March 29, 2005
TechKnowledge no. 97

When Data Security Regulations Fail, There Is an Alternative

by Jim Harper

Jim Harper (jharper@cato.org) is the director of Information Policy Studies at the Cato Institute in Washington, D.C. (www.cato.org/tech). To subscribe, or see a list of all previous TechKnowledge articles, visit www.cato.org/tech/tk-index.html.

Published on March 29, 2005

If you hadn't heard of ChoicePoint before, you have now. ChoicePoint is a data aggregator-a company that collects information about people, reselling it in different combinations to a variety of clients. Most of the time, data aggregation is a beneficial process. It adds brains to the economy, helping designers, makers, marketers, and sellers of goods and services do a better job for consumers. Data aggregation helps employers, insurers, and lenders make smarter decisions faster.

For good or bad, ChoicePoint has cured the data aggregation industry's obscurity problem. Headline after headline has discussed the fallout since ChoicePoint revealed that it was duped into selling sensitive information about 145,000 people to fraudsters last year. The scammers set up a series of fake businesses to appear like legitimate buyers of financial information. Their purpose was to use it in later identity frauds.

In the wake of the ChoicePoint affair came a deluge of other disclosures. Hoping to obscure their errors in the onrushing press whirl, or having quickly learned the importance of disclosure, a series of companies and institutions revealed similar breaches. Among them were payroll company PayMaxx, Bank of America, LexisNexis' Seisint, several universities, and a shoe retailer called DSW.

It would be wrong to say that the consumer data industry had been without controversy. Its well-known members, the credit bureaus, have been besieged for years by complaints about inaccuracy and unfairness. This despite the Fair Credit Reporting Act, a federal regulatory scheme imposed 30 years ago to address inaccuracy and unfairness in credit reporting. The FCRA was amended in 2003 to address inaccuracy and unfairness in credit reporting. Again.

To the extent they are known, the other data aggregators are poorly understood and mistrusted. They have no consumer face-not even the limited exposure of the credit bureaus. Little is known about what data they collect and how they get it, or to whom they sell it. Several of them, unfortunately, have engaged with the federal government, hoping to provide data mining and surveillance services.

Cued by the new press attention to data security, senators and representatives have stepped in front of earnestly scribbling reporters announcing their plans to make us safe. A variety of bills in the House and Senate would mandate "fair" information practices, require notice of breaches, and force data aggregators to provide consumers with access to personally identifiable information, plus the right to correct it. Many of these are long-dead proposals that have nothing to do with data security. Indeed, some would undermine it even further. But no matter. The American public and media are ready to be buffaloed.

The companies that allowed these data breaches are blameworthy, to be sure. Bank of America moved tapes with financial data about millions of account holders by ordinary air transport. It is surmised that the tapes were lost or that baggage handlers simply stole them.

Of carelessness like this, Sen. Patrick Leahy (D-VT) said, "I don't know what these people are thinking." It's a good rhetorical point. But it may have an equally good answer.

You see, one thing Bank of America may have been thinking about is the federal government's "Safeguards Rule." This is a data security regulation that was mandated by Congress in the 1999 Financial Services Modernization Act, also known as Gramm-Leach-Bliley. Intended to ensure the security of financial data about consumers, the regulation requires financial institutions to:

- designate one or more employees to coordinate data safeguards;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the safeguards for controlling those risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select appropriate service providers and contract with them to implement safeguards; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring safeguards.

Maybe Bank of America was too focused on this federally mandated security paperwork to focus on *actual data security*. In any event, federal data security regulation did not work.

Regardless, politicians' calls for "stronger" regulation are predictable because "stronger" regulation is "better"-in a press conference. In the real world, however, regulation is no more capable of divining threats to data security than, say, a common law liability regime, or even businesses' natural interest in maintaining their operations, integrity, image, brand, and assets.

As noted, data aggregation gives our economy brains. The new regulations being proposed would put a thumb on the carotid artery of information-based businesses, making them a little woozier, a little less aware, and a little less able to serve and protect consumers.

What matters with breaches such as ChoicePoint, Bank of America, and all the rest is whether anyone was harmed. Was a data-rich computer stolen and used for target practice on a backyard shooting range or was its trove of information used in hundreds or thousands of frauds?

Rather than hurried, one-size-fits-all federal regulation, imagine a rule where negligent holders of sensitive data suffer liability for damage caused by breaches. Imagine they have to pay injured parties for the consequences. Ten thousand breaches causing $1000 damage would cost a negligent data holder $10 million, along with adverse publicity and all the rest. Under such a rule, breached companies would race to shore up the damage because further damage would create further liability.

Attractive proposals like mandatory breach notifications might be useful sometimes. Just as often, notification would be a sideshow with no role in preventing consumer harm. Occasionally, notification would tip off computer thieves to the fact that they have also stolen data they could use in identity fraud. This stiff, one-note reaction pales in comparison to the multi-faceted response that would be gotten from putting the responsible party in the financial shoes of victims. Special damages-"civil penalties" and the like-are not appropriate: The objective is proportional response, and such things would detract from that.

Data security regulation is a proven failure. There is an alternative to more of the same. But how do we create this intriguing negligence rule? What has to be done?

Nothing. Just watch and wait. The rule has already been adopted by common law courts in New Hampshire and Michigan.