Do Data Breach Disclosure Laws Reduce Identity Theft?

Sasha Romanosky, Rahul Telang, Alessandro Acquisti

The Heinz College
Carnegie Mellon University

ABSTRACT

In the United States, identity theft resulted in corporate and consumer losses of $56 billion dollars in 2005, with up to 35 percent of known identity thefts caused by corporate data breaches. Many states have responded by adopting "data breach disclosure laws" that require firms to notify consumers if their personal information has been lost or stolen. While the laws are expected to reduce identity theft, their effect has yet to be empirically measured. We used panel data from the U.S. Federal Trade Commission to estimate the impact of data breach disclosure laws on identity theft from 2002 to 2009. We find that adoption of data breach disclosure laws reduce identity theft caused by data breaches by, on average, 6.1 percent.

Keywords
Data breach disclosure, economics of information security, identity theft, fixed effects regression

Do Data Breach Disclosure Laws Reduce Identity Theft?

INTRODUCTION

Data breaches occur when personally identifiable information such as names, social security numbers, and credit card numbers are accidentally lost or maliciously stolen. These breaches can result in hundreds of thousands (sometimes millions) of compromised records, and lead to identity theft and related crimes (Givens, 2000).[1] In the United States, identity theft resulted in corporate and consumer losses of around $56 billion dollars in 2005 (Javelin Research, 2006).[2] In an effort to reduce these crimes, many states have responded by adopting data breach disclosure (or "security breach notification") laws, requiring firms to notify individuals when their personal information has been compromised. However, to date, no empirical analysis has investigated the effectiveness of such legislative initiatives in reducing identity theft. In this paper, we use panel data gathered from the Federal Trade Commission (FTC) and other sources over eight years to empirically examine this effect.

The Goals Of Data Breach Disclosure Laws

In response to the recent publicity surrounding data breaches, much time and effort have been devoted to preventing breaches and helping consumers avoid, or mitigate, any resulting harm. At least four US congressional hearings have convened to discuss how data breach disclosure laws may reduce identity theft (US Congress, 2005a, 2005b, 2005c, 2005d). In a testimony to the U.S. Senate, the chairman of the FTC testified, "[t]he Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified. Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft" (FTC, 2005, p10). Moreover, the US Government Accountability Office (GAO) has stated that "notification to the individuals affected …has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft" (GAO, 2006). The US Security and

---

[1] Criminals use stolen personal information in many ways. For example, they can incur fraudulent charges on existing accounts, or apply for new utilities (phone, electrical, television, Internet) and financial accounts (such as credit cards, mortgages, and loans).

[2] This value was calculated as the estimated number of identity theft victims in 2005 multiplied by the average amount stolen per victim: 8.9M victims * $6,383 stolen/victim = $56.6B. (Actual amount lost per consumer was $422 on average.)

Exchange Commission has proposed new security and privacy guidelines, including "requirements for notices to individuals […] intended to give investors information that would help them protect themselves against identity theft" (SEC, 2008). Countries other than the United States have also argued in favor of breach disclosures. For example, the UK Science and Technology Committee has claimed that "data security breach notification law would be among the most important advances that the United Kingdom could make in promoting personal internet security" (Science and Technology Committee, 2007).

[Insert Figure 1: Adoption of breach notification laws by state from 2002-2009]

As of December 31, 2009, 45 US states had adopted such data breach disclosure laws (see Figure 1).[3] Many of these laws explicitly addressed identity theft prevention. For example, California's law was intended "to help consumers protect their financial security by requiring that state agencies and businesses […] to quickly disclose to consumers any breach of the security of the system, if the information disclosed could be used to commit identity theft" (SB1386). Further, Senator Simitian (CA), who co-wrote the California's data breach notification law, noted that the purpose of the bill was to "provide assurance that when consumers are at risk because of an unauthorized acquisition of personal information, the consumer will know that he is vulnerable, and will thus be equipped to protect himself physically and/or financially" and moreover, to "provide an incentive to those responsible for public and privacy databases to improve their security" (Simitian, 2009, 1015). The Hawaiian law is even more direct: "[t]he purpose of this Act is to alleviate the growing plague of identity theft by requiring businesses and government agencies that maintain records containing resident individuals' personal information to notify an individual whenever the individual's personal information has been compromised by unauthorized disclosure" (SB2290). Montana's breach law is "an act adopting and revising laws to implement individual privacy and to prevent identity theft" (SB732).

Requirements Under Data Breach Disclosure Laws

While details of the legislations vary across states, their central themes are consistent: the laws require that companies notify individuals when their personal information has been lost or stolen.

[3] For the purpose of this paper, we are not including the District of Columbia, nor city-specific breach laws such as in New York City. We are also not considering federal sectoral legislation such as the Gramm-Leach-Bliley Act (GLBA) as their effects are not identifiable with our econometric model.

Specifically, the laws require notification a) in a timely manner, b) if personally identifiable information has either been lost, or is likely to be acquired, by an unauthorized person, c) and is reasonably considered to compromise an individual's personal information. A breach is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business" (Hutchins, 2007). Personal information generally refers to an individual's name in addition to another piece of identifiable information such as driver's license, passport, or credit card number.

One differentiator among the state laws is the trigger, or threshold, by which notification must be made. Twenty five state laws require notification when the personal information is reasonably assumed to have been acquired by an unauthorized party whereas other state laws require notification only if it is reasonable to believe the information will cause harm to consumers. The consequences of not complying include retribution by the state attorney general or a civil right of action (the ability for affected consumers to bring a lawsuit). Many states do not specify a maximum civil penalty. However, the Arizona and Arkansas laws allow a civil penalty not exceeding $10,000, whereas the limit is $25,000 in Connecticut and Idaho, and $500,000 in Florida.

A characteristic of these laws is that the residency of the consumer, rather than the location of the breach, drives disclosure. Therefore, a firm that incurs a data breach must comply with the state laws of each of their affected consumers. For example, if a retail firm based in Oregon suffers a breach that includes personal information of residents from California, the firm must notify those California residents. Of course, not all breaches affect consumers in every state. Breaches in state government agencies (e.g. DMVs), community colleges, schools and hospitals usually only affect residents of a single state. Even breaches by national firms (e.g. chain stores) may only compromise individuals (often employees) of a single state.

The Debate Over The Impact Of Data Breach Disclosure Laws

The rationales for these laws are contained within two phrases: "*Sunlight as a disinfectant*,"[4] and "*Right to know*." First, notification can "transform [private] information about firm practices into publicly-known information as well as alter practices within the firm" (Schwartz & Janger, 2007). Hence, by highlighting a firm's poor security measures, legislators hope to create an incentive for all

[4] This phrase is originally attributed to Justice Louis Brandeis, 1933, http://www.brandeis.edu/investigate/sunlight/, accessed 11/08/07.

firms (even those that have not been breached) to improve the protection of their data, thereby "disinfecting" themselves of shoddy security practices (Ranger, 2007). This, in turn, is expected to reduce the probability of breaches and resulting harm (including identity theft). In other words, since it has been shown that consumers lose confidence in firms who suffer breaches (Ponemon, 2005), proponents believe that the laws will force firms to internalize more of the cost of a breach through notification letters, customer support call centers, and mitigating actions such as marketing campaigns and free credit monitoring.

Second, this form of light-handed paternalism often represents a preferred approach to legislative enforcement compared with a "command and control" regime (Magat & Viscusi, 1992). Consumers feel that they have the right to be informed when firms use or abuse their information. Having being notified of a breach of their personal information, consumers could then make informed decisions and take appropriate actions to prevent or mitigate the impact of identity theft. For example, to lessen their risks, consumers who have been notified of a breach may alert their bank, their credit card merchant, the FTC, or law enforcement; they may close unused financial accounts; they may place a credit freeze or fraud alert on their credit report.[5] Notifications can also enable law enforcement, researchers, and policy makers to better understand which firms and business sectors are better (or worse) at protecting consumer and employee data. However, it may only be through legislation that firms acquire sufficient incentive to actually improve their practices to reduce the likelihood of future breaches and repair consumer confidence.

Arguments in favor of such disclosure laws are compelling. However, scholars have debated whether a data breach disclosure regime does, in fact, increase social welfare. While it may improve a firm's security practices, and help some consumers mitigate the risk of identity theft, on balance, it may only serve to burden them. First, firms must comply with multiple, disparate, and perhaps conflicting state laws. Next, if the probability of suffering identity theft following a data breach is, in fact, very low, then costs incurred as a result of the laws would be unwarranted: firms would be forced to notify consumers without benefit, and consumers would be needlessly freezing and "thawing" their credit reports (FTC, 2005, p10; GAO, 2007). Cate (2009) posits that "if we think breaches really cause harm, then notices are too little. We're just shifting the burden to somebody

[5] A fraud alert informs potential creditors that a consumer may have been a victim of identity theft. The creditor must then take additional measures to verify the identity of the consumer. A credit freeze prevents a creditor from checking a consumer's credit report, or opening new accounts.

else. If breaches do not cause harm ... then notices are an unnecessary cost." Cate (2005) also argues the consumers may become desensitized if they receive too many notices. Moreover, Lenard and Rubin (2005, 2006) argue that these laws are unnecessary for a number of reasons: because they may impede e-commerce and stifle technological development by discouraging firms to innovate using consumers' personal information (or stop collecting it altogether); because the externality caused by data breaches is not so grave, as most of the cost of identity theft and fraud is already born by the firms (businesses, banks, credit card issuers, merchants);[6] and because firms can instead use self-regulated notifications as a market differentiator, and if notifications are sufficiently valued by the consumer, the market will react accordingly.

In summary, these arguments present a stimulating debate as to whether data breach disclosure laws can reduce identity theft -- an impact that, to our knowledge, no one has attempted to empirically measure. The purpose of this manuscript is to investigate the effectiveness of data breach disclosure laws in reducing identity theft. Because of the compelling controversy surrounding the connection between adoption of these laws and identity theft, we hope to offer a relevant and timely contribution to the policy debate. Using panel data on identity theft gathered from the Federal Trade Commission and other sources from 2002 to 2009, we use state and time fixed effect regression analysis to empirically estimate the impact of data breach disclosure laws on the frequency of identity thefts due to breaches. We find that adoption of these disclosure laws reduce identity thefts, on average, by 6.1 percent.

The next section in this paper provides background literature related to information economics and disclosure policies. The paper then presents the conceptual model behind our empirical approach, and the results of the data analysis. A discussion of the policy implications of our findings completes the manuscript.

RELATED WORK

Our paper draws from the literature on disclosure policies, the literature on information security economics, and the literature in criminology.

[6] As estimated by Javelin Research in 2003 (90.5 percent), 2005 (89.6 percent) and 2006 (93.7 percent)

Information Economics and Disclosure Policies

Many researchers have studied the effects of disclosure on market outcomes. For instance, Jin & Leslie (2003) investigated health information disclosure in the restaurant industry, and found that disclosing the hygiene quality of a restaurant increases health inspection scores and lowers the occurrence of food borne diseases. Moreover, disclosure becomes a credible signal to consumers, who respond by demanding cleaner restaurants. Mathios (2000) examined the effects of mandatory disclosure of food nutrition labels on salad dressing sales in a chain of New York grocery stores. He found that producers of salad dressings with the highest fat content suffer a greater decline in market share once forced to disclose nutrition information, relative to less fatty dressings. These studies provide some evidence of how information disclosure policies can affect firm behavior and improve market outcomes. (A lengthy discussion of many disclosure policies related to healthcare, auto safety, public education and more can be found in Fung et al., 2007.)

A number of studies have examined the financial impacts to firms that disclose a privacy or security breach. Campbell et al. (2003) find a significant and negative effect on the stock price of the breached company, but only for data breaches caused by "unauthorized access of confidential information." Cavusoglu et al. (2004) find that the disclosure of a security breach results in the loss of $2.1 of a firm's market valuation. Telang & Wattal (2007) find that software vendors' stock price suffers when vulnerability information in their products is announced. Acquisti et al. (2006) use an event study to investigate the impact on stock market prices for firms that incur a privacy breach, and find a negative and significant, but short-lived, reduction of 0.6 percent on the day when the breach is disclosed. Ko & Dorantes (2006) study the four financial quarters following a security breach, and find that, while breached firms' overall performance was lower (relative to firms that incurred no breach), their sales increased significantly (again, relative to firms that incurred no breach). Despite absence of more conclusive empirical findings on the effect of publicly disclosed data breaches, firms nevertheless appear to be making security and operational investments in the wake of disclosure laws (Samuelson Law, 2007).

Criminology and Victim Precaution Policies

Estimating the effect of a policy intervention (e.g., a law) on crime is a familiar research question in criminology. To be clear, the policies identified in this manuscript (data breach disclosure laws) are meant to influence safety and protection measures by both firms and potential victims of a crime (identity theft), rather than criminal behavior. While there exists some literature on the direct effect of individual crime prevention (Cook, 1986; Shavell, 1991; Kobayashi, 2005), our work contributes to the more limited body of research that examines the effect of a policy intervention on victims' precaution. For example, Ayers and Levitt (1998) examine the effect of state adoption of lojack (an unobservable vehicle theft recovery device) on auto thefts, and the positive externalities caused by its adoption. Also, Cook and MacDonald (2010) examine the effect of implementing business improvement districts (BIDs: taxing local business owners to provide, among other services, public safety) on local crime reduction. Moreover, for the purpose of this study, we gain valuable methodological insight from the overall approaches of criminology and policy evaluation. For example, criminologists frequently seek to measure the effect of law in deterring crime, generally (Robinson & Darley, 2003, Black & Nagin 1998), in regard to capital punishment (Mocan & Gittings, 2003; Wolfers & Donohue, 2006) and with respect to concealed gun laws (Lott & Mustard 1997; Donohue & Ayres, 2003; Donohue, 2004). The usage of panel data with fixed effects in this literature has led to heated debates about model robustness, since these models' results have often shown to be very sensitive to minor changes in the specification (such as the inclusion or exclusion of given geographic regions or time periods). In our analysis, we tested a number of variations on our basic model specification, and found that our results are robust to said specification changes.

IDENTITY THEFT AND BREACH DISCLOSURES: A CONCEPTUAL MODEL

Impact of Data Breach Disclosure Laws

The primary objective of data breach disclosure laws is to force firms to notify consumers when their personal information has been lost or stolen. The law is also expected to act as "sunlight as a disinfectant." Therefore, we can expect two effects from these laws: increasing consumer precautions, and increasing firm precaution in avoiding breaches.

Consumer precaution should increase, after the passage of the law, because - as more consumers are notified of a breach involving their sensitive information - they may take steps to reduce the risk and the costs of becoming a victim of identity theft. For example, they could notify their financial institutions to block transactions and cancel accounts, or apply credit freezes and fraud alerts. Moreover, such notices also could serve to increase consumer awareness in general, making them alert to possible identity thefts. Therefore, a primary effect of data breach disclosure laws should be the reduction of the incident of identity theft, as well as a mitigation of its impact, via better consumer precaution.

On the other hand, firm investment in security and protection of sensitive data should increase, as firms try to avoid the (larger) tangible and intangible costs associated with notifying consumers after a data breach. The tangible costs include replacement costs of credit cards (through bank negotiations), proving free credit counseling, setting up 1-800 numbers, etc. The intangible costs can be also significant - for instance those associated with negative reputation effects. Acquisti et al. (2007) show that repeated disclosure of data breaches and newspaper headlines could lead to a significant reputation impact and loss in share price. Ponemon (2005) suggests that consumers lose confidence in firms who suffer breaches. Therefore, another effect of the laws would be to induce firms to invest and improve their security controls - in order to avoid a data breach, and avert the direct and indirect costs associated with its notification. In turn, these investments may reduce the number of data breaches, thereby reducing the number of identity theft crimes due to breaches.

In sum, both these effects (consumers taking precautions, and firm investing in better security) should reduce the incidence of identity theft.

In order to qualify the overall effect of data breach disclosure laws, however, it is important to note that identity theft originates from different sources. Disclosure laws would reduce identity thefts for situations where consumer data is controlled by firms, but is not likely to significantly reduce identity thefts due to – say - stolen mail or garbage.[7] In a randomized phone survey conducted by Synovate (FTC, 2007b), 12 percent of identity thefts occurred as a result of interaction with firms, while another 56 percent of victims did not know the cause. In another survey conducted by Javelin Research (2006, p7), 35 percent of identity fraud was a result of information that was within the control of businesses.[8] And in 2007, researchers at the Center for Identity Management and Information Protection (CIMIP) at Utica College studied 517 identity theft cases from the US Secret Service (Gordon et al., 2007). For cases where the source could be determined (about half of the total 517), 26.5 percent originated from firms.

[7] In principle, once a consumer is affected by a breach, he/she can freeze a financial account, and thus reduce the probability of other kinds of identity theft. In practice, however, the joint probability of a given consumer applying an account freeze, *then also* suffering a different form of identity theft during the period while her account is frozen is likely small.

[8] The categories controlled by the firm are: Taken by a corrupt business employee: 15 percent, Some other way: 7 percent, Misuse of data from an in-store/onsite/mail/telephone transaction: 7 percent, Stolen from a company that handles your financial data: 6 percent.

The Impact of Disclosure Laws on Breaches

Naturally, even prior to their impact on identity theft, a first-order effect of the laws should be to reduce the number of breaches. However, we note that the number of reported breaches is endogenously affected by the law as well: only after the laws are passed, firms are forced to disclose, and their breaches enter the statistics. This may create the false impression that breaches increase following the enactment of the laws. In other words, analyzing the number of breaches directly is unlikely to provide useful results. As expected, Figure 2 shows that the number of reported breaches has increased over time.

[Insert Figure 2: Data breaches from 2002-2009]

Identity Theft Data

The most comprehensive public source for identity theft data are the consumer reports published by the FTC since 2002. The Identity Theft Act and Assumption Deterrence Act of 1998 led the FTC to establish the Identity Theft Data Clearinghouse in November 1999 to collect identity theft complaints from victims.[9] Consumer Sentinel is the web portal by which annual identity theft reports are made available to the public, and where law enforcement can further mine the data.

For our analysis, we used consumer reported identity thefts collected from the FTC for each state from the years 2002 to 2009. Note that these reports are generated by individual consumers (only once they discover the theft), rather than as an automated check-and-balance by other agencies such as consumer credit bureaus. Since only annual data are published, we invoked the Freedom of Information Act to request monthly data. In our analysis, we aggregated the monthly data to 6-month periods (2 per year) for the years 2002 to 2009 (producing 800 observations).

One of the advantages of this data source is the consistency of data collection methodologies across states (without which our estimations could be erroneous).[10] On the other hand, the data is self-reported by victims - a familiar issue for criminologists, who often rely on various forms of self-reported crime data (e.g., Uniform Crime Reports and National Crime Victimization Surveys). The frequent under-reporting of crimes is often referred to as the "dark figure" (Biderman & Reiss, 1967)

---

[9] See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=publ318.105, accessed 11/02/09.

[10] For instance, underreporting would be problematic if the reporting patterns changed suddenly over time across states. If the reporting levels change uniformly across all states - which is likely the case with FTC data - these effects would be captured by our time dummies.

and represents a potential source of error. However, not only is the FTC (to our knowledge) the only source for cross-sectional (cross-state) time series identity theft data, but, more importantly, trends in FTC time-series identity theft data are consistent with other surveys by the Bureau of Justice Statistics (Baum, 2006, 2007), Synovate (FTC, 2003, 2007b), and Javelin Research (2006, 2007).

[Insert Table 1: Identity theft reports, 2002-2009]

Summary statistics for total annual reported identity thefts based on the data we obtained through the FOIA request are shown in Table 1. In 2009, for example, California had the highest reported identity theft of over 42,000 (total) while North Dakota had the lowest, at 192. For comparison, relative rates of other reported crimes such as murder, robbery, burglary and motor vehicle theft are shown in Table 2.

[Insert Table 2: Reported offenses per 100,000 population, 2002-2008]

Figure 3 shows total identity theft reports increasing at a decreasing rate from 2002 until 2005, after which they decline slightly in 2006 and increase again until 2009. Prior to 2005, only California had adopted the law, while others followed in 2005 (n=8), 2006 (n=19), 2007 (n=8), 2008 (n=6) and 2009 (n=3).[11] Figure 3 shows the relative changes in reported identity theft rates for three groups: those that adopted in 2005 and 2006 and the 5 states that, as of the end of 2009, had not adopted the law.[12]

[Insert Figure 3: Average identity theft rates from 2002-2009]

Reported identity thefts for states that adopted the law in 2005 seem slightly greater than others, while in states that had not adopted any law (as of December 31, 2009) they seem slightly lower than others. States that adopted in 2007 (and all other groups) fall generally in between other groups. However, we find that states that adopted the laws are not statistically different from those that did not adopt the law (we discuss the issue of potential endogeneity of the laws below).

[Insert Figure 4: Identity theft rates and percent changes before/after law]

---

[11] States that adopted in 2005 were: Arkansas, Delaware, Florida, Georgia, North Dakota, Tennessee, Texas and Washington. States that adopted in 2006 were: Colorado, Connecticut, Idaho, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, and Wisconsin. States that adopted in 2007 were: Arizona, Hawaii, Kansas, Michigan, New Hampshire, Utah, Vermont, Wyoming. States that adopted in 2008 were: Iowa, Maryland, Massachusetts, Oregon, Virginia, and West Virginia. States that adopted in 2009 were: Alaska, Missouri, and South Carolina.

[12] Alabama, Kentucky, Mississippi, New Mexico, and South Dakota.

For comparison, we also include plots of identity theft rates and their changes centered around the year of adoption (Figure 4). The left panel plots the identity theft rates and changes in identity theft rates (right panel) for three groups of states (those that adopted in 2005, 2006 and those that, as of 2009, had not adopted the data breach law). We include only these three groups for clarity and consistency with previous figures (only 2005 and 2006 provides 3 time periods before and adoption. Moreover, plots for states that adopted in 2007-2009 follow no observable pattern and therefore provide no additional insight). The x-axis represents the three time periods before adoption of the law (T-3, T-2 and T-1) and three time periods after adoption of the law (T=0, T+1 and T+2). For example, for states that adopted in 2006, T-1 represents data from 2005, while T=0 represents data from 2006. Data for states without the law have been centered around 2006. T-tests of the difference of means reveal no statistical difference between the means of these groups. The left panel seems to suggest that identity theft rates are increasing before adoption of the laws for all groups but that even for those that adopted in 2006, rates continued to increase. Rates for states that did not adopt show a decline in period T+2, yet are still higher and show a gradual increase from T=0. Moreover, while identity theft rates for states without the law are lower during some periods, rates for all groups increased over time, with states that adopted in early (2005) showing the largest increase before and after.

These trends provide some initial insight into what may (or may not) be driving the changes in identity theft reporting. We scrutinized those changes using a fixed effect regression model, as described in the following sections.

Exogeneity and Adoption of Data Breach Disclosure Laws

A practical concern with all empirical analyses that investigate the effect of a treatment (such as new data breaches legislation) on an outcome (in our case, identity theft) is understanding the motivation behind the passage of law. Specifically, we need to assess whether or not the adoption of state-level laws was itself driven by high levels of identity theft within each state. If the adoption of law was endogenous to the rate of identity theft in a state, the unbiased impact of the law on identity theft would be harder to estimate. In this section, first we present theoretical and empirical evidence that suggest exogeneity, and then we discuss likely drivers of adoption of data breach laws.

Do states with higher rates of identity theft adopt more quickly?

Let us consider three important dates related to a legislative bill: the date it is first filed by a state legislator (either house/assembly or senate representative), the date it is signed by the governor, and the date when it actually becomes effective. In Table 3, we show descriptive statistics regarding the time (in months) between filing and signature, signature and adoption, and the total time between filing and adoption of data breach disclosure laws.

[Insert Table 3: Delay (months) between filing, signature and adoption]

First, notice the wide variation between filing and signature: less than a month for some states, while almost two years for other states. Moreover, one state experienced only two and a half months between filing and adoption, while another state took about 30 months. More specifically, Figure 5 illustrates the adoption durations for all states. The y-axis sorts states from highest to lowest identity theft rates (top to bottom). For example, Arizona, Nevada and Texas, had the highest rates of identity theft, while Iowa, Vermont, and North Dakota had the lowest.

[Insert Figure 5: Months to sign and adopt data breach laws]

To support the claim of endogeneity, we would expect that states with higher rates of identity theft would be quicker at both signing and adopting the bill (identified as diamonds and circles, respectively). That is, we would expect to see data points generally contained within the oval region shown in the figure: data points for states with high rates (at the top of the y-axis) would be positioned very close to the y-axis, while data points for states with low rates of identity theft (near the bottom) would be very far from the y-axis (to the right). Clearly, however, the data are very scattered for states with both high and low rates of identity theft (supported by Table 3). Moreover, adoption of the bill does not appear to occur more quickly for states at the top, relative to states at the bottom.

Furthermore, one might expect that states with higher rates of identity theft would be more likely to sign and adopt the bill. In order to examine this possibility, we performed cox proportional hazard regressions (Jones and Branton, 2005), testing whether the average probabilities of a state filing, or adopting, the law were affected by that state's rate of identity theft as shown in Table 4.

[Insert Table 4: Cox regression]

We ran two alternative specifications of the regression, differing per the dependent variable: the period in which the bills were filed (*hasFiledLaw*) and the period in which the laws were actually adopted in the state legislature (*hasLaw*). The hazard ratio in both columns is very close to one (which indicates that the estimate is economically insignificant) and is also statistically insignificant. Thus, incidences of identity thefts within a state do not seem to drive adoption of the laws.

In sum, we find no systematic correlation between the rates of identity theft and the speed at which a law is passed, nor do we find statistical evidence of high-identity theft states filing or passing laws in earlier years compared with low-identity theft states, or of high-identity theft states being more likely to file or pass the laws. Next, we address the likely reasons for the adoption of the laws.

What are the drivers of data breach laws?

We have just shown that state-specific rates of identity theft do not predict a state's probability of enacting a breach disclosure law. This does not imply that identity theft and data breaches had no role in affecting the passage of the laws. In fact, we believe that the passage of data breach disclosure laws was affected mainly by the "diffusion of innovation" of policy making among American states (Walker 1969), and the rising attention paid nationwide to data breaches and identity thefts.

Walker (1969) noted that inertia and risk aversion are often obstacles to legislators writing new laws (the "innovation"); however, these issues quickly dissipate if the legislator can point to other states that have successfully adopted the law (the "diffusion"). He defined this as the "diffusion of innovation" of policy making among American states. As more and more states adopt the law, Walker claims that, "it may become recognized as a legitimate state responsibility, something which all states ought to have. When this happens it becomes extremely difficult for state decision makers to resist even the weakest kinds of demands…once a program has gained the stamp of legitimacy, it has a momentum of its own" (Walker, 1969, 890). There is evidence that this process took place in the passage of data breach disclosure laws.

California was the first state to enact a disclosure law. The California law was co-introduced in California by representative Joe Simitian. The initial idea for the breach disclosure section of a consumer privacy bill, as Simitian describes, came during the end of a conference call with industry advisors in which he asked, "as a throwaway," if there was anything else to address. The idea for breach disclosure was proposed, discussed briefly, then accepted. As he writes, "in a split second, the decision was made. An eleventh hour afterthought became part of the bill" (Simitian, 2009, 1011).[13] According to Simitian, the California data breach bill did eventually become law only because of "a spelling error, an afterthought, an unrelated concern with digital signatures, a page three news story, rule of germaneness, the intellectual quirks of a lame-duck Senator, the personal experiences of 120 state legislators, and another bill altogether" (Simitian, 2009, 1009). When comparing the ideal legislative process to the reality of the data breach law enactment, Simitian confessed that, "in truth, [the legislative process] is far more random, dramatic, and idiosyncratic than any flow chart could ever describe" (Simitian, 2009, 1009).

Because of the California bill (enacted in July 2003), the September 2004 breach of Choicepoint (one of the largest US data aggregators) became publicly known, causing significant outcry and leading to calls for new federal legislation to protect personal information.[14] Walker (1969)'s "diffusion" process had started. In the case of data breach disclosure laws, it arguably took two forms: 1) As more states started passing disclosure laws, passing the law became "recognized as a legitimate state responsibility," as Walker put it; furthermore, 2) as more states began passing disclosure laws, more data breaches (which before would have otherwise gone undisclosed, and therefore unknown) became publicly disclosed, thereby fueling nationwide media discussion and attracting both citizens' and policymaker's attention, regardless of their state of residency.

Evidence exists for both dynamics. Throughout the 2000s, data breaches involving consumers across all states (such as the above-mentioned Choicepoint (Vijayan, 2008) and TJ Max incidents (Kaplan, 2008)) were publicized in the national media; likewise, tens of millions of estimated identity theft victims (Javelin, 2010), the increasing number of reported data breaches (see Figure 2 in the manuscript) tracked by a host of new organizations (such as datalossdb.org), as well as the increasing research by academic and legal scholars, certainly attracted the attention of legislators

---

[13] As further justification for his motivations of writing and supporting the bill, Representative Simitian stated he wanted a bill that was well defined and very likely to succeed, "when you're a new state legislator, high prospect of passage is very important" (Simitian, 2009b). Simitian further describes how, ironically, a couple of weeks after introducing this bill, there was a data breach in a California data center (Stephen Teale) that contained records of state employees, some of which were state legislators. Suddenly faced with a competing bill introduced by a very senior senator, Steve Peace, the two legislators each agreed to gut and amend their bill and create a new pair of identical bills with each being each other's cosponsor, in effect, doubling their chances of approval. Indeed, the bills were both voted on, accepted and presented to governor Schwarzenegger for signature. (Both bills were ultimately signed and became law.)

[14] See: "ChoicePoint's Error Sparks Talk of ID Theft Law - Privacy advocates call for federal legislation after company's massive data leaks come to light." Grant Gross, IDG News, Feb 23, 2005.

across the country, independently of the actual rates of identity theft in their specific state. For example, Michigan legislators explicitly referred to the nation-wide problem that “identity theft is the fastest-growing crime in America today” in advocating the passage of state level disclosure laws (Michigan Senate Journal, 2005). And the above-mentioned Choicepoint (a Georgia-based company) data breach raised such national concerns that Illinois representative Fritchey, when discussing his own state's data breach bill, declared that it “attempts to deal with what we've come to know as the choice point [sic] issue” (Illinois House transcript, 2005). (The fact that identity theft attracted the attention of legislators is clear from the fact that most of these laws specifically addressed identity theft prevention in their titles, introductions, or elsewhere in the bill.)

This increased awareness and attention paid nationwide to data breaches and identity theft was intertwined with the diffusion/imitation process described by Walker. For example, Michigan legislators argued, “[i]n comparison to other states' efforts, we are beginning to fall woefully behind. I hope we can move on this legislation and preserve and protect consumer privacy and do what is best for the citizens of this great state” (Michigan Senate Journal, 2005). Furthermore, Senator Jungbauer of the Minnesota Commerce Committee emphasized that “similar laws have been enacted in other states and [these data breach disclosure] bills are modeled on California enactments” (Minnesota Commerce Committee, 2006).

As a result, the pattern in which state lawmakers responded to rising concerns with identity theft by enacting data breach laws is compatible with both Walker’s (1969) and Rogers’ (1962) accounts of an S-Curve adoption pattern - as shown in Figure 6 below. California was the lone state with an enacted law in 2003 and 2004; in 2005, a few more states enacted similar laws; and then, between 2006 and 2007, consumer and corporate lobbying resulting from seemingly successful adoption in other states had created sufficient pressure that a vast majority of states passed similar laws almost at the same time.

[Insert Figure 6: Total adoption of breach laws over time]

It should finally be noted that the process through which innovative states (such as California) and imitator states enacted data breach disclosure laws remains nevertheless noisy. Specifically, the exact timing of filing and adoption is quite idiosyncratic and unpredictable – as exemplified by the considerable variance (highlighted above) across states in the delay between when the bills were filed, signed and finally adopted (enacted). This further supports our conclusions that the passage of the laws was not endogenous to state level rates of identity theft. All these examples, as well as our empirical tests, suggest that state-level rates of identity theft did not determine the time of filing or adoption of a data breach disclosure law in a given state.

DATA ANALYSIS

Basic Model

We now specify an econometric model of the impact of the laws' adoption on identity theft. To identify the effect of law, we exploit the panel nature of our data and employ state and time fixed effects. Our simplest model has the following form:

$$\ln(idtheft_{st}) = \beta_0 + \beta_1 hasLaw_{st} + \theta_s + \lambda_t + \varepsilon_{st} \qquad (1)$$

ln(idtheft) is the log of reported identity thefts in each 6-month period in state *s* at time *t* (we consider alternative outcome variable transformations like per capita idtheft later in this manuscript).

$hasLaw_{st}$ is a dummy variable, coded as 1 (one) if the state has adopted the law and zero otherwise. This dummy captures the effect of law on the identity theft rate. The dates of the adoption of data breach notification laws (between January 1, 2002 and December 31, 2009) were obtained from state legislature websites. For the purpose of analysis, we are interested in the date the law became effective rather than the date the law was passed. As described, we code adoption during each 6 month time period for a number of reasons, since this is the smallest time frame by which we expect firms would be able to improve their security practices. Furthermore, by way of legislative procedures, state legislatures generally design the effective date for laws to be either the beginning of the calendar year (January 1st), or the beginning of the fiscal year (July 1st).[15]

θ_s and λ_t are state and time fixed-effects and ε_{st} is the familiar error term. This state, time fixed effect model is widely used in the literature to examine the effect of a policy intervention (Bertrand et al., 2004). State fixed effects allow us to control for unobserved state specific factors and time

[15] Indeed, for our sample 30 of the 45 states adopted the laws either exactly on, or within 1 month after either of these dates. Seven more states had effective dates within two months of a new period, in which case we coded the law has having being adopted in that period. For the remaining 8 states (those that adopted 3 or more months into the period), the law was coded starting the following period. E.g. if adoption occurs more half way through a 6-month period, we set the adoption to occur in the next period. Thus, we estimate what we feel is a more conservative effect of law (that they have less time to be effective). We present results from the alternative specification (coding the adoption by these 8 states as occurring in the current period) later in this manuscript.

dummies allow us to control for time trends. Thus, the unbiased effect of *haslaw* can be identified from variation across state and time.

Basic Model with Demographic Controls and Related Privacy Laws

Additional factors, such as related privacy laws, or demographic factors that change over time and across states, may influence the relationship between the effect of the laws and identity theft. We consider this in Eq. (2):

$$\ln(idtheft_{st}) = \beta_0 + \beta_1 hasLaw_{st} + \sum_i \rho_i\, related_{st} + \sum_j \delta_j economic_{st} + \theta_s + \lambda_t + \varepsilon_{st} \qquad (2)$$

$Related_{st}$ represents credit-related laws that may also affect (prevent) identity thefts. One such legislation is the credit freeze law. These laws enable consumers to apply access control to their credit reports, thereby preventing firms with whom they have no prior agreement to make credit inquiries. If an attacker is trying to open a new account that requires a credit check, they will be stopped and this kind of identity theft will be prevented.[16] The Fair and Accurate Credit Transactions Act (FACTA)[17] is a federal legislation that was passed as a response to identity theft. It allows individuals to request a free annual credit report. This legislation was enacted over the period from December, 2004 to September, 2005 beginning with west coast states and ending with east coast states. A variable was coded as 1 (one) if the law existed in a given state/time and 0 (zero) otherwise.

$Economic_{st}$ is a vector of state-level economic and demographic controls, as are commonly used in crime analysis (Lott & Mustard, 1997; Donohue, 2004; Wolfers & Donohue, 2006), such as the log of population, per capita income, and the average unemployment rate over each 6 month period (16 periods total). State population data were obtained from the US Census bureau. Unemployment rates were collected from US Department of Labor, Bureau of Labor Statistics. Personal income was gathered from the Bureau of Economic Analysis of the US department of commerce. With the exception of population, which is only available annually, all data is available either monthly (identity theft, unemployment rate, adoption of related laws) or quarterly (income). In the case of population, we linearly extrapolated the missing data point as the average of the two adjacent years.

---

[16] Note that it will not prevent victimization if the attacker uses an existing account.

[17] See http://www.ftc.gov/opa/2004/11/facta.shtm, accessed 10/07/07

For example, the first 6-month period in 2008 was computed as the average of the second 6-month period in 2007 and the first 6-month period in 2008.

Extended Model

The basic model in Eq. (1) and Eq. (2) estimates the average effect of law. Next, we extend that model to examine how the laws may have differential effects.

Lagged law. It is conceivable that the effect of the laws increases as firms invest in security measures over time. To test this, we introduce three lagged dummies, *d1PerOld*, *d2PerOld*, and *d3PerOld*, representing 1 (6 months), 2 (one year) and 3 or more (1.5 years+) periods after the law is adopted, respectively.

Interstate effect. While the majority of breaches are, indeed, confined within a state, any diffusion across states may nevertheless reduce the ability to identify an effect of law. We use two measures to control for this. First, we weight identity theft by interstate commerce activity in 2002 as a proxy for how connected a state is with other states. Ideally, we would include this as an explanatory variable in our econometric model, however only cross sectional (not panel) data were available. Second, we interact the *hasLaw* dummy variable with the percentage of all American states that have adopted the law by that time (*hasLaw*PercStatesWLaw*). The *hasLaw* dummy can now be interpreted as the effect of law when no other states have adopted these laws. If the effect is national, then we should find that once a few states adopt the laws, then the marginal impact of law may reduce considerably.

Differential effects. Finally, we consider a number of specifications that reflect how the effect of the law on identity theft may be different across the states. The Bureau of Justice, National Crime Victimization Survey on Identity Theft (Baum, 2007) reported greater levels of identity theft for households in more urban locations and with higher incomes. First, using data on percent urbanization for each state,[18] we set an indicator variable equal to 1 if the state's percent urbanization is greater than the mean of 68.8 percent (the results we present below do not change using the median urbanization). We then interacted urbanization with the state's adoption of the law (*hasLaw*Urban*). Second, we created an indicator variable for high income, setting it equal to 1 if the state's income is greater than the median income from 2009 ($37,124). States coded as high-

---

[18] See http://allcountries.org/uscensus/37_urban_and_rural_population_and_by.html, accessed 01/10/08.

income in this period remain high-income in all time periods. We interacted this high income dummy variable with the breach law (*hasLaw*HighIncome*). Third, we relaxed the assumption that all breach disclosure laws are homogenous. Specifically, we considered that some laws may be stricter if they exhibit the following properties: are acquisition-based (forcing more disclosure from a lower threshold of breach), cover all entities (businesses, data brokers and government institutions), and allow for a private right of action (i.e. individual or class action law suits). Based on the examination of state laws, we classified 9 states as having stricter laws: California, Hawaii, Maryland, Massachusetts, Minnesota, Rhode Island, Tennessee, Vermont and Virginia, We then interacted strictness with the state's adoption of the law (*hasLaw*Strict*) to compare states with strict and non-strict laws.

Mediating and Observable Variables in the Model

While our conceptual framework identifies mediating variables (for example, individuals who are notified and firm investments) the empirical model focuses on observable variables which ultimately affect the outcome of interest: identity theft. This practice is not unfamiliar. For instance, researchers who study the effects of concealed gun laws recognize mediating effects, but relate the dependent and independent variable through observable control variables (Lott & Mustard, 1997; Black & Nagin, 1998; Cleary & Shapiro, 1999), and those who study capital punishment are often interested in the deterrent effect on murder rates (Dezhbakhsh & Shepherd, 2004). In both cases, the analysis of the treatment effects acknowledges the mediating but unobservable factors, but uses crime as the dependent variable, and the effect of law and other economic and demographic controls as the independent variables. In addition, as previously discussed, there is a crucial relationship between data breach disclosure laws and identity theft that legislators have drawn, and which provides the specific motivation for this analysis.

As discussed above, identity thefts occur for various reasons – only one of them being the result of data breaches. An important consideration for both our conceptual model and empirical estimation, therefore, is whether we are measuring the change in identity theft caused by *all sources*, or change in identity theft caused by data breaches only. In Appendix A, we demonstrate that data aggregation may cause our standard errors to increase, but will *not* lead to a biased estimate.

RESULTS

Basic model

Descriptive summary statistics for the main variables of our model are provided in Table 5.

[Insert Table 5: Descriptive statistics]

Table 6 presents the results of the regression in Eq. (1) (the Basic Model with just time and state fixed effects) in Column 1 and the results of Eq. (2) (the Basic Model augmented with controls for demographics and related laws) in Column 2. The dependent variable in all columns is the log of identity thefts (we provide robustness checks for alternative outcome variable transformations in the next section). All specifications use cluster-corrected standard errors by state and include 16 time dummies, although we do not report those estimates for improved readability.

[Insert Table 6: Effect of law on identity theft, Eq. (1), Eq. (2)]

The variable of interest is *hasLaw*, the effect of data breach disclosure laws. We hypothesized a negative coefficient, indicating that the data breach laws do, indeed, reduce identity thefts. The coefficient of *hasLaw* in Column 1 suggests that adoption of the law reduces identity thefts by 5 percent and is significant at the 10 percent level. However, once we control for basic economic and related variables (Column 2), the results suggest that the law reduces identity theft by 6.1 percent, which is significant at the 1 percent level.

Extended model

The results of the extended model are reported in Columns 3-5 of Table 6. Column 3 shows the effect of the lagged adoption of law, and suggests that there is no significant change after 6 months, whereas 12 months after adoption identity theft decreases by 3.7 percent and is significant at the 1 percent level.

The dependent variable in Column 4 weights the log of identity thefts by the percentage of interstate commerce as an attempt to compensate for consumer reports in one state that could have actually occurred in another state. The coefficient of *hasLaw* in Column 4 confirms our previous results: the adoption of the law reduced the identity theft rate by 4.7 percent, on average (the results remain consistent when we apply the interstate commerce weights directly to the identity theft rates). In regard to the other control for interstate activity, we find a negative (though not statistically significant) result from the interaction of breach laws with the percent of all states that have adopted the laws (*hasLaw*PercStatesWLaw*)

Column 5 tests the marginal effect of more urban states. The coefficient of interest is the interaction between *urban* and *hasLaw*. The results suggests that, indeed, the data breach laws reduce identity theft in more urban states by just over 10 percent, relative to less urban states. We did not find significant interactions, however, between the impact of the law and either its strictness or the indicator variable for higher-income states. While this may suggest that stricter laws do not necessarily reduce identity thefts more than weaker ones, such results should be considered with caution, as smaller sample size of these interactions makes such statistical inferences less reliable.

ROBUSTNESS

Alternative Outcome Variables

Table 7 presents regression results using alternative outcome variable transformations: per capita identity theft (identity theft per 100,000 population) in Columns 1-2 and log of per capita identity theft in Column 3-4.

[Insert Table 7: Robustness checks]

First, note that the coefficients of *hasLaw* in all Columns 1-4 are negative. The estimate in Column 2 is -1.411, and marginally significant at the 10 percent level. Using the overall average identity theft rate (per 6-month period) of 32.8, the estimate suggests that, on average, adoption of data breach disclosure laws reduces the identity theft rate by about 4.3 percent (1.411/32.8), which is comparable to the 6.1 percent obtained in the main result. Column 4 (log of per capita identity theft) supports the estimate of the log-level specification in Table 6, a reduction of 6.1 percent, significant at the 1 percent level. Note that our main specification, log(identity theft), achieved the best fit for the data (i.e. an R^2 of 0.85).

Graphical Robustness Methods

As mentioned, empirical analyses of the effect of laws on crime can be fraught with debate over model specification and sensitivity across observational units (states) or time (as with the debate over concealed gun laws and capital punishment). In order to partially address these concerns, we perform a detailed robustness analysis as described by Dugan (2002) and shown in Figure 7.

[Insert Figure 7: T-statistics for per capita and log identity theft]

The y axis represents the t-statistics from regressing identity theft on the full set of covariates and state and time fixed effects, Eq(2). The left panel refers to per capita identity theft (per 100,000 population) while the right panel refers to log(identity theft). Each box plot represents the distribution of t-statistics as we omit one of each 50 states at a time (50 observations per boxplot). Then, we do this 6 times, first omitting data from 2005, then 2006, 2007, 2008, 2009. The "X" represents the inclusion of a year's data, while the "0" represents the exclusion of that year. For example the left box plot (in both panels) represents the distribution of t- statistics when we omit data from 2005 (0XXXX). The rightmost boxplot (in both panels) includes data from all years (XXXXX). The plots are presented on the same y-axis scale for easier comparison.

First, we notice that the t-statistics for per capita identity theft (left panel) are generally smaller compared with log(identity theft), though the outliers are more pronounced in the left panel. The outliers for most boxplots (in both panels) are those states which have never adopted the law (Alabama, New Mexico, Mississippi and South Dakota). Interestingly, the upper outliers (those which reduce the t-statistics are generally Alabama, New Mexico and Mississippi) while the lower outlier is generally South Dakota.

Generally, this method is most useful for testing whether our average coefficient results are driven by particular states or years. For example if the boxplots for all years except 2009, were tight around -1.0, but then the boxplot for 2009 was much lower (say, -5.0), then this would be cause for concern. However, we see no such extremes in either panel. Overall, this analysis provides further evidence that our results are robust to state and year outliers.

Awareness Bias

A further consideration of disclosure laws is that they may produce a conflicting (opposing) effect by increasing consumer awareness - what we call an *awareness bias.* Since identity theft rates are based on self reported information, the passage of law may increase consumer awareness, causing more people to report incidents. This, in turn, would dampen our estimates. First, as more consumers are notified of breaches, the number of consumers who will check their credit reports and discover instances of identity theft may increase. Second, when more state-level disclosure laws are passed, this fuels an increase in media attention from data breaches and the threat of identity theft. This may cause more victims from all forms of identity theft (not just from data breaches) to report the crime. We address this awareness bias in two ways.

First, and to the extent that awareness bias exists, we believe it would bias our regression estimates to produce a lower bound on the effect of law. Therefore, we expect that the true effect of law is at least as strong in sign and magnitude as found in our analysis. Recall, however, that all regression models revealed a negative coefficient, with most revealing statistically significant results.

Second, we attempted to estimate the effect that the passage of a disclosure law in a given state may have had on consumer awareness of their identity theft. Since one of the effects of the laws was to force firms to disclose their breaches, more media reports appeared, following a state law enactment, publicizing breaches (and the related risk of identity theft). This increased media coverage would have captured the attention of consumers and may have increased their likelihood of checking their credit reports in order to establish whether they had been victim of identity theft. To control for this, we used Google archive to count the presence of phrases "identity theft" and "data breach" in newspaper articles across all states from 2002 to 2009. For each state, we collected data from two newspapers that included either the capital or a major metropolitan area (or both). We then counted of hits for either, and both, search phrases, for each 6-month period from 2002 to 2009, creating a panel dataset. Descriptive statistics for these news reports are also included in Table 5. The news reports steadily increase from 2002 (total count of 1245) until 2006 (maximum of 3186), after which they decline slightly until 2009 (to 2034).We then used the state-level counts of either or both phrases as additional controls in a new set of regressions. We find that even when controlling for this awareness bias, our results hold, as shown - for one exemplary specification - in Column 5 of Table 7.

Alternative Coding of Law Adoption

We previously described how 30 of 45 states adopted the laws either exactly on, or within 1 month of January 1st or July 1st and that for 8 states (those that adopted 3 or more months into the period), the law was coded starting the following period. For instance, if adoption occurred more than half way through a 6-month period, we set the adoption to occur in the next period. One might wonder whether the coding for these 8 states may drive our estimates. Therefore, as a further robustness test, we coded these 8 observations with the law being adopted in the current period. As shown in Column 6 of Table 7, the coefficient of hasLaw is now 0.065 and still highly significant, suggesting that our main result represents a more conservative estimate.

Falsification Check

Another category of crimes catalogued by the FTC is "Fraud" which is collected, managed and reported in a virtually identical method as identity theft. It includes such crimes as fraudulent shop-at-home/catalog sales, prizes/sweepstakes, fraudulent internet auctions and foreign money offers. Considering these types of crimes and given the similarity to identity theft in the way they are tracked, we believe that frauds can provide a simple falsification test: we expect the data breach laws to affect identity theft, but not fraud. Therefore, a regression of the law on fraud (using the same explanatory variables as with Eq. (2)) should reveal no significant effect. Indeed, as shown in Column 7 of Table 7 such regressions produce no statistically significant results.

Sampling Bias

Another potential issue of these FTC data is that of sampling bias: that those reporting the crimes are somehow systematically different from the total population suffering from them. While we only observe a small amount of demographic information regarding the consumer identity theft reports, we can, at least, compare age distribution of those who reported complaints to the FTC (FTC, 2007a) with age distributions from victim survey data (Baum, 2006, 2007) and the FTC (2007b). In both cases, results reveal that the 18-29 year old cohort consistently reports more identity thefts relative to those aged 60 or older, which provides some evidence that those reporting the crimes are similar to the best estimate of the total population of identity theft victims.

DISCUSSION

Our research analyses the impact of data breach disclosure laws on identity theft. We use a standard econometric approach commonly used in literature and have controlled for various limitations in the data. We find that adoption of these laws reduce identity theft due to breaches by a statistically significant amount of 6.1 percent, on average, and are robust to multiple specifications, including transformations of the outcome variable and exclusion of individual states and years. To place the results in context, recall that the average amount stolen from consumers in 2005 was $6,383 (Javelin, 2006) and the mean number of identity theft reports over 2002-2009 was 238,791. Given a mean reduction of 6.1 percent (and 95 percent CI of 10.66 and 1.54), this provides a mean reduction in the cost of identity theft by $93 million (0.061 * $6,383 * 238,791; with a 95 percent confidence interval between $162 million and $23 million).

We do not find any significant relationship regarding the strictness of these laws on identity theft, nor do we find any significant effect of the laws in regions of higher population. While we do not find evidence of the laws gaining strength with time, we do find some evidence that the laws were effective in a short term (6-12 month) period. This could be explained by a temporary heightened awareness by consumers of the notifications, causing them to briefly take more precautions. Perhaps, then, as more notices are sent, and without noticeable signals of the effect of their actions, consumers would become desensitized and ignore further notices.

The lack of otherwise economically stronger findings may be due to a number of factors. One obvious explanation is that the laws are simply not particularly effective at reducing the number of identity theft victims either because of lack of consumer or firm action.

Consumer inaction may likely be a result of behavioral decision biases such as *optimism bias* (consumers perceiving their chances of suffering identity theft to be very low), *rational ignorance* (consumers believing the cost of taking precautions outweighing any benefits they may receive), and *status quo bias* (consumers' own inertia inhibiting them from anticipating the consequences of identity theft and responding) (Loewenstein et al.). Magat and Viscusi (1992) argue that disclosure legislation will only be effective if the human element is considered. They claim that consumers are not always rational decision makers and that notices "must convey information in a form that can be easily processed, and in an accurate and meaningful way that will enable individuals to make informed decisions." For example, there is evidence that very few disclosure letters inform consumers of the data that was actually compromised or provide customer support contact information (Samuelson Law, 2007). In addition, fewer than 10 percent of the 163,000 consumers availed themselves of free credit monitoring services following the Choicepoint breach (Brodkin, 2007) and another study found that 44 percent of identity theft victims ignored breach notification letters (FTC, 2007b). A recent Ponemon survey discovered that 77 percent of respondents claimed to be concerned or very concerned about loss or theft of personal information, but only 47 percent of respondents took advantage of free or subsidized credit monitoring services (Ponemon, 2008).

On the other hand, managers of firms may also believe their probability of suffering a breach is small enough that they may still not fully appreciate (and therefore internalize) the associated penalties. Or, they may estimate the net direct and indirect costs of breaches to be quite small, compared to the investments necessary to significantly decrease the probability of those breaches.

For example, Choicepoint incurred a total of $26 million in fines and fees (Vijayan, 2008) - and they survived, with their assets (consumer personal information) being valuable enough to become a recent acquisition target by Reed Elsevier (the parent company of LexisNexus; see Nakashima et al., 2008). In addition, TJ Max reported costs of $178M for a breach that was disclosed in early 2007 and involved over 47 million customer records. Despite this, they enjoyed a quarterly increase in profits by 47 percent one year later (Kaplan, 2008).

Furthermore, if the vast majority of identity theft does not originate from data breaches (either because the information is simply lost and will never be used maliciously, or because credit card companies reimburse consumers for their loss) then the maximum effectiveness of these laws is inherently limited.

It is also conceivable that limitations in the FTC data may restrict our inferences about the true effect of law. However, reported crime data is commonly used as a proxy for actual crimes in empirical studies. Moreover, effects such as awareness bias common to all states (say, from a nationally syndicated news program or nationally circulated online or printed magazine) would be captured in our regression by time fixed effects. Similarly, unobserved state variables such as race or income which could potentially influence identity theft rates would be captured by state fixed effects.

A broader issue relevant to policy makers is whether there are other means by which this law could (and should) be evaluated. Environmental disclosure laws often measure a deterrent policy by their effectiveness at reducing not just the frequency of incidents, but also the severity of incidents and a firm's compliance with the regulation (Cohen, 2000). Therefore, it is possible that these disclosure laws could help reduce the severity of the crimes (as measured by consumer losses or type of identity theft), or reduce the number of records lost/stolen per breach. Indeed, studies have shown that a victim loses less money the sooner they become aware of fraudulent activity (FTC, 2007b; Javelin Research, 2006). Javelin claims that losses are 21 percent lower when consumers detect identity theft within the first week, and 65 percent lower when consumers detect the crime within a year. Our own analysis (using available breach data from 2002-2007) suggests that adoption of these laws did reduce the number of consumer records lost per breach, by about 800 on average; a change of 34 percent.

CONCLUSION

As information security and privacy concerns rise, we will increasingly see legislation used as a tool for consumer protection, generating policy debates and significant lobbying. In this paper, we investigated the effects on identity theft rates of increasingly popular, though contentious, data breach disclosure laws. Despite many US states having adopted these laws since 2003, we have not seen any empirical work that examines their efficacy. Using panel data from 2002 to 2009, we conducted an empirical analysis to examine whether these laws have reduced the identity theft. We found that the passage of law had reduced the identity theft by about 6.1 percent.

Clearly, it appears that the effectiveness of data breach disclosure laws relies on actions taken by both firms and consumers. Firms can improve their controls; however, once notified, consumers themselves are expected to take responsibility to reduce their own risk of identity theft – something which only a minority appears to be doing. It may be that only with time we will see more firms internalize the costs of breaches (and ensuing identity theft), more consumers respond to the risks, and the victimization rates decline.

Proper research on the effectiveness of data breach disclosure laws is hampered by a relative scarcity data. Hoofnagle argues that the current collection of identity theft records is not sufficient, and that banks and other organizations should be required to release identity theft data to the public for proper research (Hoofnagle, 2007). We certainly agree with this view. To the extent that sampling and awareness biases can be reduced, it will allow researchers to more accurately measure the impact of disclosure laws. Moreover, we believe that the better collection of identity theft victimization, consumer and firm losses, and changes in firm behavior will be valuable information for researchers, policy makers and consumers.

APPENDIX A

We noted in the text that identity thefts occur for various reasons, and an important consideration for both our conceptual model and empirical estimation, therefore, is whether we are measuring the change in identity theft caused by *all sources*, or change in identity theft caused by data breaches only. We show here that data aggregation may cause our standard errors to increase, but will not lead to a biased estimate.

Consider, in fact, a dependent variable (Y = total identity theft) consisting of two elements: identity thefts caused by data disclosure (y_1), and identity thefts caused by other reasons (y_2). If the effect of law (say, x_1) is to reduce only y_1 but not y_2, then the preferred regression is:

$$y_1 = \beta_0 + \beta_1 * x_1 + \varepsilon_1 \qquad \text{(A1)}$$

However, we do not observe y_1, but only $Y = y_1 + y_2$. Hence, the estimated model is:

$$Y = \gamma_0 + \gamma_1 * x_1 + \nu \qquad \text{(A2)}$$

The question is: how significantly biased is γ_1 from β_1? To estimate this, note that from A1 we have:

$$E[y_1 \mid x_1] = \beta_0 + \beta_1 * x_1$$

From A2 we have:

$$E[Y \mid x_1] = E[(y_1 + y_2) \mid x_1]$$

$$= E[y_1 \mid x_1] + E[y_2 \mid x_1]$$

As long as y2 is independent of x1 (which is by construction):

$$= E[y_1 \mid x_1] + E[y_2]$$

This implies:

$$E[Y \mid x_1] = \beta_0 + \beta_1 * x_1 + E[y_2]$$

$$E[Y \mid x_1] = (\beta_0 + E[y_2]) + \beta 1 * x_1 \qquad \text{(A3)}$$

Comparing A3 with A2, notice that $\gamma_0 = (\beta_0 + E[y_2])$ and $\gamma_1 = \beta_1$. Thus, γ_1 represents an unbiased estimate of the effect of law (though it will suffer from higher standard errors). If a covariate is correlated with y_2, then it would indeed be biased. In summary, even though our dependent variable reflects identity thefts due to reasons other than data breaches, we will still achieve unbiased estimates when these crimes are uncorrelated with the effect of law. This implies that the estimates we obtain reflect the effect of law on identity theft due only to breaches, and not identity thefts due to other causes, such as lost or stolen wallets.

Figures

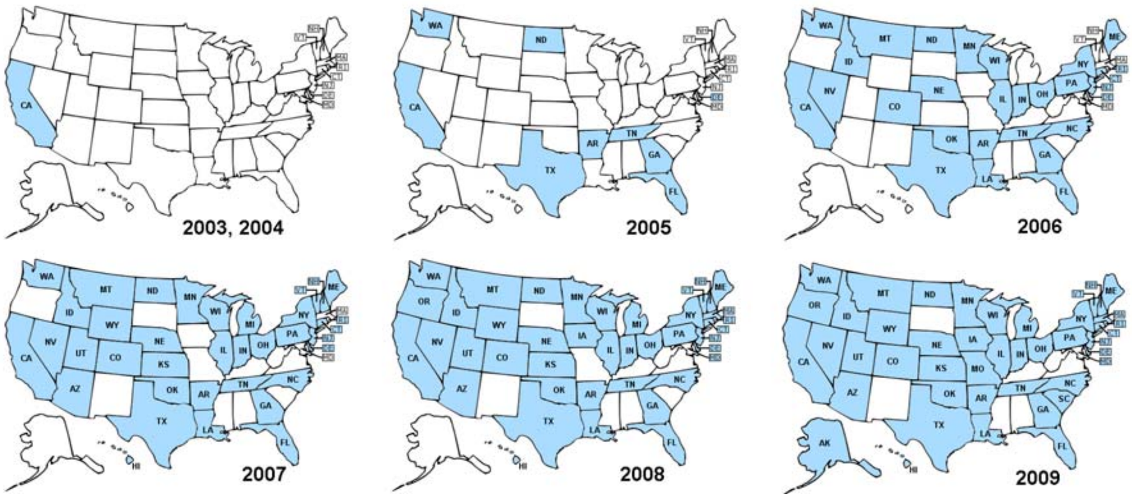

Figure 1: Adoption of breach notification laws by state from 2002-2009

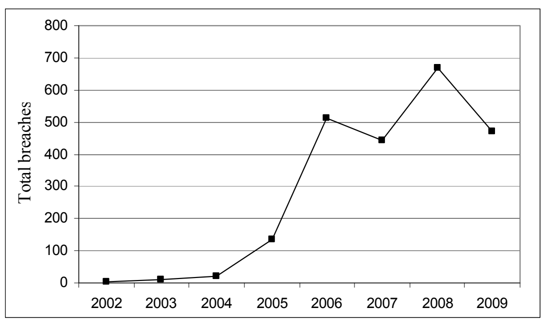

Figure 2: Data breaches from 2002-2009

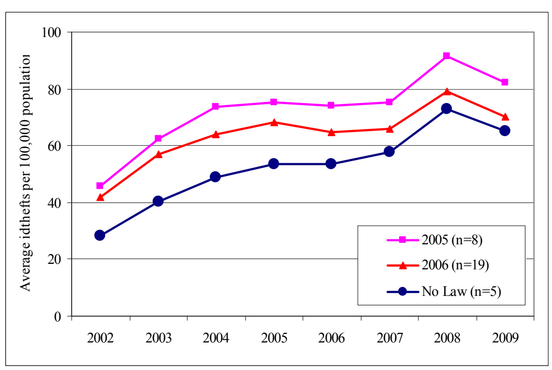

Figure 3: Average identity theft rates from 2002-2009

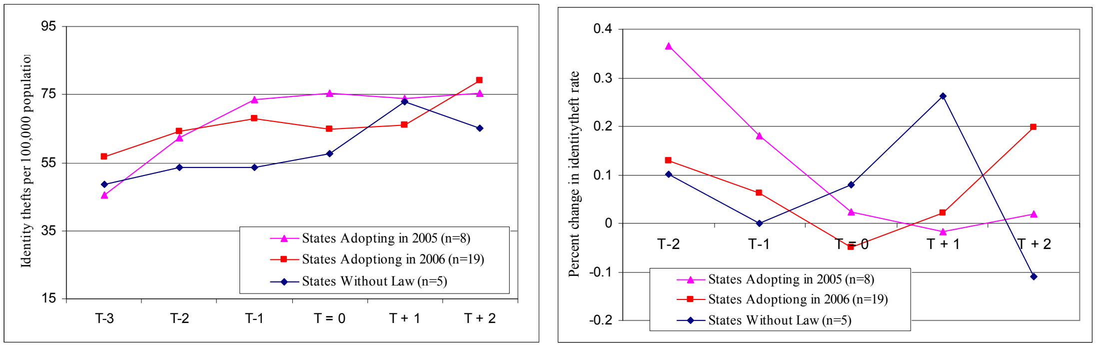

Figure 4: Identity theft rates and percent changes before/after law

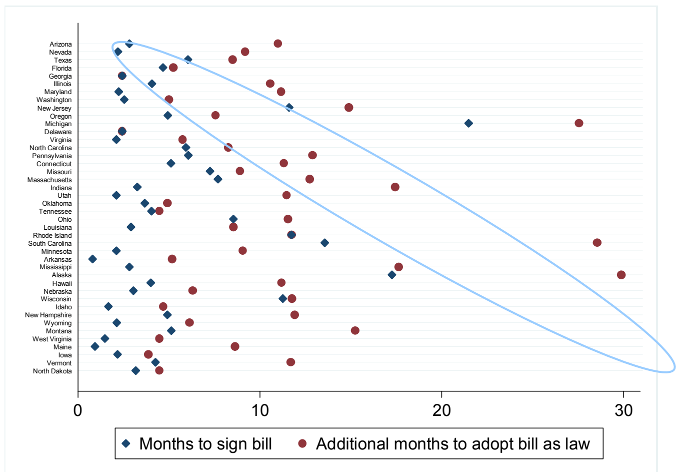

Figure 5: Months to sign and adopt data breach laws

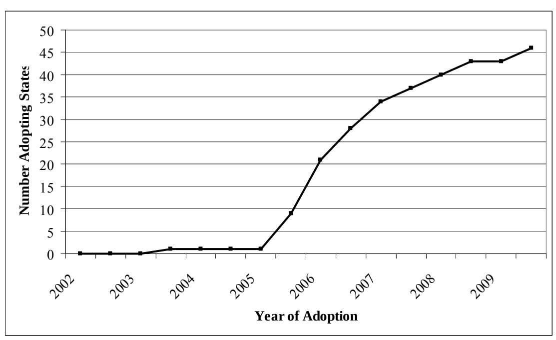

Figure 6: Total adoption of breach laws over time

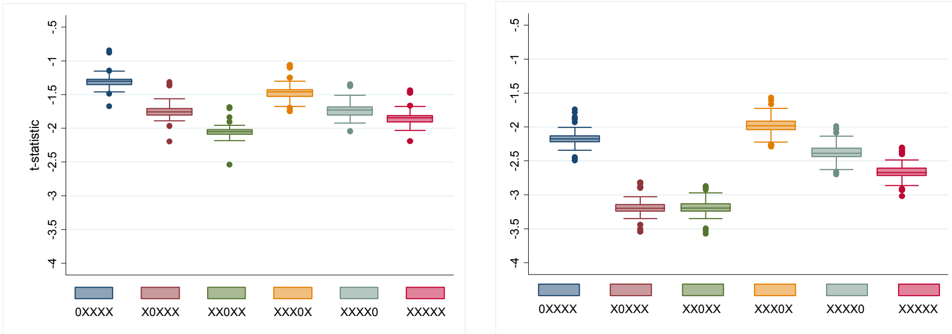

Figure 7: T-statistics for per capita and log identity theft regressions

Tables

Table 1: Identity theft reports, 2002-2009

Year	Total	Average	Stdev	Min	Max	IDtheft rate
2002	154,327	3,087	5,059	81	30,782	53.7
2003	207,116	4,142	6,576	127	39,500	71.5
2004	239,037	4,781	7,520	179	43,900	81.7
2005	247,747	4,955	7,676	158	45,180	83.9
2006	238,627	4,773	7,228	178	41,415	80.1
2007	250,597	5,012	7,662	182	44,020	83.3
2008	300,184	6,004	9,047	227	50,930	98.8
2009	265,876	5,318	7,794	192	42,239	86.8

Table 2: Reported offenses per 100,000 population, 2002-2008

Year	Murder	Robbery	Burglary	MV Theft
2002	5.6	146.1	747.0	432.9
2003	5.7	142.5	741.0	433.7
2004	5.5	136.7	730.3	421.5
2005	5.6	140.8	726.9	416.8
2006	5.7	149.4	729.4	398.4
2007	5.6	147.6	722.5	363.3
2008	5.4	145.3	730.8	314.7

Table 3: Delay (months) between filing, signature and adoption

	Mean	Median	Stdev	Min	Max	n
Filing - Signature	5.3	4.0	4.5	0.8	21.5	41
Signature-Adoption	5.1	4.2	3.8	0.0	15.0	45
Filing- Adoption	10.2	9.1	6.4	2.4	29.9	41

Table 4: Cox regression

	(1)	(2)
Status/dependent variable:	*hasLaw*	*hasFiledLaw*
log(idtheft)	1.01	0.975
	(0.052)	(0.065)
% neighbors with law	0.939	0.944
	(0.054)	(0.078)
Other explanatory variables	Y	Y
Log Likelihood	-137.7	-146.8
Observations	545	477

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 5: Descriptive statistics

Variable (per 6-month period)	**Mean**	**Std. Dev**	**Min**	**Max**
Log(identity theft)	6.97	1.32	3.58	10.18
Identity theft rate (per 100,000)	32.00	13.49	5.67	84.74
Identity theft (total)	2,379.39	3,709.80	36	26,374
Has data breach law	0.38	0.48	0	1
Has FACTA	0.63	0.48	0	1
Has Credit Freeze Law	0.34	0.48	0	1
d1PerOld (6 months old)	0.05	0.22	0	1
d2PerOld (12 months old)	0.05	0.22	0	1
d3PerOld (18 months old)	0.05	0.22	0	1
Per capita income	$35,547	$6,701	$23,019	$66,690
Unemployment rate	5.42	1.73	2.37	14.37
Log(population)	15.11	1.01	13.11	17.43
Newspaper articles	21.48	26.32	0	167
Log (fraud)	7.88	1.14	5.21	11.08

Table 6: Effect of law on identity theft, Eq. (1), Eq. (2)

Dep var: log(idtheft)	(1) Basic	(2) Basic + Controls	(3) Lagged	(4) Interstate	(5) Urban
Has Law	-0.050*	-0.061***		-0.047**	
	(0.026)	(0.023)		(0.019)	
d1PerOld			-0.020		
			(0.015)		
d2PerOld			-0.037***		
			(0.012)		
d3PerOld			-0.023		
			(0.014)		
Has Law * Urban					-0.105***
					(0.027)
Has FACTA		0.035*	0.034*	0.006	0.036*
		(0.019)	(0.018)	(0.011)	(0.019)
Has credit freeze law		0.036	0.020	0.032*	0.039*
		(0.022)	(0.025)	(0.018)	(0.021)
Income per capita		-0.000	-0.000	-0.000	-0.000
		(0.000)	(0.000)	(0.000)	(0.000)
Unemployment rate		0.003	0.002	0.006	0.008
		(0.010)	(0.010)	(0.007)	(0.010)
Log (population)		-0.268	-0.300	-0.532*	-0.092
		(0.343)	(0.353)	(0.278)	(0.276)
State and time fixed effects	Y	Y	Y	Y	Y
Constant	6.852***	11.248**	11.718**	12.612***	8.359*
	(0.014)	(5.317)	(5.490)	(4.327)	(4.327)
Observations	800	800	800	800	800
R-squared	0.848	0.850	0.848	0.808	0.859
Number of states	50	50	50	50	50

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 7: Robustness checks

	(1) Dep var: idtheft rate	(2) Dep var: idtheft rate	(3) Dep var: log(idtheft rate)	(4) Dep var: log(idtheft rate)	(5) Control: Awareness Bias	(6) Alt. Coding of Law Adoption	(7) Falsification, dep var: log(fraud)
Has Law	-0.928	-1.411*	-0.052*	-0.061***	-0.061***	-0.065***	-0.008
	(0.818)	(0.760)	(0.027)	(0.023)	(0.023)	(0.022)	(0.023)
News articles					-0.000		
					(0.000)		
Has FACTA		1.963**		0.035*	0.034*	0.038**	0.008
		(0.767)		(0.019)	(0.019)	(0.019)	(0.024)
Has credit freeze law		1.212		0.036	0.035	0.036	-0.026
		(0.743)		(0.022)	(0.022)	(0.022)	(0.018)
Income per capita		0.000		-0.000	-0.000	-0.000	-0.000
		(0.000)		(0.000)	(0.000)	(0.000)	(0.000)
Unemployment rate		0.106		0.003	0.003	0.003	0.003
		(0.430)		(0.010)	(0.010)	(0.010)	(0.008)
Log (population)		0.208		-1.268***	-0.282	-0.273	1.476***
		(12.728)		(0.343)	(0.341)	(0.343)	(0.351)
State and time fixed effects	Y	Y	Y	Y	Y	Y	Y
Constant	29.06***	20.2	3.28***	22.76***	11.46**	11.331**	-13.40**
	(0.364)	(196.062)	(0.015)	(5.317)	(5.274)	(5.326)	(5.373)
Observations	800	800	800	800	800	800	800
R-squared	0.752	0.756	0.822	0.833	0.851	0.851	0.970
Number of states	50	50	50	50	50	50	50

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

REFERENCES

Acquisti, A., Friedman, A. & Telang, R. (2006, June 26-28). Is There a Cost to Privacy Breaches? An Event Study. Fifth Workshop on the Economics of Information Security.

Ayres, I., & Levitt, S. (1998). Measuring Positive Externalities from Unobservable Victim Precautions: An Empirical Analysis of Lojack. Quarterly Journal of Economics 113 (1: 43-77).

Baum, K. (2006). Identity Theft, 2004. Bureau of Justice Statistics Special Report, NCJ 212213.

Baum, K. (2007). Identity Theft, 2005. Bureau of Justice Statistics Special Report NCJ 219411.

Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How Much Should We Trust Differences-in-Differences Estimates? The Quarterly Journal of Economics, MIT Press,. 119(1), 249-275.

Biderman, A. D. & Reiss, Jr., A. J. (1967). On Exploring the 'Dark Figure' of Crime. Annals of the American Academy of Political and Social Science, Vol. 374, Combating Crime, 1-15.

Black, D. & Nagin, D. (1998). Do Right-to-Carry Laws Deter Violent Crime? The Journal of Legal Studies, 27(1), 209-219.

Brodkin, J. (2007, April 10). Victims of ChoicePoint data breach didn't take advantage of free offers. Network World. Available at http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html. Access date September 12, 2009.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11, 431-448.

Cate, F. (2005, February 27). Another notice isn't answer. USA Today. Available at http://www.usatoday.com/news/opinion/2005-02-27-consumer-protection-oppose_x

.htm. Access date October 15, 2009.

Cate, F. (2009, March 6). Presentation at BCLT/BTLJ 2009 Symposium. University of California Berkeley, Berkeley Center for Law & Technology.

Cavusoglu, H., Mishra, B.& Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1).

Cleary, J. & Shapiro, E. (1999). The Effects of "Shall-Issue" Concealed-Carry Licensing Laws: A Literature Review. Information Brief, Minnesota House of Representatives, Research Department.

Cohen, M. A. (2000). Empirical Research on the Deterrent Effect of Environmental Monitoring and Enforcement. Environmental Law Reporter, 30, 10245-52.

Cook, P. (1986). The Demand and Supply of Criminal Opportunities. Crime and Justice, 7 (1-27).

Cook, P. & MacDonald, J. (2010). Public Safety Through Private Action: An Economic Assessment of Bids, Locks, and Citizen Cooperation. NBER Working Paper 15877.

Dezhbakhsh, H. & Shepherd, J. (2004). The Deterrent Effect of Capital Punishment: Evidence from a 'Judicial Experiment.' American Law and Economics Association Working Paper No. 18.

Donohue, J. & Ayres, I. (2003). Shooting Down the 'More Guns, Less Crime' Hypothesis. Stanford Law Review 51.4.

Donohue, J. (2004). Guns, Crime, and the Impact of State Right-to-Carry Laws. Fordham Law Review 73.

Dugan, L. (2002). Identifying Unit-Dependency and Time- Specificity in Longitudinal Analysis: A Graphical Methodology. Journal of Quantitative Criminology, 18(3):213-237.

Federal Trade Commission. (2003). FTC Identity Theft Survey Report: 2003. Federal Trade Commission and Synnovate.

Federal Trade Commission. (2005, June 16). Data Breaches And Identity Theft. Prepared Statement of the Federal Trade Commission Before The Committee On Commerce, Science, And Transportation, U.S. Senate.

Federal Trade Commission. (2007a). Consumer Fraud and Identity Theft Complaint Data: January-December 2006. Federal Trade Commission.

Federal Trade Commission. (2007b). FTC Identity Theft Survey Report: 2006. Federal Trade Commission and Synnovate.

Fung, A., Graham, M., &Weil, D. (2007). Full Disclosure: The Perils of and Promise of Transparency. Cambridge University Press.

Gordon, G. R., Rebovich, D.J., Choo, K & Gordon, J. B. (2007). Identity Fraud Trends and Patterns: Building a data-based foundation for proactive enforcement. Center for Identity Management and Information Protection (CIMIP), Utica College.

Government Accountability Office. (2006). Testimony Committee on Government Reform, House of Representatives; Preventing and Responding to Improper Disclosures of Personal Information. Statement of David M. Walker, Comptroller General of the United States, GAO-06-833T.

Government Accountability Office. (2007). Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. GAO publication GAO-07-737.

Givens, B. (2000). Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions. Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information.

Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law and Technology, Vol. 21.

Hutchins, J. P. (ed). (2007). Data breach disclosure laws - State by State. American Bar Association.

Illinois House Transcript, 2005 Reg. Sess. No. 38, April 12, 2005.

Javelin Research. (2006). Identity Fraud Survey Report: 2006. Javelin Strategy & Research.

Javelin Research. (2007). Identity Fraud Survey Report: 2007. Javelin Strategy & Research.

Javelin Research. (2010). 2010 Identity Fraud Survey Report: Identity Fraud Continues to Rise – New Accounts Fraud Drives Increase; Consumer Costs at an All Time Low. Javelin Strategy & Research.

Jin, G. Z. & Leslie, P. (2003). The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards. Quarterly Journal of Economics, 118(2), 409-51.

Jones, B. S, & Branton, R. P. (2005). Beyond logit and probit: Cox duration models of single, repeating, and competing events for state policy adoption. State Politics and Policy Quarterly 5(4): 420-443.

Kaplan, D. (2008, February 20). TJX reports soaring profits one year after breach disclosure. SC Magazine. Available at http://www.scmagazineus.com/TJX-reports-soaring-profits-one-year-after-breach-disclosure/article/107072/. Access date October 20, 2009.

Ko, M, & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. Journal of Information Technology Management, 17(2).

Kobayashi, B., (2005). An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods. George Mason University School of Law Working Papers Series.

Lenard, T. M. & Rubin, P. H. (2005). Slow Down on Data Security Legislation. Progress Snapshot 1.9. The Progress & Freedom Foundation.

Lenard, T. M. & Rubin, P. H. (2006). Much Ado about Notification. Regulation, 29(1), 44-50,

Loewenstein, G., John, L. & Volpp, K. (in preparation). Using decision errors to help people help themselves. In E. Shafir (Ed.), The Behavioral Foundations of Policy. Princeton, NY: Princeton University Press.

Lott, Jr., J. R. & Mustard, D. B. (1997). Crime, Deterrence and the Right-to-Carry Concealed Handguns. Journal of Legal Studies, 26(1), 1-68.

Magat, W. A. & Viscusi, W. K. (1992). Informational approaches to regulation. MIT Press.

Mathios, A. (2000). The Impact of Mandatory Disclosure Laws on Product Choices: An Analysis of the Salad Dressing Market. Journal of Law and Economics, 43(2), 651-77.

Michigan Senate Journal, 2005 Reg. Sess. No. 106, November 30, 2005.

Minnesota Commerce Committee 2006 Update, MN S. Comm. Up., 2006 COM, April 03, 2006.

Mocan, H. N. & Gittings, K. (2003). Getting Off Death Row: Commuted Sentences and the Deterrent Effect of Capital Punishment. Journal of Law and Economics, 46(2), 453-78.

Nakashima, E. & O'Harrow, R. Jr. (2008, February 22). LexisNexis Parent Set to Buy ChoicePoint. The Washington Post. Available at http://www.washingtonpost.com/wp-dyn/content/article/2008/02/21/AR2008022100809.html. Access date November 1, 2009.

Neal, T. (2005). Learning the Game: How the Legislative Process Works. National Conference of State Legislatures.

Ponemon Institute. (2005). National Survey on Data Security Breach Notification. The Ponemon institute.

Ponemon Institute. (2008). Consumer's Report Card on Data Breach Notification. ID Experts and The Ponemon Institute.

Ranger, S. (2007, September 3). Data breach laws make companies serious about security. Silicon.com. Available at http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1. Access date September 7,2009.

Robinson, P. H. & Darley, J. M., (2003). The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best. 91 GEO. Law Journal, 949-1002.

Samuelson Law, Technology, & Public Policy Clinic. (2007). Security Breach Notification Laws: Views from Chief Security Officers. University of California-Berkeley School of Law.

Security and Exchange Commission. (2008). Part 248—Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information; Proposed Rule. Available at http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf.

Science and Technology Committee. (2007). Personal Internet Security. House of Lords, Science and Technology Committee, 5th Report of Session 2006–07, HL Paper 165–I.

Schwartz, P. & Janger, E. (2007). Notification of Data Security Breaches. 105 Michigan Law Review 913.

Shavell, S. (1991). Individual Precautions to Prevent Theft: Private versus Socially Optimal Behavior. International Review of Law and Economics, 11 (123-132).

Simitian, J, (2009). How a Bill Becomes a Law, Really. Berkeley Technology Law Journal, 24(3), 1009-1017.

Simitian, J, (March 6, 2009) 13th Annual Symposium: Security Breach Notification, Berkeley Center for Law & Technology, Berkeley Technology Law Journal.

Tarr, G. Alan. (2000). Understanding State Constitutions. Princeton University Press.

Telang, R. & Wattal, S. (2007). An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. IEEE Transactions on Software Engineering paper, 33 (8), 544-57.

U.S. Congress. (2005a). Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs.

U.S. Congress. (2005b). Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services.

U.S. Congress. (2005c). Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary.

U.S. Congress. (2005d). Securing Consumers' Data: Options Following Security Breaches: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce.

Vijayan, J. (2008, January 29). ChoicePoint to pay $10M to settle breach-related lawsuit. Network World. Available at http://www.networkworld.com/news/2008/012908-choicepoint-to-pay-10m-to.html. Access date November 1, 2009.

Walker, J. (1969). The diffusion of innovations among the American states. American Political Science Review 63:880-899.

Wolfers, J. & Donohue, J. J. (2006). Uses and Abuses of Empirical Evidence in the Death Penalty Debate. CEPR Discussion Paper No. 5493.