The Case for Strong Data Breach Notification Legislation

Douglas E. Salane
dsalane@jjay.cuny.edu
Center for Cybercrime Studies
John Jay College of Criminal Justice
October 31, 2012

Data Breach Notification Legislation

In 2003, California enacted the first comprehensive data breach notification legislation, the California Security Breach Notification Act (Cal. Civil Code). Prompted at the time by a major breach at a California state agency that compromised the names, addresses and social security numbers of state employees, including legislators, the California Senate modified a proposed data protection law to require notification to California residents when sensitive personal information was breached. Under the original statute, information triggering breach notification included a first and last name along with any of the following items: (a) social security number, (b) driver's license number or California State ID card number, (c) an account, debit or credit card number in combination with any security information that could be used to authorize a transaction, for example, the security code on a credit card. The legislation received almost unanimous support in the legislature.

The California breach law was landmark legislation. It was one of the first attempts to codify sensitive personal information whose unauthorized use could cause harm to consumers. The law recognized that organizations that collect and store sensitive consumer information have an obligation to safeguard that information and inform consumers when it is compromised so they can protect themselves. The law provided the basic structure for similar breach notification legislation, which as of August 2012 is available in 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands (National Conference, 2012)

Many states are in the process of updating existing data breach laws, generally to strengthen and broaden them. For example, California updated its statute in 2008 to include medical records and health insurance information. More recently, it updated its law to include notice to the attorney general. In addition, the new California law requires notifications to include a general description of the incident, the type of information breached and the time of the breach. Connecticut recently updated its law to include notification whenever there is unauthorized acquisition of sensitive personal information (Wong, 2012). State laws are

evolving to address new risks to consumers, and most state legislatures come down strongly on the side of consumer protection when it comes to data breaches.

The Need for Strong, Broad Based Consumer Protections

Data breach notification legislation is a form of broad based consumer protection. Strong consumer protection laws provide incentives for organizations that hold sensitive personal information to put in place secure systems. Data breach notification imposes a penalty for data loss, not only in the cost of notification, but also because the breach cannot remain a secret. For the most part, consumers do not know who holds their data or how the holder will use it. With so many parties holding and sharing sensitive personal data, broad based consumer protections that cut across industries and technologies are needed to ensure organizations secure sensitive personal data.

Notification laws foster at least some level transparency. Privacy Right Clearing House, a non-profit privacy advocacy and education organization, has maintained a list of data breach incidents since 2005 (Privacy Rights). Since then, data breaches have resulted in the loss of 563 million records, and Privacy Rights maintains that the number is probably far larger. Most of the information Privacy Rights obtains comes from reports to state attorney generals, which are mandated by most state laws when the number of breached records exceeds a significant threshold.

Even without breach notification laws, security analysts eventually would learn about most major breaches, e.g., the major breaches in the card payment industry (CardSystems Solutions, 2005; Heartland Payment Systems, 2009; Global Payments, 2012). It would have been quite some time, however, before anyone outside the breached companies learned the magnitude of the breaches or any details surrounding the breaches. Breached organizations usually release as little information as possible, even if the information would advance security at other organizations within their own industry. A recent report by the Federal Reserve banks of Philadelphia and Chicago identified “rapid and detailed information sharing by breached parties across industry sectors “as a key factor in mitigating and limiting the impact of a data breach. Breach notification requirements ensure organizations include consumers in the information sharing and provide incentives to share breach information in a timely fashion.

Consumers and organizations cannot rely on security technologies alone to guarantee information security. Security experts concede that they are losing the security battle at the information technology level (Garfinkle, 2012). Policy and legal experts argue information security requires incentives that are rooted in law and policy (Cate, 2009). For example, many new payment systems, often developed for mobile platforms, are largely unregulated. Although consumers are conditioned to rely on service providers to ensure the security of

payment systems, cost advantages in these new systems might be achieved by avoiding the extensive security infrastructures of established payment systems (Anderson, 2012). Broad based consumer protections are needed to ensure security costs are factored in when such new systems are offered to the public.

With strong consumer protections in place, developers have added incentives to give security high priority from the start. The following comment by a developer at a recent ACM roundtable discussion of mobile system developers (Creeger, 2011) illustrates the point: "Data loss requires notifying each client of the breach and potential access by anyone including a competitor. Loss of a mobile device means data notification requirements are triggered if data security is not provable to some level of technical certainty. Being able to prove that guarantee drove us to ensure that proper screen locks and encryption were in place." No data breach notification legislation mentions mobile phones, but, nonetheless, this legislation is influencing security decisions in the area mobile payment system development.

Data Breach Costs

Data breaches can be expensive, but consumer notification mandated by breach legislation is not the main cost. A Ponemon Institute survey of major corporations across various industry sectors found the average cost per breached record in 2011 was about $194, down from $214 per record in 2010. An earlier survey of chief security officers (CSO) at 14 different organizations pegged the cost at roughly $64 per lost record (Samuelson Law, 2007). In addition, the CSO survey found that notification costs, which include call centers, costs of legal counsel, defense services and victim compensation (reissuing cards or payment discounts), account for about 29% of breach costs. The Poneman study shows that only about 35% of breach costs are due to consumer notification.

Data breaches expose organizations to liabilities for damages. Typically, breach notification legislation does not enable consumers to sue for damages. In several states, however, notification laws do allow individuals to bring a private right of action to recover damages if breach notification was not expeditious (Winn, 2009).

The most significant costs of a breach are often lost customers, damaged reputation and even lowered stock valuations. The extent of these types of losses will depend largely on whether the company can show it acted responsibly in trying to protect consumer data and on how it responds to the breach. Normally company stock valuations recover, especially for companies that take a proactive approach to breach response, as was the case in Heartland breach. Even though there is great incentive to lower the bar for breach reporting to avoid publicizing breaches, lack of transparency in breach response undermines the confidence of both customers and business partners.

Why Attempts at Federal Legislation Fall Short

There have been eight attempts to implement federal data breach legislation that would preempt state laws. The latest is Data Security and Breach Notification Act of 2012, Senate bill S.3333. Although similar to California breach law, many feel the federal versions of breach notification legislation raise the bar that triggers reporting. Basically most .proposed federal laws would require notification only if there is evidence of harm to consumers, which would be determined by the data handler.

Making reporting requirements subject to consumer harm is tricky. Harm is very difficult to predict or monitor as is the extent of losses to consumers as the result of a breach. What level of harm should trigger breach notification? Moreover, letting data holders decide when harm is evident, raises serious concerns. There is little incentive for a data holder to error on the side of notification. Also, different organizations in a given industry are likely to employ different standards. Thus, organizations that elect to put customer protection first might be penalized.

Many who advocate for a uniform national standard for data breach notification cite the complex task businesses face in complying with a "haphazard patchwork" of breach notification laws (Roggenbaum, 2006). As the author notes, however, businesses have taken the conservative approach of complying with the most stringent of requirements across all states, thereby establishing a de facto standard. Also, as already discussed, consumer notification is not the major cost of a data breach.

Establishing uniform national standards is not a simple matter in the federal arena. A uniform standard for reporting must specify triggers for breach disclosure, parties to be notified, timing for notification, the form and type of personal information affected, possible ways notices can be delivered, notice exceptions and penalties for noncompliance. States have been in a better position to determine these factors for their residents than the federal government, which has been unable to produce passable legislation.

The key concern should be obviating the need for reporting by protecting consumer data. The first step is to store sensitive personal information in encrypted form whenever feasible since compromised protected data does not trigger a notification requirement. Too often organizations try to protect data by relying on security of private networks, which now is almost impossible since a boundary between the Internet and a private network can seldom be maintained. The second is to store sensitive consumer data only when required. Finally,

organizations must ensure that third parties with whom consumer data is shared take all appropriate measures to safeguard the data.

Concluding Remarks

Strong data breach notification laws are a form of broad based consumer protection that makes organizations responsible for consumer data, regardless of the industry, service or technology involved. Such protections are needed in a world where the information systems we use are inherently insecure, yet integral to our social and economic well-being. Most importantly, breach notification laws give both consumers and businesses the information they need to factor security into purchase decisions and to mitigate risks when breaches occur.

References

Cate, Fred H., Abrams, Martin E., Bruening, Paula J. and Swindle, Orson. 2009. "Dos and Don'ts of Data Breach and Information Security Policy." *Faculty Publications,* paper *234*. Available at http://www.repository.law.indiana.edu/facpub/234.

Anderson, Ross. March 2012. "Risk and Privacy Implications of Consumer Payment Innovation." Presented at the coference *Consumer Payment Innovation in the Connected Age*, Federal Reserve Bank of Kansas City, Kansas City, Mo. March 29-30, 2012. Available at http://www.kc.frb.org/publicat/pscp/2012/anderson.pdf.

Cal. Civil Code §1798.29, 1798.80-1789.84

Cate, Fred H.2009. "Security, Privacy, and the Role of Law." *IEEE Security and Privacy* 7 (5): 60-63.

Cheney, Julia S., Hunt, Robert M., Jacob, Katy R., Porter, Richard D., Summers Bruce J. October 2012. "The Efficiency and Integrity of the Payment Card Systems: Industry Views on the Risks Posed by Data Breaches," Report of Federal Reserve Bank of Philadelphia and the Federal Reserve Bank of Chicago. Available at www.philadelphia.org/payment-card-center/publications/discussion-papers.

Creeger, Mache 2011. "ACM CTO Roundtable on Mobile Devices in the Enterprise," Communications of the ACM 54 (9): 45-53.

Garfinkle, Simson. 2012. "The Cybersecurity Risk." *Communications of the ACM 5 (6):* 26-32.

National Conference of State Legislatures. August 2012. "State Security Breach Notification Laws." Available at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

Poneman Institute LLC. March, 2012. "2011 Cost of a Data Breach Study." Available at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011

Privacy Rights Clearinghouse. "Chronology of Data Breaches." Available at http://www.privacyrights.org/data-breach/print (accessed Oct. 1, 2012)

Roggenbaum, Frances, R. 2006. "Data Breach Notification Another 'Haphazard Patchwork' of state-by-state requirements." *Journal of the Federal Regulatory Counsel 17 (4).* Available at http://www.forc.org/public/journals/4.

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

Winn, Jane K. 2009. "Are 'Better' Security Breach Notification Laws Possible?" *Berkley Technology Law Journal 24.* Available at http://ssrn.com/abstract=1416222.

Wong, K. June 2012. "Connecticut to Require Notice to Attorney General Following a Breach." *Data Privacy Monitor*. Available at http://www.dataprivacymonitor.com/data-breach-notification-laws/changes-to-connecticuits-data-breach-notification-statute/.