri Becomes the 45th State to Enact Data Breach Notification Legislation, http://www.digestiblelaw.com/datasecurity/blogQ.aspx?entry=6064&id=34 (July 20, 2009).

and *right to know*.[72] Consider Figure 4. First (upper path), as more states adopt disclosure laws, more consumers are notified, allowing them to take action to mitigate potential harm, such as identity theft. This system is entitled the "right to know." Next (lower path), as more states adopt the laws, more organizations are forced into the "sunlight," increasing the amount of consumer loss internalized by the organization, thus increasing their incentives to improve their security controls. Together, these effects should result in fewer breaches, reducing harm and leading to lower losses overall. The effect of public shame and embarrassment from breaches also contributes to the internalization of the loss.

Figure 4: Information Disclosure



Other statutes also provide for consumer notification in the event of a data breach, and a number of federal bills along similar lines have been written, though they have not passed.[73] For example, the Health Information

71. This phrase is originally attributed to Justice Louis Brandeis from his book. LOUIS BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914).

72. DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 134 (2004), *available at* http://docs.law.gwu.edu/facweb/dsolove/Digital-Person (discussing "right to know" in the context of information privacy); WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION 1 (1992) (discussing "right to know" in the context of environmental regulation).

73. *See* Anne Shelby, *Pending Privacy and Data Security Legislation in the 110th Congress*, PRIVACY & SECURITY LAW BLOG, Mar. 30, 2007, http://www.privsecblog.com/2007/03/articles/federal-legislation/pending-privacy-and-data-security-legislation-in-the-110th-congress; Data Breach Notification Act, S. 239, 110th Cong. (2007), S. 139, 111th Cong. (2009); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007); Data Security Act of 2007, S. 1260, 110th Cong. (2007), H.R. 1685, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007), H.R. 2221, 111th Cong. (April 30 2009); Notification of Risk to Personal Data Act, S. 1350, 108th Cong. (2003), S. 115, 109th Cong. (2005), S. 751, 109th

Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act specifically addresses unauthorized disclosure of personal health information.[74]

III. THE IMPACT OF CONSUMER DATA PROTECTION LAWS

The judgment of the relative costs and benefits of the different legislative approaches we have presented in the previous Section remains nebulous. Since many of the laws described within this Article have only recently been adopted (or will soon be adopted), rigorously estimating their impact is sometimes impossible. Moreover, it is not always clear what metrics should be used to estimate their impact: Even when the stated function of the law may be clear (for instance, forcing firms to disclose breaches they suffered), the ultimate intent may be more ambiguous. Is the purpose of a data breach notification law to afford some level of protection to consumers' data by forcing firms to internalize consumers' losses, or simply to increase the amount of information available to consumer about the handling of their data? Is the legislature trying to fine-tune an "optimal" balance between the costs and benefits of data privacy and commercial flows of information, or trying to achieve a given standard of protection, independently of its economic trade-offs?

Against such background, below we attempt to provide some suggestive evidence for how each of the three legal mechanisms have impacted firms, consumers, data breaches, and the resulting harm from these breaches.

A. EX ANTE REGULATION

We begin by looking at the fines and sanctions that have been levied by regulatory agencies against firms for violating data protection regulations—in particular, the SEC and the FTC. To our knowledge, the SEC has imposed only one sanction against a company for failure to meet minimum standards of care. In July, 2008, the SEC fined LPL Financial $275,000 for shoddy se-

---

Cong. (2005), S. 1326, 109th Cong. (2005), H.R. 1069, 109th Cong. (2005), H.R. 5582, 109th Cong. (2006), S. 239, 110th Cong. (2007).

74. *See* James B. Wieland, *The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"): Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements in the Stimulus Bill*, HEALTHCARE INFORMATION PRIVACY, SECURITY AND TECHNOLOGY BULLETIN, Feb. 19, 2009, http://www.ober.com/shared_resources/news/client_alerts/alert_health/alert_health_021909.html. Specifically, section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act, "HITECH") of the American Recovery and Reinvestment Act of 2009 discusses breach notification requirements. Pub. L. No. 111-5, § 13402, 123 Stat. 115, 227 (2009).

curity controls which led to a breach of consumer data and unauthorized trades.[75] In the settlement, the SEC stated, "[d]espite its being aware as early as 2006 that it had insufficient security controls to safeguard customer information at its branch offices, LPL failed to implement adequate controls, including some security measures, which left customer information at LPL's branch offices vulnerable to unauthorized access."[76]

As mentioned, the FTC has enforced sanctions, both pecuniary and privacy policy-driven ex ante, and also in response to a data breach, where harm may or may not have been directly attributable. For example, in *In re Eli Lilly*, the FTC alleged that Eli Lilly violated its own privacy policy by identifying subscribers' e-mail addresses in an e-mail related to Prozac.[77] The FTC settlement required that Lilly augment its security controls and practices.[78] In *In re Microsoft*, the FTC alleged that Microsoft violated its stated privacy policy of protecting users' information within their .NET Passport service and required them to develop a "comprehensive information security program" certified by an "independent professional every two years" for twenty years.[79] Overall, these cases provide some evidence that federal agencies such as the SEC and FTC can and do impose fines on firms that fail to meet certain standards of care for protecting consumer data.

Regarding PCI DSS, the total volume and actual fines imposed on firms from breaches of credit card data is unclear.[80] VISA claims that acquiring banks are subject to a $100,000 fine for not reporting a confirmed breach and a $500,000 fine for any of their merchants that suffer a breach while non-compliant.[81] In actuality, VISA reported levying fines against U.S. acquiring banks for $3.5M in 2005, $4.6M in 2006, and $11.5M in 2007.[82] In October of 2007, VISA began fining U.S. acquiring banks $25,000 for each

75. *See* SEC Exchange Act Release No. 58515, 7 (Sept 11, 2008), *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.

76. *Id.* at 4.

77. *In re* Eli Lilly, 133 F.T.C. 763, 767 (2002).

78. *Id.* at 784-85.

79. *In re* Microsoft Corp., 134 F.T.C. 709, 742 (2002). Other examples of FTC action ex ante include *In re* Petco Animal Supplies, Inc, 139 F.T.C. 102 (2005), and *In re* Guess?, 136 F.T.C. 507 (2003).

80. While it is the merchant who must demonstrate compliance with the PCI DSS standard, it is the merchant's acquiring bank that is subject to a fine by a credit card company. This is because only the acquiring bank has a direct relationship with the credit card company, not the merchant.

81. *See* VISA, *If Compromised*, http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html (last visited July 10, 2009).

82. *See* VISA, Keeping Electronic Payments Secure, *available at* http://www.corporate.visa. com/md/fs/security/security.jsp (last visited Feb. 21, 2008) (describing vendor compliance and fines levied by VISA).

Level 1 merchant that was non-compliant,[83] and MasterCard is allegedly fining Level 1 and 2 merchants $375,000 annually, and Level 3 merchants $150,000 annually for non-compliance.[84] In particular, VISA fined TJX's acquiring bank $880,000 for the retailer's non-compliance with the PCI DSS standards.[85] Recently, Heartland admitted that "a majority" of the $12.6 million paid in fees from its massive breach went to MasterCard.[86]

While the FTC and SEC clearly do not levy fines against all institutions that incur data breaches, they do act, if only against visibly egregious breaches of consumer data. Furthermore, there is a shortage of data regarding fines imposed for non-compliance of the PCI DSS standard. In short, it is difficult to draw robust conclusions.[87]

B. EX POST LIABILITY

Measuring the impact of an ex post liability policy is also difficult. Private actions brought by consumers against firms often employ negligence claims as a way to recover losses from data breaches. Some of the data breach disclosure laws do allow for private right of action in the event of a data breach. Often, however, courts dismiss negligence claims because of the plaintiff's inability to show actual damages as required by negligence tort claims. This economic loss rule makes it very difficult for plaintiffs to be compensated for strictly pecuniary losses under tort law.[88] These rulings generally establish that

83. *Id.* "Level 1" merchants are defined by VISA to be those that process more than 6 million credit card transactions per year. *See* VISA, Merchants, http://usa.visa.com/merchants/risk_management/cisp_merchants.html (last visited July 19, 2009) (describing the levels and their associated validation requirements).

84. Quarterly fines to level 2 merchants are allegedly $25K, $50K, $100K, $200K while quarterly fines to level 3 merchants are $10K, $20K, $40K, $80K. *See* Branden Williams, *MasterCard to Fine Merchants for Non Compliance*, BRANDEN WILLIAMS' SECURITY CONVERGENCE BLOG, http://blogs.verisign.com/securityconvergence/2009/07/mastercard_to_fine_merchants_f.php (last visited July 30, 2009). Level 2 and 3 merchants are those processing from 1–6 million and 20k–1 million transactions annually, respectively.

85. Ross Kerber, *Visa Fines Bank After Losses in TJX Breach*, BOSTON GLOBE, Oct. 29, 2007, at F1.

86. *See* Heartland Payment Systems, Inc., 6, http://www.sec.gov/Archives/edgar/data/1144354/000119312509107150/d10q.htm; Alex Goldman, *Heartland Hit With $12M Breach Tab*, INTERNET NEWS, May 8, 2009, http://www.internetnews.com/security/article.php/3819596 (citing that $6 million in fines went to MasterCard and $1 million to VISA).

87. Some argue that the actual fines imposed by the credit card companies on merchants are inconsequential compared to increases in transaction fees (called interchange fees).

88. For instance, in *Kahle v. Litton Loan Servicing LP*, the court ruled that, "any injury of Plaintiff is purely speculative" and dismissed the case claiming that the plaintiff "failed to establish an injury." 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007). In *Forbes v. Wells Fargo Bank*, the court ruled that the "the plaintiffs' injuries are solely the result of a perceived risk of future harm." 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006). In *Key v. DSW Inc.*, the court ruled

"unless you have an actual showing of harm as a victim of identity theft, potential harm will not suffice."[89]

Not surprisingly, individuals are also unable to recover costs from efforts to reduce potential identity theft. The Seventh Circuit in *Pisciotta v. Old National Bancorp* did not believe it was reasonable for the company to pay identity theft monitoring services for its consumers because "had the Indiana legislature intended that a cause of action should be available against a database owners for failing to protect adequately personal information, we believe it would have made some more definite statement of that intent."[90] In *Forbes v. Wells Fargo Bank*, the court also explained that costs involved in "expenditure of time and money were not the result of any present injury, but rather the anticipation of future injury that has not materialized."[91] The court ruled similarly in *Kahle v. Litton Loan Services* stating that the case "clearly reject[s] the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring her credit."[92] Yet, consumers continue to try to bring actions for data breaches, for instance, against Starbucks,[93] Heartland,[94] Hannaford Bros,[95] and RBS WorldPay.[96]

---

that the plaintiff's "potential injury is contingent upon her information being obtained and then used by an unauthorized person for an unlawful purpose." 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006). In *Randolph v. ING Life Ins. & Annuity Co.*, the court stated that the plaintiffs failed to demonstrate that any damages were "actual or imminent, not conjectured or hypothetical" and therefore dismissed the claim, charging that "the plaintiff's allegations therefore amount to mere speculation that at some unspecified point in the indefinite future they will be victims of identity theft." No. 06-1228, 10 (D.D.C.Feb. 20, 2007); *see also* Guin v. Brazos Higher Educ. Serv. Corp., No. 05-668, 2006 U.S. Dist. LEXIS 4846, at *10 (D. Minn. Feb. 7, 2006). In *Giordano v. Wachovia Sec., L.L.C.*, the court stated that, "a plaintiff must allege an actual injury or that an injury is so imminent as to be 'certainly impending.' " No. 06-476, 2006 U.S. Dist. LEXIS 52266, 11 (D.N.J. July 31, 2006).

89. Michael Santarcangelo & Patrick Romero, *Do Data-Breach Laws Give You The Power to Hold Corporations Liable?,* SECURITY CATALYST, Nov. 1, 2007, http://www.securitycatalyst.com/do-data-breach-laws-give-you-the-power-to-hold-corporations-liable-2/. Most recently, in *Ruiz v. Gap*, the U.S. District court for the Northern District of California held that an increased risk of identity theft was sufficient for a plaintiff to establish standing but insufficient to maintain a negligence claim. 2009 WL 941162 (N.D. Cal. Mar. 24, 2008); *see* Hogan & Hartson, *Privacy and Data Security Briefing* at 8, June 2009, http://www.hhlaw.com/files/Publication/1f6d3cbc-6ad2-4d0a-a4ca-4fcf4a04b891/Presentation/PublicationAttachment/8dee823c-f6d1-473b-a34f-d2c8407ed313/PrivacyBriefing.pdf.

90. Pisciotta v. Old Nat'l. Bancorp, 499 F.3d 629, 637 (7th Cir. 2007).

91. *Id.* at 55; *see Forbes*, 420 F. Supp. 2d at 1020.

92. *Kahle*, 486 F. Supp. 2d at 711. In *Kahle*, the court ruled that "any injury of Plaintiff is purely speculative" and dismissed the case, claiming that the plaintiff "failed to establish an injury." 486 F. Supp. 2d at 710.

93. Robert McMillan, *Starbucks Sued After Laptop Data Breach*, PC WORLD, Feb. 23, 2009, http://www.pcworld.com/article/160042/starbucks_sued_after_laptop_data_breach.html.

Others take a more creative approach by considering alternative legal arguments, such as medical cases that allow damages for monitoring one's health after being exposed to toxic chemicals.[97] However, it is questionable whether these arguments have legal standing. In *Stollenwerk v. Tri-West Healthcare Alliance*, the district court dismissed a claim that used health analogies (i.e. "toxic torts") because in such cases there is potential for actual (physical) harm.[98] Here, the court stated that "despite findings that identity theft results in more than purely pecuniary damages, including psychological or emotional distress, inconvenience, and harm to his credit rating or reputation, as a matter of law identity theft and credit monitoring must still be differentiated from toxic torts and medical monitoring."[99]

Defending the condition of causality has also been problematic for plaintiffs. Consider a consumer who shops at three competing retail stores using his customer loyalty cards.[100] Quite often, loyalty card applications require the consumer's social security number in order to perform a credit check. Consider then that he receives a breach notification from two of the three companies, and that sometime shortly after, he notices a new loan application (with charges!) on his credit report. He has just become a victim of identity theft. But was it because of these breaches or from something else? Even if he could link the source of the fraudulent application to one of the two companies, from which one exactly did the criminal steal his information? This is precisely what he must prove.

In summary, while consumers do appear to suffer losses as a result of data breaches (whether they be financial, psychological, or expenditures for prevention of future harm), such harms have yet to be fully recognized by

---

94. Elinor Mills, *Heartland Sued over Data Breach*, CNET NEWS, Jan. 28, 2009, http://news.cnet.com/8301-1009_3-10151961-83.html.

95. Trevor Maxwell, *Judge tosses all but one Hannaford data breach claim*, PORTLAND PRESS HERALD, May 13, 2009, http://pressherald.mainetoday.com/story.php?id=256153.

96. Robert Lemos, *Data-breach Lawsuit Follows $9 Million Heist*, SECURITY FOCUS, Feb. 06, 2009, http://www.securityfocus.com/brief/903.

97. Chandler, *supra* note 7.

98. Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185PHXSRB, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. Sept. 8, 2005), *aff'd*, 254 Fed. Appx. 664 (9th Cir. 2007); *see also* Posting of David Navetta to InfoSec Compliance Blog, Stollenwerk v. Tri-West Health – Rise of the Phoenix?, http://infoseccompliance.com/2008/01/04/stollenwerk-v-tri-west-health-%e2%80%93-rise-of-the-phoenix/ (Jan. 4, 2008) (reviewing the case as well as a recent appellate ruling (9th Cir. Nov. 20, 2008) which upheld the lower court's ruling regarding the "toxic tort" claim).

99. *Id.* at 6.

100. The loyalty card, recall, provides the consumer with discounts and special promotions in exchange for his personal information and acceptance of the firm monitoring his shopping habits.

the court system. However, in situations with tangible losses and clear causation, the breached-against party can recover.[101]

C. INFORMATION DISCLOSURE

Above, we presented anecdotal and suggestive evidence regarding the impact of regulation and liability in terms of consumer data protection. In this Section we present evidence of the impact of information disclosure in regards to firm and consumer behavior. Some have tried to determine how the laws have changed organizations' behavior. The authors of a recent study interviewed corporate executives and found that companies are, indeed, improving their practices.[102] Specifically, the laws "empowered [the Chief Security Officers] to implement new access controls, auditing measures, and encryption," and increased awareness within the companies of the importance of information security.[103] There is also evidence to support the belief that disclosure laws can reduce the costs of identity theft, because the sooner one is notified of potential harm, the more quickly one can take action to prevent losses.[104]

Another potential outcome of the notification laws is that public disclosure (the sunlight effect) of a data breach could have a material effect on consumer behavior. Indeed, two surveys suggest that 21%[105] and 19%[106] of respondents claimed to have ceased relationships with the company that suf-

101. For example, TJX recently settled with VISA for $41 million for the cost of replacing credit cards. Linda McGlasson, *TJX, Visa Agree to $40.9 Million Payout for Data Breach*, BANK INFO SECURITY, Dec 4, 2007, http://www.bankinfosecurity.com/articles.php?art_id=648.

102. SAMUELSON LAW, TECHNOLOGY, & PUBLIC POLICY CLINIC, UNIVERSITY OF CALIFORNIA-BERKELEY SCHOOL OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS (2007).

103. *Id.* at 4.

104. SYNOVATE, FEDERAL TRADE COMMISSION: 2006 IDENTITY THEFT SURVEY REPORT 24 (2007) [hereinafter SYNOVATE] (finding that: (1) 30% of those who discovered that their personal information was being misused 6 months or more after it started had to spend $1,000 or more, compared to 10% of those who found the misuse within 6 months; (2) 69% of those who discovered the misuse within 6 months spent fewer than 10 hours compared to 32% of those who took 6 months or more to discover it; and (3) 31% of those who discovered the misuse of their information 6 months or more after it started reported that the thief obtained $5,000 or more, compared to 10% of those who found out in less than 6 months). Other reports provide similar qualitative findings. *Id. at* 8; JAVELIN STRATEGY & RESEARCH, 2009 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 9 (2009), *available at* http://www.idsafety.net/901.R_IdentityFraudSurveyConsumerReport.pdf.

105. Ellen Messmer, *Data Breaches Hurt Corporate Image but Don't Necessarily Drive Customers Away*, NETWORK WORLD, Aug. 29, 2007, http://www.networkworld.com/news/2007/082907-data-breaches-hurt-corporate-image.html?page=1.

106. PONEMON INSTITUTE, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 4 (2005).

fered a data breach. A note of caution, however, is that results obtained through customer surveys can be more reflective of *intended* rather than *actual* behavior.

Some research efforts have also focused on estimating the cost of a data breach to both firms and consumers. For instance, a recent study found that the average cost to a firm from a data breach has been increasing steadily since 2005 ($4.54M in 2005, $6.35M in 2007, $6.65M in 2008).[107] The study calculates totals by aggregating costs of investigation, notification, legal fees, consumer redress (and services such as credit monitoring or reimbursement of credit cards) and customer churn. In fact, the study claims that the majority (69%) of total costs in 2008 was due to lost business, and this percentage increased relative to 2007 and 2006 (65% and 54% of total costs, respectively).[108] If true, this suggests that consumers are indeed punishing firms for data breaches.

However, another recent empirical study attempted to measure the effect of data breach notification laws on identity theft. Using reported identity theft data from the FTC from 2002–2007 and a variation of adoption of data breach disclosure laws across U.S. states, the researchers found that adoption of disclosure laws reduced identity theft by about 2%, though this is only a marginally statistically significant level.[109] Meanwhile, despite increased adoption of data breach disclosure laws, identity theft also appears to be increasing. According to the FTC, reported cases of identity theft have been steadily increasing since 2000 with almost 314,000 consumer complaints in 2008.[110] Another report shows an increase of 8.6% in identity fraud victims in 2008 over the previous year.[111]

In summary, while robust, empirical evidence regarding data breach disclosure laws is minimal, these early studies provide some evidence that the laws may be affecting firm and consumer practices, but only have a marginal effect on identity theft due to breaches.

---

107. PONEMON INSTITUTE, 2008 ANNUAL STUDY: COST OF A DATA BREACH 11 (2009).

108. *Id.* at 12.

109. Sasha Romanosky et al., Do Data Breach Disclosure Laws Reduce Identity Theft? (Sept. 16, 2008) (unpublished article, on file with the Berkeley Technology Law Journal), *available at* http://ssrn.com/abstract=1268926.

110. FTC, CONSUMER SENTINEL NETWORK DATA BOOK 5 (2008). 2006 was the only one year that saw a decline in reported cases (246k down from 256k in 2005, a change of 3.7%). Note that this report reflects total identity theft complaints, only some of which are due to data breaches.

111. *See* JAVELIN, *supra* note 104, at 18. However, the number of 2008 victims (487) is lower than in 2003 (514). This survey also estimates that 11% of identity fraud is due to data breaches while another 11% is due to "online activity." *See* Figure 2 *infra.*

D. DISCUSSION

Though it may be difficult to express a reliable valuation of the impact of these three policy interventions, it is fair to say that their impact has been, at best, mixed.

We can reasonably conclude that the state data protection laws and self-regulations (PCI DSS) are building a foundation for a stronger duty of care for firms to adequately protect consumer information. However, the existence of a relatively small number of sanctions by the FTC, SEC, and the credit card companies, as well as the rising number of reported data breaches,[112] suggest that firms continue to fail in this duty.

Moreover, it appears that these policies have not been subject to rigorous scrutiny, because the legal initiatives are so new, because there is a dearth of reliable quantitative data, or because few attempts have been made to empirically estimate their effects. As mentioned above, it is also not clear what should be the appropriate metric by which to estimate their impacts. Even when the legislature's intention may, at first glance, seem transparent (i.e. defend consumers' privacy), the actual objective may be more ambiguous. For instance, is the objective of data breach notification laws to decrease the instances of identity theft, to decrease the amount of damage they cause on average, to improve firm practices, or all of the above?

Next, we will provide a brief economic analysis of each of these policy approaches in order to offer insight into the conditions under which they become more (or less) effective.

IV. THE ECONOMIC ANALYSIS OF EX ANTE SAFETY REGULATION, EX POST LIABILITY, AND INFORMATION DISCLOSURE

Above, we illustrated the causal mechanisms upon which ex ante safety regulation, ex post liability, and information disclosure rely, and we discussed their limited impacts. Now, we ask the question: given the choice, which policy approach would a social planner (e.g. regulator, government, policy maker, etc.) implement? While companies and consumers will naturally lobby to minimize their own private costs, the social planner's goal is to minimize *the sum* of these costs.

We leverage the economic analysis of accident law and define cost equations for two economic agents: the firm (injurer) and the consumer (victim),

112. See the annual statistics on reported data breaches from DatalossDB. DataLossdb.org, Data Loss Statistics, http://datalossdb.org/statistics (last visited Apr. 30, 2009).

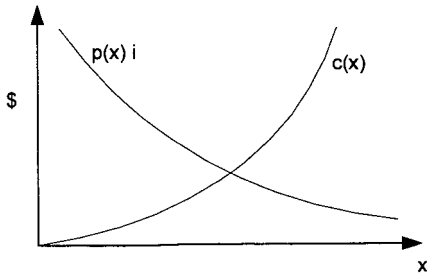
and determine how their costs are affected by each policy approach. The social planner's cost function, therefore, is simply the sum of firm and consumer costs. While they are abstractions from reality (and therefore necessarily inaccurate), these models are useful to understand how incentives and liabilities drive agents' behavior.

First, we will write equations that reflect the simple mechanism of each policy approach, what we will call the "basic equations." This first step will help us understand how these policies operate in an ideal situation. Next, we identify and discuss inefficiencies of each policy—practical conditions under which the policies deviate from theory. Finally, we will update the basic models to reflect these inefficiencies in order to better understand how firms and consumers *actually* behave, what we will call the "extended equations."

A. GENERAL FORMS

Consider a firm that faces the threat of a failure in its product or service (for instance a data breach or environmental pollution) which could harm its consumers. The firm can invest in some level of care, x, to avoid such harm, but the cost of this care, c(x), increases with investment. However the probability of the accident, p(x) and thus the expected harm p(x)i (calculated as the probability multiplied by i, the cost of investigating the cause of the accident) decreases with investment, as shown in Figure 5.[113] The firm's strategic decision is to determine in how much care they should invest in order to minimize their total private costs.

Figure 5: Basic cost functions



Therefore, one might write the firm's loss equation as:

113. The X axis in Figure 5 represents the level of investment in care (security controls) and the Y axis represents cost. As is commonly portrayed, the cost of care, c(x), becomes increasingly steep, implying that it costs more to protect something the more one has already invested. Similarly, the change in probability of an accident occurring, p(x), declines as one invests more in care.

$$\text{Firm loss} = c(x) + p(x)\, i \qquad (1)$$

where, x, c(x) and p(x) and i are as described above. In the event of an accident, consumers may suffer losses and so we can write their loss function as:

$$\text{Consumer loss} = p(x)\, h \qquad (2)$$

where h is the total consumer harm. Finally, the total social loss is composed of both consumer and firm loss:

$$\text{Social loss} = c(x) + p(x)\, [i + h] \qquad (3)$$

Recall that in our model, the decision variable is x, the level of care taken by the firm. Therefore, the objective of the social planner is to achieve a value of x that minimizes equation (3), because social costs are lowest when the firm invests in the socially optimal level. In order to have the firm invest at this level, it must internalize the full amount of its harm.[114] However, since firms are motivated (only) by their own private costs, they invest in a level of care that minimizes (1), not (3), which is always less than socially optimal.[115]

Together, these three equations define our system and the losses to each party, absent any legal intervention. Next, we show how the equations can be modified to reflect ex ante safety regulation, ex post liability, and information disclosure. Note that economic models for regulation and liability have already been explored by a number of scholars, so we present general forms of their results below in an attempt to build upon, not repeat, existing work.[116]

---

114. In familiar economic terms, the social planner wishes to increase the level of care (x) until the marginal cost of the next "unit" of prevention equals the marginal benefit from that unit. That is, until the incremental benefit from one more unit is perfectly offset by the cost of that additional unit. If the firm's cost function is the same as equation (1), then the firm would choose to invest in the same level of care as that desired by the socially planner (i.e. the socially optimal level). An important note, of course, is that the social planner is not choosing to *minimize* accidents, but *optimize* them. This is achieved by minimizing the sum of firm and consumer loss, as seen in equation (3).

115. The concept of an entity not bearing the full cost of their actions (i.e. an externality) is fundamental to microeconomic theory. *See generally* LANDES & POSNER, *supra* note 32 (discussing externalities as applied to tort law).

116. *See id.*; Steven Shavell, *Economics and Liability for Accidents*, (John M. Olin Center for Law, Economics, and Business Discussion Paper No. 535); Kolstad et al., *supra* note 33, at 890.

1. *Ex Ante Safety Regulation*

Under ex ante safety regulation, the social planner must set a standard of care that is constant for all firms no matter their risk of harm. Hence the total cost to society becomes:

$$\text{Social loss} = c(s) + p(s)\,[i + h] \tag{4}$$

where s is a mandated standard that holds the social cost constant with any change in care, x.[117] Firm and consumer costs are similarly given by:

$$\text{Firm loss} = c(s) + p(s)\,i \tag{5}$$

$$\text{Consumer loss} = p(s)\,h \tag{6}$$

2. *Ex Post Liability*

Finally, ex post liability allows compensation to victims for harm caused by firms. In effect, this causes a transfer of cost from the injurer to the injured.[118] However, prior analysis reveals a more complicated form that recognizes how a firm's total cost is reduced because of some probability of evading lawsuit:[119]

$$\text{Firm loss} = c(x) + p(x)\,[i + \alpha\, h] \tag{7}$$

$$\text{Consumer loss} = p(x)\,[1 - \alpha]\,h \tag{8}$$

$$\text{Social loss} = c(x) + p(x)\,[i + h] \tag{9}$$

Where α effectively captures the probability of being held liable for damages and the portion of consumer harm internalized by the firm ($0 < \alpha <$

117. Given a distribution of harm across all firms, and absent better information, the regulator must choose a level of care that reflects the average amount of harm. Its objective, then, is to determine the level of care that minimize c(s) + p(s) E(h), where E(h) is the expectation operator that represents the average level of harm. *See* Shavell, *Model*, *supra* note 33, at 273.

118. We have generalized the type of liability by not specifying negligence versus strict liability. However, in general, privacy harms are best dealt with using negligence liability for which a firm is held liable if they invest in a level of care lower than the standard of care (due care).

119. *See* Shavell, *Model*, *supra* note 33, at 273 (defining the firm's loss function). The social loss function remains unchanged from Equation 3. The difference is simply in how costs are partitioned between injurer (firm) and injured (consumer). Shavell also considers cases where the firm faces the potential for bankruptcy (judgment proof). However, given the extreme rarity of such cases due to data breaches, we will ignore this complexity.

1),[120] and h is again total consumer harm. The consumer loss is then a function of the probability of harm and the remaining cost not paid by the firm.

3. Information Disclosure

As discussed, information disclosure creates two important incentive devices. First, information about potential harms allows consumers to take action to reduce their loss (e.g., notify banks and credit card companies, close accounts, check credit reports, etc.). Second, consumers are also empowered to force firms to internalize some of their loss by "punishing" them for bad practices.[121] Modifying equations (1) and (2) as shown below represents these changes:

$$\text{Firm loss} = c(x) + p(x)\,[i + \lambda\, h(e)] \qquad (10)$$

$$\text{Consumer loss} = p(x)\,[1 - \lambda]\, h(e) \qquad (11)$$

$$\text{Social Loss} = c(x) + p(x)\,[i + h(e)] \qquad (12)$$

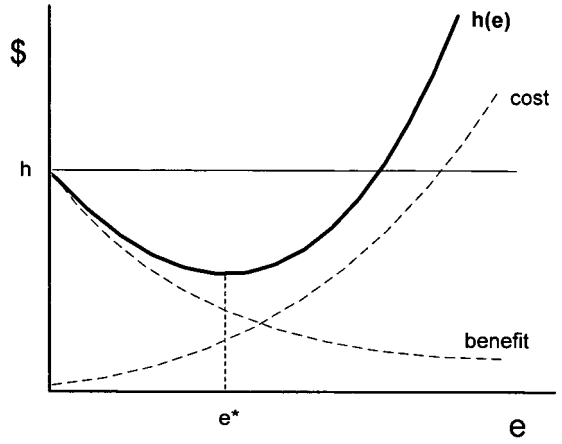
where λ is the amount of consumer loss internalized by the firm ($0 < \lambda < 1$), and the remaining portion, $1 - \lambda$, is that which is born by the consumer.

Further, consumer harm is no longer a constant (h), but becomes a function of consumer action, e. Naturally, we recognize that any action incurs both cost and benefit, and therefore the consumer's strategic decision is to invest in a level of care that minimizes their harm. Total consumer harm, h(e), therefore, is the sum of the dashed cost and benefit curves as shown in Figure 6.

120. As α approaches 1, the company becomes more liable. A value of 1 would imply that the company is always liable (strict liability), whereas a value of 0 would imply that the company always evades lawsuit.

121. For example, they can stop purchasing goods or services from the merchant, sell its stock, or publicly communicate their negative experiences to potential customers. We make the assumption that consumer action affects the *magnitude* of their loss as opposed to the *probability* of the harmful event occurring. These assumptions could easily be relaxed but at the expense of increased complexity and without additional insight. The ability for an individual to contribute in reducing their harm is also known as bilateral care. *See* Shavell, *supra* note 32, at 182 (where both injurers and potential victims are able to affect the probability, not magnitude of harm). And so a characteristic of information disclosure policies is to transform unilateral-care accidents into bilateral-care accidents.

Figure 6: Consumer harm



At small levels of consumer action, the marginal benefit is greater than the marginal cost. Conversely, for very large levels of care, the cost greatly outweighs any benefit. Importantly, there will be a point somewhere in between where the incremental gain from one additional unit of action is perfectly offset by the cost. This point is depicted as e* and represents the optimal level of consumer action.[122]

4. Discussion

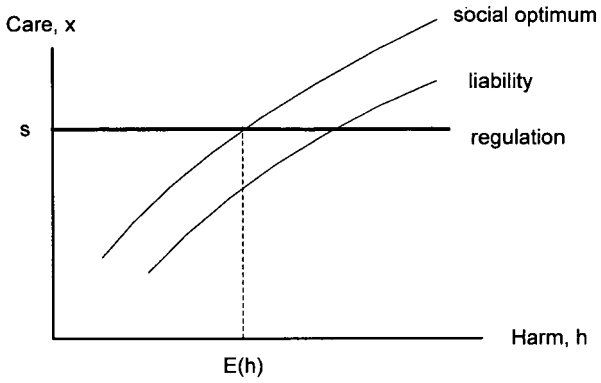
We are now able to provide some initial analysis and comparison between these policy approaches in order to understand whether, at this basic level of analysis, these interventions would incentivize firms and consumers to behave optimally. Two important questions arise: (1) do firms now have incentive to invest in the socially optimal level of care?; and (2) which policy approach ensures the lowest social cost?

First, regulation and liability can be compared against the basic model with regard to care as a function of harm as shown in Figure 7.[123]

122. For the purpose of this model, we assume that h(e=0) = h. That is, the amount of consumer harm from no consumer action is equivalent to h, the level of harm absent disclosure legislation. The distinction between absolute and marginal cost/benefit curves is this: absolute curves depict the total cost or benefit (measured in dollars) of consumer action. Marginal curves, however, depict the incremental change in cost or benefit from one more "unit" of care. Also, note that e* is achieved at the intersection of the *marginal* cost and benefit curves (not shown), not absolute cost and benefit curves as shown in Figure 6.

123. Shavell, *Model*, *supra* note 33, at 275.

Figure 7: Level of care for regulation, liability and social optimum



Given that the level of prevention (x) should reasonably increase with harm,[124] it is clear that the level of care taken by the firm under liability will always be less than is socially optimal for any given amount of harm, h, because of the probability of evading lawsuit. Inefficiencies could also exist in liability because of asymmetric information between legislators, firms, and consumers. For example, in negligence rulings, courts and juries need to compare the level of due care to the injurer's actual level of care. Errors in either establishing the proper standard of care or in the court's estimation of an injurer's level of prevention would result in an inefficient outcome, further reducing α.[125] However, because liability "harnesses the information that victims have about the occurrence of harm," ex post liability may be preferred when consumers, rather than the State, have better information about the impact from harmful activities.[126] Liability may also enjoy lower administrative costs than ex ante safety regulations because the costs are incurred only when harm is demonstrated.[127] Nevertheless, costs arise from each lawsuit and include legal expenses and time for both plaintiffs and defendants. Some even claim that administrative costs can be at least as large as the fines paid from a liability settlement.[128]

As expressed, regulation enforces a constant level of care that becomes socially optimal only at the average level of harm, E(h). The critical assump-

124. That is, the more harm a company is likely to cause, the more prevention measures they should take.

125. Polinsky & Shavell, *supra* note 32.

126. Shavell, *supra* note 116.

127. Though it is not clear whether strict or negligence liability is more efficient. *See id.*

128. *See* Shavell, *supra* note 32, at 281 (describing how administrative costs can be at least equal to the amount awarded to plaintiffs); LANDES & POSNER, *supra* note 32, at 58 (describing how almost 2/3 of every dollar awarded is paid in administrative expenses).

tion is that firms are homogeneous in their likelihood of causing harm. However, this becomes inefficient because it enables high risk firms (those that are more likely to cause harm) to under-invest in care and forces low risk firms (those that are less likely to cause harm) to invest more than they should.[129]

It can be shown that when firms do not suffer the full cost of their harm, they will under-invest in care. That is, the level of care that best satisfies the firm will always be lower than the best social level. These results can be confirmed by observing the firm's loss equations, reproduced in Table 1 for convenience. Notice how the firm's losses are always less than society's.

Table 1: Basic loss equations

Policy Intervention	None	Regulation	Liability	Disclosure
Social loss	$c(x) + p(x)[i + h]$	$c(s) + p(s)[i + h]$	$c(x) + p(x)[i + h]$	$c(x) + p(x)[i + h(e)]$
Firm loss	$c(x) + p(x)\, i$	$c(s) + p(s)\, i$	$c(x) + p(x)[i + \alpha h]$	$c(x) + p(x)[i + \lambda h(e)]$
Consumer loss	$p(x)\, h$	$p(s)\, h$	$p(x)[1 - \alpha]\, h$	$p(x)[1 - \lambda]\, h(e)$

By examining the cost functions presented, inefficiencies are not simply a casual outcome of one of these approaches, but are *systematic to all* of them. In short, only in rare and extreme cases will any of these policy approaches be able to achieve the socially optimal outcome. Further, we see that for the same level of care, social loss is equivalent under the basic model (equation 3) and that of ex post liability (equation 9). Social loss for information disclosure (equation 12) will be lower for any e where $h(e) < h$ which would certainly be the case for $h(e^*)$ and implies that disclosure is much less effective if consumers do nothing to prevent possible harm. Finally, it is not immediately clear whether total costs from regulation (equation 6) would be higher or lower than other approaches, only that it is constant for any change in care, x.[130]

129. This raises the question of which characteristics of an organization (government agency, school, private company, etc.) would cause them to be lower or higher risk. A recent data breach study revealed that companies with between 11–100 and 1001–10,000 employees suffered the greatest percent of breaches (26% and 27% respectively) while companies sized between 101–1000 and 10,001–100,000 were breached 17% and 18%, respectively. Also, more than sixty percent of breached firms were from the retail (31%) or financial services (30%) industries. However, financial services firms suffered 93% of all records lost. *See* VERIZON BUSINESS, 2009 DATA BREACH INVESTIGATIONS REPORT 6-7 (2009) (sampling almost 600 breaches over the years 2004–2008).

130. To be clear, however, simply examining social costs across approaches *for the same level of care* is not sufficient. A proper analysis would require comparing social costs for each approach *given the firm's optimal level care.*

This Section presented a general discussion of economic models of ex ante safety regulation, ex post liability, and information disclosure. Regulation is efficient only for a single set of firms causing the average amount of harm; liability is efficient only when suits are always initiated and firms always pay for their harm; and information disclosure is efficient when firms bear all of the consumer harm and will reduce total social loss when consumers take action to reduce their harm. Next, we provide a more practical analysis of these approaches in a more specific context and identify how incentives, and therefore levels of care, would change.

B. INEFFICIENCIES IN CONSUMER DATA PROTECTION APPROACHES

This Section refines the previous economic analysis by discussing practical limitations of each of these legal interventions within the context of data breaches and consumer data protection.

1. Ex Ante Safety Regulation

Some scholars claim that regulation focuses on inputs rather than outputs—on prevention controls, rather than actual damage. That is, it enforces minimum standards of safety rather than penalizing injurers for the harms. The trouble is that there may be little correlation between a mandated standard and a decrease in harmful activity.[131] Thus, regulation raises costs to firms while failing to solve the problem.[132] Robert Smith echoes this conclusion:

> First, standards may bear no relationship to hazards in a particular operation, yet compliance (at whatever cost) is mandatory. Second, by requiring a certain set of safety inputs rather than by penalizing an unwanted outcome, such as injuries, the standards approach does not encourage firms to seek other, perhaps cheaper, ways of reducing injuries. Third, the promulgated standards are so numerous . . . and workplaces so diverse, that one must question how comprehensive or knowledgeable inspections can be.[133]

The implication, in the context of data breaches and personal data protection, is that regulations that require specific technologies such as data encryption may be misguided. One commentator argued that such efforts would create a "security floor" that may meet current needs but would soon

131. Cento Veljanovski, *The Economics of Law* 151 (Inst. of Econ. Affairs, Hobart Paper No. 157, 2006), *available at* http://ssrn.com/abstract=935952.

132. *Id.*

133. Robert S. Smith, *The Feasibility of an "Injury Tax" Approach to Occupational Safety*, 38 LAW & CONTEMP. PROBS. 730, 730 (1974).

be insufficient.[134] Moreover, data encryption, while possibly useful at preventing unauthorized access, would not affect the probability of a successful cyber-attack.[135]

In regards to PCI DSS, some claim that the fines may be driving "fine avoidance"[136] rather than improved security and that firms are "tick[ing] boxes without having any idea what they have answered"[137] in an attempt to avoid imposed fines due to non-compliance.[138] These comments reinforce the point that firms may only be driven to avoid legal or contractual penalties rather than improving the firm's security posture. The PCI DSS standards may also be creating a false sense of security. By abiding by a series of guidelines or commandments, firms cease to be proactive in protecting against future computer attacks, privacy violations and data breaches.[139]

However, ex ante safety regulation may be appropriate in some conditions. For instance, Kolstad et al. note that if the probability of a firm being held liable for damages is low enough (approaching zero), then ex ante safety regulation may provide one of the only remedies.[140] They explain that this might occur when there is a great deal of uncertainty associated with the harm, such as when the harm is "so new that those it affects and the consequences of the harm are unclear but suspected of being catastrophic", or when the level of accident costs borne is "so small that he or she might not even recognize it, even though many individuals are affected."[141] In a sense, this perfectly describes the duality of privacy harms (including identity theft) caused by data breaches. We have seen the great difficulty that consumers face when bringing negligence claims against firms for data breaches, in part

134. Posting of Ben Worthen to The Wall Street Journal: Business Technology, *Congress Moves on Data Security*, http://blogs.wsj.com/digits/2007/10/11/congress-moves-on-data-security (Oct. 11, 2007).

135. Encryption of stored data can be very useful at preventing unauthorized disclosure of confidential data, but does not, in and of itself, prevent the theft or acquisition of such data.

136. Evan Schuman, *PCI Fines: Nuisance Or A Ticket To ROI?*, STOREFRONT BACKTALK, Nov. 30, 2008, http://www.storefrontbacktalk.com/uncategorized/pci-fines-nuisance-or-a-ticket-to-roi/.

137. John Leyden, *Regulatory Compliance "Irrelevant" to Security: PCI DSS Credit Card 12 Commandments Standard Flawed*, THE REGISTER, Apr. 15, 2008, http://www.theregister.co.uk/2008/04/15/pci_dss_compliance/.

138. *Id.*

139. *Id.*

140. Kolstad et al., *supra* note 33, at 900.

141. *Id.*

because of the uncertainty regarding the prevalence and magnitude of harm.[142]

Finally, a very pragmatic justification for safety regulation is that monitoring a firm's security controls ex ante can be much easier than measuring harms ex post.[143] That is, it may be much easier for the social planner to monitor a firm's compliance with a standard than it is to quantify all possible costs from an accident. So while ex ante regulation may be an imperfect measure (predictor) of ex post harm, it can be preferable when determining ex post harm becomes more uncertain—which is often the case with data breaches and resulting identity theft.

2. Ex Post Liability

Legal scholars have argued that common law, and in particular, tort law, is a socially efficient means of reducing loss to injured parties.[144] Bagby argues that common law is "self-correcting" and that efficiency is achieved when bad rulings are appealed and overturned, creating new precedent, while efficiency is strengthened when good rulings that dissuade litigation are made.[145]

However, a challenge faced by the application of tort liability to data breaches and consumer data protection is the dichotomy between the economic and the legal interpretation of privacy costs. While tort law often ignores losses that are not actual or immediately realized, economic considerations of privacy costs are more promiscuous. From an economic perspective, the costs of privacy invasions can be numerous and diverse. The costs and benefits associated with information protection (and disclosure) are both tangible and intangible, as well as direct and indirect.[146] Direct costs are those

142. This is not to say that identity theft is not real or potentially devastating for some individuals. We merely highlight that specific harms *due to breaches* are, for the most part, difficult to quantify.

143. *See* Donald Wittman, *Prior Regulation versus Post Liability: The Choice between Input and Output Monitoring*, 6 J. OF LEGAL STUD. 208 (1977).

144. *See generally* LANDES & POSNER, *supra* note 32; Mark Geistfeld, *Efficiency, Fairness, and the Economic Analysis of Tort Law*, *in* THEORETICAL FOUNDATIONS OF LAW AND ECONOMICS 234 (Mark D. White ed., 2009) (discussing arguments supporting and refuting the justification for an "efficiency" approach to tort law).

145. JOHN W. BAGBY, COMMON LAW DEVELOPMENT OF THE CUSTODIAL DUTY OF INFORMATION SECURITY IN FINANCIAL PRIVACY RIGHTS 6, 8 (2007), *available at* http://faculty.ist.psu.edu/bagby/Pubs/CommonLawEfficiency-CustodyDutyInfoSecurity1.pdf.

146. *See generally* Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (Mar. 2002), *available at* http://epic.org/reports/dmfprivacy.pdf. However, some observers only focus on the presence, or lack of evidence, of monetary costs. P. H. RUBIN & T. M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 45-46 (2001).

immediately realized, such as adverse price discrimination following the revelation of a consumer's personal taste and preferences.[147] Indirect costs are the potential harms from identity theft once personal data has been compromised. Both direct and indirect costs can be tangible and intangible: for example, the tangible monetary loss due to price discrimination and the intangible shame associated with having portions of one's life exposed to the public.

Most often, when personal data is compromised, different types of costs are combined together. For instance, the costs associated with identity theft include direct dollar losses as a result of the crime, and indirect losses associated with investigation, recovery and coping with the ramifications. Examples of indirect losses include: lost wages, lawyers' fees, higher interest rates, anxiety and inconvenience of being denied utility service, time expenditures and psychological stress of dealing with debt collectors, and the distraction of being subject to civil lawsuit or criminal investigation.[148]

To complicate things, costs associated with privacy invasions are often speculative and uncertain (they are probabilistic). After a data breach, a consumer's personal information *may* fall into the wrong hands and *may* then be used in manners that harm that consumer. For an economist, the difference between an actual and a possible cost is simply a matter of probability and uncertainty; in both cases, the breach of a consumer's data has heightened the *expected* costs—be they tangible or intangible—that he will suffer when and if his data is abused. Such ambiguity is, most of the time, unacceptable to the law.[149] As previously discussed, a plaintiff bringing a negligence action against a firm for a data breach is unlikely to recover damages for *future* or *potential* identity theft, which *may* have originated from the disclosure of their personal data. Furthermore, for a plaintiff, it is difficult to prove that the harm originated from a *particular* instance of data breach: the victim may not be even aware that his data was in the possession of a certain firm, may not know that his data has been breached, and may not be able to connect the harm born to the actual breach—since his data may have been available at the same time to many other merchants or third parties. Even worse, since the harm may take place long after the breach episode, the victim may have no practical way of recovering losses from the breached firm. These costs

147. Acquisti & Varian, *supra* note 12.

148. Katrina Baum, *Identity Theft, 2004*, *in* BUREAU OF JUSTICE STATISTICS BULLETIN (2006), *available at* http://www.ojp.usdoj.gov/bjs/abstract/it04.htm.

149. *See generally* Robinson, *supra* note 8 (regarding the difficulties of claiming damages for probabilistic harm); Wright, *supra* note 8 (discussing arguments by legal and economic scholars related to causation for probabilistic harm).

create challenges to the application of liability solution in the case of data breaches and data protection.[150]

3. Information Disclosure

As mentioned, information disclosure allows potential victims to take action to prevent harm. Data breach disclosure laws, for example, enable consumers to notify banks and credit agencies to help prevent the risk of identity theft. Moreover, they can provide valuable information to consumers and the marketplace about a firm's security posture. However, such mechanisms rely on the rationality of consumer behavior; specifically, that consumers are able to understand their risks and know exactly what actions to take and when, and that they can execute those actions without cost. The reality, however, is that consumers suffer from a number of behavioral biases and face a number of transaction costs that prevent or hinder their ability to reduce or avoid loss.

First of all, in the presence of a breach notification, a consumer may not recognize the proper course of action since it is not always clear what actions he should take. Magat and Viscusi argue that consumers do not always react rationally to information regarding a change in risk.[151] Thus, information must be properly conveyed so that consumers understand how to evaluate and use it.[152] How is it even possible for a consumer to compute the risk of a data breach notification for example? Even (or especially) if a consumer could compute such risks, consider the case where in response to a data breach, he chooses to punish a financial firm for faulty security controls by changing to a competitor. Ostensibly, he is reducing his risk of identity theft. Instead, however, he has now disclosed his personal information to another firm and actually *increased* his risk of future harm. In this case, a seemingly incentive-compatible action has had the opposite effect.

Second, the cost of acting may be too great. For example, transaction costs economics refers to the many forms of costs that can be incurred during a transaction.[153] A transaction can be the familiar exchange of goods or services,[154] a contract negotiation, an interaction with another person, or part

150. Solove, *supra* note 6, at 5.

151. WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION 17 (1992).

152. *Id.*

153. *See generally* Oliver E. Williamson, *Transaction-Cost Economics: The Governance of Contractual Relations*, 22 J.L. & ECON. 233 (1979).

154. The transaction costs involved in the exchange of goods are simply those incurred beyond the cost of the good, such as the time involved in traveling to a store, searching for a good, and waiting to pay.

of cognitive decision making.[155] For example, consider an individual who just received a data breach notification. They may incur transaction costs when calling the breached firm to obtain more information or when notifying banks and merchants to cancel transactions. Such costs may be greater than any perceived benefit—effectively (and unfortunately) hampering the intended impact of the legislation.

Third, disclosure laws rely implicitly on firm and consumer rationality: that consumers care and that firms know consumers care. But what happens when consumers aren't fully rational, or when firms do not care? Firms may not care when any negative consequence of ignoring the law is less damaging than the benefits of engaging in (and not disclosing) abusive data practices. More concerning, firms may not care if they notice that the marketplace does not react in a significant manner to abusive practices. Consider the results mentioned above indicating that companies subject to data breaches suffer stock market losses[156] and that their customers claim that they would cease relationships with a firm that suffered a data breach. The same results indicate that the stock-market losses are short-termed, while customers who claim to sever their relationship may not follow up on their threats. In fact, it is possible that the escalating number of data breaches reported in the media may create an effect of psychological *habituation*,[157] desensitizing both consumers and firms to their effects—and therefore minimizing the desired impact of notifications.

Furthermore, research in behavioral economics and behavioral decision making provides ample evidence that consumers are unable to conceive of all possible outcomes and risks of data disclosures.[158] Additionally, consumers have trouble with innate judgment biases, such as bounded rationality, rational ignorance, or hyperbolic discounting.[159] Expecting consumers to punish firms that violate their data, or expecting consumers to act upon the reception of breach notifications assumes a level of knowledge, expertise, alertness, and self-control that they may simply not have. For instance, Romanosky, Telang, and Acquisti consider that the effect of the data breach disclosure laws is a function of both firm and consumer action and they both

155. Such as the cognitive effort required to process available information, consider practical alternatives, and finally select a course of action.

156. Acquisti et al., *supra* note 14.

157. *See generally* Jonathan L. Freedman & Scott C. Fraser, *Compliance without Pressure: The Foot-in-the-Door Technique*, 4 J. PERSONALITY & SOC. PSYCHOL. 195 (1966).

158. *See generally* Colin F. Camerer & George Lowenstein, *Behavioral Economics: Past, Present, Future*, *in* ADVANCES IN BEHAVIORAL ECONOMICS 3 (2003).

159. Acquisti, *supra* note 13, at 3-5.

need to take responsibility to prevent breaches and resulting identity theft.[160] But consumers already have enough to worry about. A process akin to "rational ignorance"[161] may lead the consumer to willingly ignore the notification, or to avoid learning about—or acting on—it. Fewer than 10% of individuals whose data had been stolen by criminals availed themselves of the credit protection and insurance and monitoring tools in the Choicepoint breach.[162] Similarly, an FTC survey found that 44% of identity theft victims ignored breach notification letters.[163]

No doubt, information disclosure also imposes additional costs on firms too. These can include: (1) the financial cost of having to engage legal counsel, notify customers either by mail, phone, or public media; (2) establishing call centers and responding to customer inquiries; (3) providing customers redress such as credit monitoring or other identity theft prevention services; and (4) regulatory fines or other fees (such as to the FTC, SEC, or VISA/MasterCard for PCI DSS violations). We discuss a potential outcome of this in the next Section.

C. DISCUSSION

The previous Sections presented simple economic models for consumer, firm and social cost under the three policy interventions. We then highlighted practical limitations of each approach as they related to consumer data protection and data breaches.

We can now incorporate these limitations into our basic economic models and observe the outcomes. For instance, by considering these characteristics, would we now find that firms and consumers have more incentive to behave in a socially optimal manner? Would these result in lower social costs?

As discussed above, ex ante safety regulation focuses on inputs (specific security-enhancing technologies such as encryption), rather than outputs (the actual harm from data breaches). This implies that the firm's cost of care would remain unchanged, but now the probability of harm would be higher because care no longer perfectly corresponds to lower probability of harm. Equation (3) would then become:

---

160. Romanosky et al., *supra* note 109, at 16.

161. *See generally* Bryan Caplan, *Rational Ignorance vs. Rational Irrationality*, 54 KYKLOS 3 (2001).

162. Jon Brodkin, *Victims of ChoicePoint Data Breach Didn't Take Advantage of Free Offers*, NETWORK WORLD, Apr. 10, 2007, http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html.

163. SYNOVATE, *supra* note 104, at 57.

$$\text{Social loss} = c(s) + \beta\, p(s)\, [i + h] \tag{13}$$

where $\beta\, p(s)$ represents the increase in the probability of harm, $\beta > 1$.

Next, ex post liability demonstrates inefficiencies because: (a) consumers incur direct and indirect costs from privacy invasions; (b) probabilistic harm is generally not compensable under tort law; and (c) plaintiffs filing negligence claims are often unable to demonstrate causality. The probabilistic and causation characteristics of privacy violations have already somewhat been captured in our model by the parameter α from equation (7) so a more accurate loss function would simply attenuate the value of α as α' where $\alpha' < \alpha$ (note that the social loss would remain unchanged):

$$\text{Firm loss} = c(x) + p(x)\, [i + \alpha' h] \tag{14}$$

Finally, information disclosure suffers from inefficiencies because: (a) consumers may not know what action to take in response to information; (b) transaction, direct, and indirect costs impose a barrier to consumer action; and (c) consumers may suffer from cognitive biases which impair their rational judgment of perceived risks. We also observed how disclosure imposes additional costs on firms, as shown below:

$$\text{Consumer loss} = p(x)\, \gamma h(e)\, [1 - \lambda] \tag{15}$$

$$\text{Firm loss} = c(x) + p(x)\, [i + d + \lambda\, \gamma h(e)] \tag{16}$$

$$\text{Social loss} = c(x) + p(x)\, [i + d + \gamma h(e)] \tag{17}$$

Consumer costs and biases could be accounted for by modifying $h(e)$ as $\gamma\, h(e)$, with $\gamma > 1$, while the cost to the firm from notification is reflected in d, with $d > 0$.

We now present the extended loss equations as shown in Table 2.

Table 2: Extended loss equations

Policy Intervention	Regulation	Liability	Disclosure
Social Loss	$c(s) + \beta\, p(s)\, [i + h]$	$c(x) + p(x)\, [i + h]$	$c(x) + p(x)\, [i + d + \gamma\, h(e)]$
Firm Loss	$c(s) + \beta\, p(s)\, i$	$c(x) + p(x)\, [i + \alpha' h]$	$c(x) + p(x)\, [i + d + \lambda\, \gamma\, h(e)]$
Consumer Loss	$\beta\, p(s)\, h$	$p(x)\, [1 - \alpha']\, h$	$p(x)\, [1 - \lambda]\, \gamma\, h(e)$

Could any of these policy interventions achieve a first-best outcome? Posed another way, under which conditions would the firm's loss function approach the social loss? Some scholars have already concluded that ex ante regulation and ex post liability could be used together to achieve better out-

comes than if each were used individually.[164] However, their results apply to very general cases and not to the context of data breaches and consumer harm.

While we have provided examples of ex post liability, evidence suggests that the current state of negligence liability is unable to compensate for consumer harms incurred from data breaches, implying an effective value of α (or α') close to zero. Financial institutions, on the other hand, are able to recover losses stemming from reissuing credit cards. This makes sense because in these situations, the conditions of (at least strict) liability are clear: causality from harm is apparent and the costs are tangible and physical (the payment card). The net result is that total social cost remains constant, but the effect on firm costs is unclear because while the firm is internalizing more costs incurred by financial institutions it is also avoiding more consumer costs.

Regulation, however, suffers from a very different symptom. Firms bear no consumer loss to begin with, and the inefficiency of inputs (investment in security measures) to outputs (reduction in breaches) only exacerbates the problem by requiring a standard of care greater than necessary in order to obtain the same total cost.[165] The net result is that social costs increase with β, the divergence between inputs and outputs. It may become impossible, therefore, for regulation to ever be used on its own to obtain a first-best option, despite its apparent ease of use.

In regard to information disclosure, one might consider the cost of notification to be a kind of tax imposed on the firm due to a breach. Moreover, recall how the socially optimal level of care is achieved when the firm internalizes all consumer loss. Thus, the more consumer loss internalized by the firm, the lower the disclosure "tax" would have to be in order for the firm to behave optimally. Conversely, the lower the consumer loss internalized by the firm, the greater the disclosure tax needs to be.

V. CONCLUSION

This Article analyzes personal data protection efforts in the United States through the lenses of three economic theories: ex ante safety regulation, ex post liability, and information disclosure. We have described evidence of their impacts and analyzed the mechanisms through which they operate using economic modeling. While these models are simplistic by design, they can

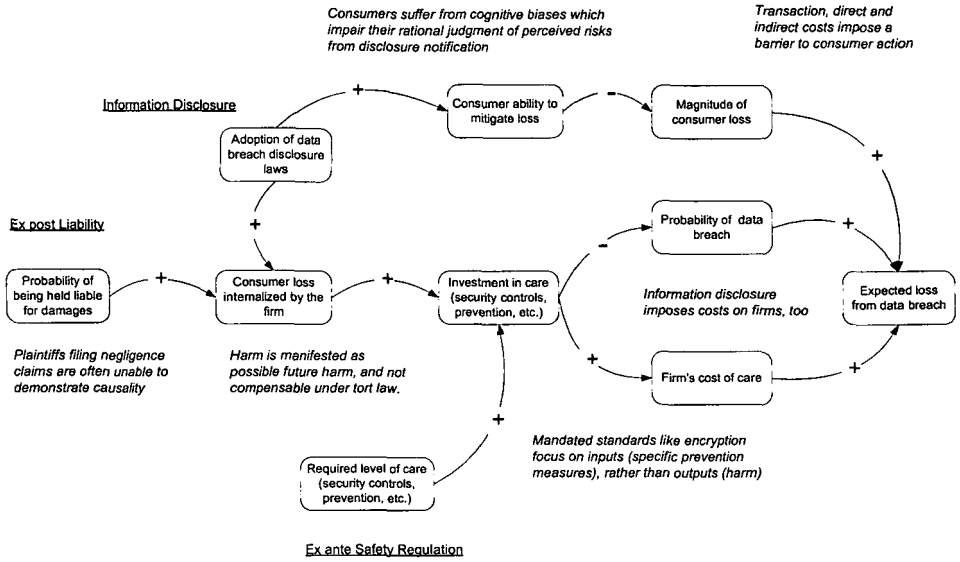
164. *See generally* Shavell, *Model*, *supra* note 33, at 271-80; Kolstad et al., *supra* note 33; Schmitz, *supra* note 33.

165. That is, the standard must be raised such that a probability of a breach offsets the inefficiency.

still be useful to clarify the costs and incentives that drive firm and consumer behaviors. We have also illustrated, both ideally and practically, how these legal mechanisms can suffer from inefficiencies, specifically with respect to data breaches and the protection of consumer data.

The policy mechanisms are illustrated together as we combine Figure 2, Figure 3, and Figure 4, as shown in Figure 8.

Figure 8: Legal mechanisms and their inefficiencies



Each of the policy approaches are underlined, while the inefficiencies are italicized. This figure illustrates the causal relationships between the policy approaches, their intended effects on firm and consumer behavior, and where major assumptions lie.

There are a number of reasons why the policy mechanisms addressed here may not be having a stronger effect. On one hand, they may simply not leverage the proper devices to allow injured parties to avoid or be compensated for loss. On the other hand, they may not be offering the proper incentives for firms and consumers to act either in their own best interests, or that of society. For example, under liability approaches, it becomes difficult for consumers to recover costs. In other cases, it is not clear what the best action is for consumers. What appears to empower them may, in fact, increase their chances of harm.

In conclusion, consider three main categories of costs associated with data breaches discussed in this Article: (1) those incurred by the breached firm itself; (2) those incurred by consumers; and (3) those incurred by financial institutions. Firms will respond naturally to private costs paid as a direct re-

sult of a breach (through investigation, attorney general settlements, and other regulatory sanctions) causing them to increase their care. In regard to costs incurred by banks due to their merchants' breaches, we have shown examples of how self regulation and new state liability laws are holding firms accountable. In this regard, the harm is clear, and so legislative efforts are effective. Alleviating consumer privacy harms, however, is most difficult. The harm is probabilistic and manifested as both direct and indirect, as well as a financial and psychological loss. It can be catastrophic for some, while inconsequential for others. And unfortunately, because reliable information regarding the cause, severity and volume of privacy violations is lacking, contemporary policy approaches appear ill-equipped to adequately prevent or mitigate consumer loss due to data breaches.