Legislation and Policy Brief

Volume 1
Issue 2 *Spring 2009 - An Economy in Crisis: What Can Be Done?*

Article 4

9-24-2010

Disincentives to Data Breach: Problems with Notification and Future Legislative Possibilities

Ross Schulman
American University Washington College of Law, rs6484a@student.american.edu

THE LEGISLATION AND POLICY ROUNDTABLE

AN ECONOMY IN CRISIS: WHAT CAN BE DONE?

VOLUME 1, ISSUE 2
SPRING 2009

Disincentives to Data Breach: Problems with Notification and Future Legislative Possibilities

Ross Schulman

Introduction

In the modern digitized and networked world, personal identifying information has quickly become a commodity that can be traded, sold, or given away like any other. The uses and potential abuses of personal identifying information, however, distinguish this commodity from any other. Personal identifying information can be copied infinitely, is often not protected nearly as well as physical commodities, and, most importantly, can have particular importance to the person identified by that information. The producer of a bushel of apples presumably cares very little about where his apples end up, as long as he is paid for them to begin with. The "producer" of a piece of personal information, however, is likely to care very much about where that information ends up and what the various handlers along the way are doing with it.

The information collected, which can be as benign as an address or as important as a Social Security number, is often given willingly as a legitimate part of a business transaction. It is when that information is removed from the original context it was given in that the problem arises. Giving the original producers of information knowledge on how to avoid theft of that personal identifying information is currently accomplished, however, insofar as it is accomplished at all, by a number of different incentive structures. These structures operate on both the companies that keep the data and the consumers whose data is being collected. The incentives include negative consequences upon businesses that allow data to be stolen from them, public information campaigns on avoiding identity theft for consumers, and some state

laws that mandate disclosure of data breaches to those consumers who may be affected.[1] The currently existing incentives can overlap and interact in complicated ways, but ultimately they do not appear to accomplish the desired result: drastically reducing the number of data breaches that impact consumers.[2] To address this concern, some analysts have suggested a move away from indirect incentives and toward affirmative incentives regarding the storage of users' data.[3] This article will examine these incentives, question whether and why they do or do not work, and explore the need for further legislation. In conclusion, this article will offer some ideas for future legislation that modifies the existing incentive structure to better accomplish the goal of consumer protection.

Current State of Privacy Laws

Privacy laws within the United States cover a mix of jurisdictions. On the federal level, no one law covers all areas of information privacy. Laws are instead aimed at individual industries that often deal with sensitive private data, such as the credit reporting agencies,[4] health care providers,[5] and financial institutions.[6] Each of these laws places varying requirements on the controlled entities, and uses differing means of enforcement.

[1] *See, e.g.*, Deter. Detect. Defend. Avoid ID Theft., http://www.ftc.gov/bcp/edu/ microsites/idtheft/ (last visited April 10, 2009) (public campaign by Federal Trade Commission to educate the dangers of identity theft).
[2] *See generally* THE PONEMON INST., 2008 ANNUAL STUDY: COST OF A DATA BREACH (2009) (cost of data breach only going up).
[3] *See* Tom Espiner, *Symantec, RSA Call for Unified Data-Breach Law*, ZDNET.CO.UK, Apr. 9, 2008, http://news.zdnet.co.uk/security/0,1000000189,39382600,00.htm (quoting RSA president Art Coviello as saying that "Congress should pass a law to establish baseline security practices").
[4] *See, e.g.,* Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681-81x (2009).
[5] *See, e.g.,* Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d-2 (2009).
[6] *See, e.g.,* Gramm-Leach-Bliley Act (GLB), 15 U.S.C. §§ 6801-09 (2009).

Companies that do not fall under the auspices of one of those sector-oriented laws are free to operate as they like under federal law.[7] Even if these unregulated companies take in personal identifying information from their customers for other reasons, how they interact with those customers is regulated only by the terms of the parties' service contracts.[8] No public law is applicable.

Having a sector-based system of privacy protection along these lines made some sense in a pre-networked world. It could be argued that each industry uses data in different ways and no one set of practices should govern all of them. But today, nearly every company that does business on the Internet is likely to collect user information, and even most non-Internet based companies keep the information they collect in electronic form. Most of that information is outside the scope of current federal privacy laws.

Individual states have stepped up to address elements of data privacy that they find important and unregulated by the federal government. One example is in the area of data breach avoidance and notification. A data breach notification law has been proposed many times in Congress, but has failed to garner the support necessary to pass both houses. The 110th Congress saw data breach notification bills from Senators Dianne Feinstein, Patrick Leahy, and Daniel Inouye, all of which were reported out of Senate Committees favorably.[9] According to the Congressional Research Service, "[s]everal other data security bills were also introduced."[10] Despite this legislative action, no federal law has been enacted.

---

[7] *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 367-68 (2006) (proposing a privacy regime that would address the current problem with a sectoral privacy system that leaves open large gaps in regulation).

[8] *See, e.g.*, EphemeralLaw, http://ephemerallaw.blogspot.com/ (July 20, 2007, 12:50 EST) (showing the possibilities and problems inherent in basing privacy protections on private contract law).

[9] CONG. RESEARCH SERV., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2009).

[10] *Id.*

States have stepped in to fill this gap. California, the home of many of the country's technology companies, led the way in July of 2003 when SB 1386 became the first operative data breach notification law in the nation.[11] It requires that any company that suffers a breach of unencrypted personal data to notify any affected resident of California about the breach.[12] Since California passed its law, forty-three other states have followed suit.[13] The states vary somewhat in their approaches to the bill, but they mostly follow the model laid out by the California law. Some states provide exemptions for data that was encrypted when it was stolen, or for data that is "immaterial" (i.e., could not lead to an identity theft situation for the victim).[14] Some states also require proactive efforts by companies to prevent data breaches in addition to notifying consumers of breaches after they happen.[15]

Current state legislation, and the possibility of federal legislation, offers an opportunity to explore the incentives surrounding consumer control of data, and corporate responsibility for that data.

The Incentives of Data Breach Notification

Incentives to action created by mandated data breach notification fall into two general categories: those that act upon the companies that collect, store, and sell consumer data; and those that act on the consumers that are giving their data to companies, generally in return for services. The first should encourage, or force, companies that deal with data to protect it as efficiently as possible to avoid breach. The second should operate to inform consumers about

[11] CAL. CIV. CODE § 1798.29 (West 2008).
[12] *Id.*
[13] Posting of Dan Kaplan to SC Magazine Blog, http://newsteam.scmagazineblogs.com/ (Dec. 30, 2008).
[14] *See, e.g.*, MINN. STAT. ANN. § 325E.61 (West 2006) (Minnesota notification statute exempts breaches of encrypted data).
[15] *See*, NEV. REV. STAT. ANN. 597.970 (West 2008) (mandating that any transfer of personal information by a business be encrypted).

corporate practices so that they can place the proper monetary value on their data as they see fit, and then make the best decision between competitors for its protection.

Without a legal mandate, it is clear that companies have no incentive to release information about a breach.[16] Without that information, consumers are unable to make proper decisions about where their information is safest. Fortunately, since the enactment of California's notification law and the subsequent follow-on in other states, the potential interactions between the laws encourages companies subject to breaches to simply notify all the affected customers rather than attempt to parse the individual laws. Unfortunately, notification requirements have not put a stop to breaches in the industry.

Incentive to Avoid Disclosure Without Legal Mandate

Before the California state law went into effect in 2003, there was no legal disclosure requirement for breaches of personal data in the United States.[17] Disclosure was incumbent upon the breached company, but the potential for bad publicity and costly lawsuits provided a healthy *disincentive* to let out any information about the breach.

For example, ChoicePoint, a large-scale data broker that was once a part of the Experian credit-reporting agency and did work as a government contractor had a data breach of some of the personally identifiable information they kept.[18] Because the breach occurred after California's law went into effect, they were forced to disclose the breach to California residents

[16] *See* Kelly Shermach, *How to Respond to a Data Breach, Part 2*, CRM BUYER, Feb. 13, 2007, http://www.crmbuyer.com/story/55710.html (detailing the procedures companies should use to prepare themselves and their public relations strategy for an eventual data breach).
[17] *See* Editorial, *Identity Theives' Secret Weapon*, N.Y. TIMES, April 15, 2005, at A18 ("But for a single innovative law in California, the nation's consumers might not even be hearing some of the more outrageous news about mass heists of supposedly secure computer information from reputedly trustworthy sources").
[18] *See generally* Robert O'Harrow Jr., *ChoicePoint Data Cache Became a Powder Keg*, WASHINGTON POST, Mar. 5, 2005, at A1.

that may have been affected. Those residents alerted the media. From that breach of 145,000 people's information (according to ChoicePoint; California law enforcement estimated the number of affected people as closer to 500,000),[19] ChoicePoint was subject to $15 million in fines by the Federal Trade Commission, in addition to $11.4 million in costs to the company for notifying victims, and legal and professional fees.[20] While ChoicePoint managed to survive the controversy and recover its business, data breach is an expensive possibility that could bankrupt a company. Given the costs incurred by companies that disclose data breaches as required by law, there would be a clear incentive to save the company and stockholders money by refusing to disclose a breach.

Similarly, if there is no incentive to disclose a breach, and therefore no great harm comes to the company because of breaches, there is a lack of incentive to take steps to avoid a breach or the consequences of a breach in the first place. While it may be unlikely that any company will ever be able to completely do away with data breaches, there are a number of steps that they can take to mitigate them. These include encrypting all sensitive data, limiting access to the data, and limiting the forms in which the data can be transported. One example is not placing the data on laptops which can be subsequently lost or stolen, as a number of organizations, including the U.K. Government, have done recently.[21] Avoiding the consequences of breach in advance may be one of the major routes to limiting the impact of future breaches. Yet, most data breach laws in the United States focus on notification rather than prevention.

[19] Sarah D. Scalet, *ChoicePoint Data Breach: The Plot Thickens*, CSO, May 1, 2005, http://www.csoonline.com/article/220341/ChoicePoint_Data_Breach_ The_Plot_Thickens ("California law enforcement says that the number may be closer to 500,000").
[20] Patti Waldmeir, *Company Fined $15m for Failing to Protect Data*, FINANCIAL TIMES, Jan. 27, 2006, at 11.
[21] *See, e.g.*, NATIONAL INST. OF STANDARDS AND TECH., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (DRAFT) (2009), *available at* csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf.

Limited Availability of Information Absent Notification

In order for economic incentives to properly lead the market, every party involved must be aware of the various forces at work in order to make informed choices. If consumers are not made aware of data breaches by some companies, they will be unable to properly evaluate whether to trust those companies with their personal data. Making consumers concerned about their own personal data is a hard enough task; it becomes even harder when consumers do not even have the necessary knowledge to determine what choices are the right ones.

This fact is particularly true given the current level of concern that the public has about the possibilities of identity theft.[22] While most people are now aware of the threat posed by personal data falling into the wrong hands, it does not seem to be the case that people are aware of how to form practical decisions about what services will protect their personal identifying information.[23] Disclosure both informs those consumers that are already worried about data security about a new breach, and raises the profile of breaches to those consumers who are not yet aware of the issue.

Part of this lack of knowledge may be based on yet another level of obfuscation involved in the sale and use of personal information by companies. To use ChoicePoint as an example again, it is unlikely that any affected people knew before the breach that the company was keeping data on them. The company is a data aggregator (a company that collects diverse forms of data on large numbers of individuals and sells the results), and no person whose data they kept likely had direct dealings with them.[24] In order to make the informed decisions that are

[22] *See* PONEMON INST., *supra* note 2 at 16 (2009) (showing increased customer churn rates after a company reports a data breach, and concluding that customers care enough about breach to cut off business relations, but also showing that firms are able to regrow customer bases through marketing).
[23] *See generally* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Processes in the Digital Age*, 10 N.C. J. L. & TECH. 1 (2008) (naming some of the problems inherent in current data collection practices, including the practices of data aggregators).
[24] *See id.*

necessary in the market, consumers may also need to know not just the data practices of the company that they are dealing with, but also those of any companies where their data might end up. Unfortunately, in the current market this knowledge is in most cases completely unavailable to consumers. Obfuscation of the data flows involved, either willful or through the sheer complexity of the data aggregation system, serves to make informing the public a difficult proposition.

Sufficiency of State Based Notification Solution

There are many who argue that the current system, in which forty-four states and three federal territories have individual notification requirements in the case of a data breach, voids the necessity for a federal law with the same requirements.[25] Again, the ChoicePoint breach is illustrative of this claim. At the time, only a very few states, including California, had notification laws. Despite this fact, the ChoicePoint breach was rapidly made public after ChoicePoint was forced to notify California residents of the event.[26] Even if only one affected consumer informs the media of the breach, the damage to the breached company is done.

In today's legal landscape, companies that experience a breach are much more likely to inform every affected consumer; the effort involved in determining which of them live in states that require notification vastly outweighs the meager benefit that might be gained by being selective. The individual state solutions obviate the need for a federal solution that may end up weaker than some states' laws, and may serve to preempt them.

As a consequence of the current lay of the land, David Sohn, from the Center for Democracy and Technology, says impetus for a federal breach notification law in Congress has

[25] *See* Marcia Coyle, *Industry, Government Fret Over Tactics for Fighting Data Theft*, THE NAT'L L. J., Aug. 10, 2006, http://www.law.com/jsp/article.jsp?id=900005550622.
[26] *See* Scalet, *supra* note 19.

died down.[27] Currently, there are no data notification bills that are likely to become laws. But, warns Sohn, another large-scale breach could quickly revive interest, bringing consumer groups to Capitol Hill and forcing business groups to engage in the legislative process in the hopes of reaching a positive compromise. Drifting requirements in state laws could lead to the same result, as businesses forced by conflicting requirements may turn to the federal government to resolve the issue and preempt state law.[28]

Insufficiency of Breach Notification in General

Despite the apparent incentives put in place by breach notification requirements, the fear of the publicity of breach does not seem to be affecting the companies that gather consumer data.[29] Sohn says that while it is still early to make a conclusive determination about the efficacy of breach notification laws, it seems clear that they are still happening through a variety of avoidable means.[30] Many companies have done relatively little to protect the requisite data. The reason may be that large-scale protection of data is still too complicated and expensive to make the costs of a breach overcome the costs of protection.[31] In addition, data breaches and their costs may simply not be on the radar of average companies that gather data as an incident to, rather than the main purpose of, their businesses.

Questioning why the current set of incentives appears not to be working, Sohn wonders whether this can be attributed only to a failure of the existing incentive structure. He inquires as

[27] Interview with David Sohn, Senior Policy Counsel and Dir., Project on Intellectual Prop. and Tech., Ctr. for Democracy & Tech. in Washington, DC (Mar. 12, 2009) [hereinafter Sohn Interview].
[28] *Id.*
[29] *See* PONEMON INST., *supra* note 2(showing that the number of breaches by third party organizations has increased, as has the total costs of data breach by $300,000 from 2007).
[30] Sohn Interview, *supra* note 27 (discussing a number of possible means, including access controls, encryption and physical integrity of data).
[31] *See* PONEMON INST., *supra* note 2, at 15 (detailing measures used to avoid breaches by companies that have already been breached once).

to how much time it should take for the lessons of the current incentives to sink in, and whether the companies should be given more time to learn the processes of protecting data and how to implement those processes effectively.[32]

Regardless, the incentives that attempt to drive behavior by requiring disclosure (that is, indirectly compel behavior) do not appear to be sufficient to encourage most companies to take the steps needed to protect consumers' data before a breach occurs. While notification of breaches is still necessary as a post hoc protection measure for consumers, legislators should be searching out other solutions that will serve to encourage or force (if necessary) companies to properly protect the data they keep.

Legislatures Should Explore Data Security Mandates

In the absence of effective incentives to secure sensitive data, companies will focus on their bottom line, and data security rarely will be seen as the best place to spend capital, especially in tough economic markets. Consequently, the government should step in and arrange more direct and nation-wide requirements that encourage or demand data security on the part of companies that do not adequately protect the information they keep.

A claim that government should step in raises other questions regarding what form the regulation should take and which governments, federal or state, should enact it. Both of these questions will affect the usefulness of the regulation toward implementing the required incentives.

[32] Sohn Interview, *supra* note 27.

Direct Requirements of Security for Sensitive Information Are Necessary

To properly protect the information of millions of consumers in the United States and abroad, any government regulation in this area must induce companies that gather information to protect that information in their dealings with it. There are a number of ways in which companies can make that happen. It may be that the law should not mandate any single one of them, and instead allow innovation to drive a diversity of the most secure methods.

The most obvious solution is to require full encryption of any sensitive information held by the company.[33] This solution protects against the inadvertent loss of data, such as leaving a laptop with sensitive data in a taxi or at an airport. It does not, however, protect against deliberate but unauthorized access to data by insiders who have access to the encryption key, but are using the data for purposes other than for which it was gathered.[34]

Another potential solution is requiring strict access controls on the databases that hold sensitive information by only allowing those with true needs to access the data to do so, and keeping detailed logs on who accessed the data, when, and for what purpose.[35] Alongside this requirement may be a training requirement that assures that employees understood the importance of the data and the repercussions for misuse. These types of requirements would act as the obverse of the above, militating against malicious or negligent access by insiders, but not addressing accidental losses of data.

An alternate approach, advocated by computer security expert Bruce Schneier, is to place liability for breaches directly on the producers of software, and allow them to purchase insurance

[33] *See* PONEMON INST., *supra* note 2, at 26 (advertising for PGP Corporation, a sponsor of the study and a vendor of data and email encryption software).
[34] *See, e.g.*, *Obama Urges Inquiry into Passport Snooping*, CNN, Mar. 21, 2008, http://www.cnn.com/2008/POLITICS/03/21/obama.passport/index.html.
[35] Robin Hattersley Gray, *Data Breach Prevention: 13 Best Practices You Should Implement*, CAMPUS SAFETY MAGAZINE, July/Aug. 2008, http://www.campussafetymagazine.com/Articles/?ArticleID=189 (including "Determine Who Has Access").

to cover the risk.[36] Arguably, insurance companies already know how to evaluate risk, and therefore they are in the best place to mitigate it, and to drive, through the rates they charge, companies toward more secure solutions. This approach could also be adapted to place liability on data collectors.

These possibilities are just examples of the various types of efforts that can be taken to protect user data. One can imagine other methods or technological innovations that might solve the problem in similar or more effective ways. Legislators seeking to craft an effective law should take this into account. While requiring some approach that appropriately protects user data, a potential law could lay out what the result should be—safety of sensitive data—while leaving the details of implementation to the market.

Final approaches may lie with the regulatory state. Actions are already being taken by the Federal Trade Commission (FTC) against companies that did not adequately protect data and had their security breached.[37] Right now, while the FTC can bring actions against these companies, its ability to win civil penalties is hampered by procedural rules that limit FTC court wins to disgorgement of ill-gotten gains, rather than civil penalties.[38] Congress could streamline the system to encourage the FTC to seek monetary penalties of this sort. Sohn suggests that, as a means of encouraging rising standards of protection of data, Congress or the FTC could create a "safe harbor" for companies that abide by industry best practices, which would eliminate the prospect of these monetary penalties.[39] Alternatively, the law could take affirmative steps to examine the practices of companies that store data, in the same way that the Food and Drug

[36] Schneier on Security, http://www.schneier.com/blog/ (Nov. 3, 2004, 15:00 EST).
[37] *See, e.g.,* Press Release, Fed. Trade Comm'n, Consumer Electronics Company Agrees to Settle Data Security Charge; Breach Compromised Data of Hundreds of Consumers (Feb. 5, 2009), *at* http://www.ftc.gov/opa/2009/02/compgeeks.shtm.
[38] 15 U.S.C. § 57b(b) (2009) (limiting the FTC only to equitable remedies, such as disgorgement of improper profits by corporate wrongdoers, which often does not apply in the case of companies that have been the subject of data breach, unless that company operated in collusion with the person stealing the information).
[39] Sohn Interview, *supra* note 27.

Administration examines the facilities of food producers or the way some organizations must provide regulators with privacy analyses.[40]

There are also a few different approaches to mandating actions on the part of the companies involved. The law could mandate certain protections and penalties, and then assess, in the case of a breach, whether the company was complying with the measures at the time of breach. All of the above approaches have benefits and drawbacks that would need to be weighed by the legislature. Absent other considerations, a prudent course of action may be to allow for post hoc penalties and see how those affect the business world, before creating the sort of mandates and administrative action required by a more invasive course.

Any Law Should Be Federal

State based control over notification laws seems to be a workable proposition. The various regulations contemplated here, however, are complex and varied so businesses likely will prefer a federal law for its consistent application. A federal law may also be more appropriate because regulating business nationwide is clearly the province of the federal government.[41] The business community, however, is not eager to have substantive security regulation, either at the state or federal level, and would prefer no new regulation over either state or federal laws.[42]

For the time being, however, business is still fighting the early stages of this fight against passage of security laws in the states. Both Massachusetts and Nevada currently have laws that

[40] *See, e.g.*, Dep't of Homeland Sec., Privacy Impact Assessments, http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.
[41] U.S. CONST., ART. I, SEC. 8 (Congress has the responsibility to regulate interstate commerce).
[42] Sohn Interview, *supra* note 27.

begin to address these issues.[43] Sohn mentions that if business interests continue to lose these fights in the states, they may turn to Congress for relief.[44]

Conclusion

The problem facing both consumers and businesses in the handling of sensitive information is a complex one with real consequences for all involved. Tailoring the economic and legal incentives involved for the purposes of encouraging the necessary protections for that data is of paramount importance. In the past, Congress has been content to allow the individual states to pass breach notification statutes. It is becoming increasingly clear, however, that this approach is not having the desired effect. Further regulation that directly addresses the practices that keep this data secure will be called for, and lawmakers should explore the options laid out here and elsewhere to achieve the most effective incentives to data security. L&PR

[43] *See, e.g.*, MASS. GEN. LAWS ANN. Ch. 93H, § 2 (West 2007).
[44] Sohn Interview, *supra* note 27.