Adam Shostack
Jan 14, 2008

Richard Simpson
Director General
Industry Canada
Electronic Commerce Branch
300 Slater Street
Ottawa, Ontario K1A 0C8

Dear Director Simpson,

I am writing today in response to your request for public comment on "implementation of the government response to the fourth report of the standing committee on access to information, privacy and ethics on the personal information protection and electronic documents act." Please allow me to introduce myself, offer some comments as a general framework for considering what should be done, and then comment on some of the specifics in Industry Canada's response to recommendations 23, 24 and 25.

I have worked in computer security and privacy for nearly 20 years. Today, I am responsible for security design analysis techniques at a large software manufacturer. I am representing only myself in this letter. I am the co-author of the forthcoming book, *The New School of Information Security*, (Addison Wesley, 2008). I am familiar with the Canadian privacy law, having spent three years in Montreal leading the advanced research team for Zero-Knowledge systems. Over the last few years, I have become convinced that breach notification is a tremendously important opportunity for computer security as a profession.

The most important message as you consider how to implement security breach notification is that breach notices are about far more than identity theft. There are three primary ways in which this is true. The first is that breach notices offer us a window into security failures, from which we can learn. Second, breach notice is about transparency and fairness—the same fairness that underlies the Fair Information Practices on which the OECD guidelines and PIPEDA are based. The third is that breaches often involve deeply personal information that cannot be used for identity theft. The policy treatment of these breaches should be determined by society, not only by commercial interests with a penchant for "sweeping them under the rug." I'll examine each of these in turn.

Breaches offer us a window into security failures.

Today, we have little data about what goes wrong in security. Organizations often believe that their customers will flee, their stock will plummet, or they'll go out of business after a breach. After reviewing over 800 breaches, we know

that these are myths. The Ponemon Institute studies[i] rates of customer "churn," and has found that in almost no case do more than 2-3% of customers leave. Aquisiti, Friedman and Telang[ii] have studied impact of breach notices on stock prices, and in most cases, the stock price impact is at most 2-3% loss for a few days, followed by a recovery. Only two companies have ever gone out of business due to a breach, and those were in unusual circumstances. To the contrary, sales at TJX were up the two quarters after it admitted to one of the largest breaches ever by criminals. Yet these unfounded fears cause organizations to cover up their mistakes.

We in information security have no equivalent of the National Crime Victimization Survey, or the FBI's annual crime statistics. (Please forgive the American examples.) In security we are blind, because of those fears. Mandatory breach notification has offered a window into what goes wrong. It would be a shame to slam that window shut, or to fog it with imprecise criteria around what needs to be reported.

Security will only progress if we can study our efforts and their outcomes. Today, we have many security pundits who can offer opinions, and few who offer data to back them up, because we never get to study outcomes. As the data around breaches expands and becomes more detailed, we will be able to ask questions of the effectiveness of security advice.

Breach notice is about transparency and fairness.

Transparency is a basic principle of privacy. Organizations often commit to keeping their customer's data secure. They invest heavily in telling their customers that their data will be kept safe. Those customers rely on those promises as part of their contracts. (No one would do business with an organization that promised to leave their personal data in boxes on the street.)

Even if there is no danger (or other reason to disclose), an individual should be able to make decisions based on full data. If a rental car company routinely had no cars on its lot, a smart traveler would reserve elsewhere. A dry cleaner who stained clothes would lose customers. Claims that customers don't care about breaches, and *therefore should be kept in the dark* are farcical. If customers don't care, let them chose not to care. That a company is able to cover up their mistakes does not lead to that being used as a principle of regulation.

Breaches often involve deeply personal information

When Biofilm accidentally exposed information about those ordering their personal lubricant product, Astroglide, on the internet[iii], it was not covered by any breach disclosure law. Nevertheless, it was deeply personal information, and customers deserved to be notified.

As an aside, accidental information releases are an excellent example of what breach notification allows us to discover. Such disclosures are nearly as common as hacking incidents.

I'll now turn to the recommendations, and Industry Canada's responses to them.

Recommendation 23

First, I'd like to commend you for the recognition of the value of consistency in reporting. I'd like to encourage you to expand this vision, into understanding that consistency is helpful not only to consumers, but also to researchers. The more clear the reporting requirements, the more scientific validity the data will have, and our ability to learn from it will be greater.

Second, I believe it is unfortunate that you repeat the "notification fatigue" canard. I track these issues closely, and I have never once heard anyone, not even an industry spokesperson, assert that they have personally gotten too many notices and are tired of them. I have seen no survey research—not even a push poll—which supports the idea that people don't want to know about breaches. We can consider how ridiculous the idea would be if we were discussing toys. No one would dare to suggest that we shouldn't notify consumers of lead paint on their toys, even if much of the damage may be in the past, or in the hard-to-foresee future. With toys, it is easy to remove risk by removing the toy, a response which may be harder in the case of privacy breaches.

People do want more effective ways to respond to breaches, but that is not the same as not wanting to know about them. They may be unable to effectively leave, especially if the entity who lost their data is a bank that is required to keep their details for audit. In the United States, we have seen the emergence of a new class of business providing improved authentication and identity theft protection. Examples include Lifelock and Debix (I am a shareholder in Debix.) As long as we are honest about the scale and scope of the problem, I fully expect to see more organizations emerge to help breach victims.

Recommendation 24

I agree that notice to individuals ought to be based on an assessment of risk of harm. If there is no risk to the consumer, is it sensible to ask a business to incur the extra costs? Unfortunately, I believe that we lack the data to honestly make such assessments in most cases. How hard is it to recover data off a password-protected laptop? (Trivially easy; "Live CDs" are available free from the internet to assist in forensic investigations.) How hard is it to recover data from a tape? We have little idea. How much is stolen from them? We have literally no way of knowing today.

In most cases, identity theft victims have *no idea* how the fraudster got information about them. Fraud may take years to occur after a theft of data (e.g., evidence of misuse of stolen data from Polo Ralph Lauren first emerged more than two years after the theft). In some cases, such as the TJX case, we have a floor: we know a few people were arrested using credit card data. We don't know how many more may have avoided arrest. In other cases, say that of a tape lost five years ago, before breach notification, the victims may have no idea who lost their information. Even if they have received notice, there is no clear causal link. For example, information about "Bob" may have been stolen from the Acme company and abused. However, his information may have been stolen 3 times, and he's only gotten two notices. He might infer a link to one of those, where it really was the third dataloss that caused the issue. If Bob has correctly identified Acme as the source, he may or may not bother to notify them. If he does notify them, they may not record that data accurately. (It would be in their interest to do a poor job in such record keeping, so they could say they have no data that their customers were impacted.)

Therefore, while a risk of harm analysis is a goal worth striving for, such analysis is hard to perform, and if the analysis is wrong, it has the unfortunate effect of creating further difficulties for analysis. I would therefore urge you to set a high bar that companies must clear to demonstrate that there is no risk of harm.

The office of the Privacy Commissioner, as you point out, is well positioned to understand this. I dispute, for the reasons just explained, your statement that the Commissioner is well positioned to assess the risks. As a security professional, the most I would state is that the commissioner could provide relative risk assessments.

Finally, as a researcher who reads breach reports regularly, I was heartened to see the Commissioner's report on the TJX case. I would urge you to explicitly make complete and unredacted breach reports and analysis available on the Commissioner's web site. Such public data would enable Bob, above, to perhaps discover that an organization with his data had lost it years before, and report it. This would be far lower cost than notifying Bob in an incident where the risk is believed to be low. It would also enable researchers to consider the causes and effects of dataloss across a broader dataset then we have available today. For example, the Acquisiti et al. study mentioned in note (2) below was based on publicly available data. It is one of many studies that have been done.

Recommendation 25

I agree strongly that the specifics of triggers and thresholds are critical, and urge you to create them in light of the fact that *breach disclosure is about more than identity theft.* In particular, as I framed things in the opening of this letter, breaches offer us a window into security problems; breach notice is about

transparency and fairness; and breaches often involve deeply personal information.

With respect to considering notifying additional organizations, in particular credit agencies, I would like to urge you to ensure that the credit agencies be forbidden from crafting commercial advantage from such notification, such as "You're at risk for identity theft! Buy our services!" Secondly, I would urge you to ensure that such notification could not be used to deny credit, or to lower credit scores, but that instead, it would be used only to perform additional quality checks on incoming reports.

I would like to thank you for the opportunity to comment on the proposed regulations. I would be happy to discuss these matters further.

Yours,

Adam Shostack

---

[i] See Ponemon Institute, "2007 Annual Study: Cost of a Data Breach," available after registration at Vontu.com. See page 13: "Following a data breach, organizations suffered an average increased customer churn rate of 2.67 percent, up from 2.01 percent in 2006. Four out of the 35 organizations suffered abnormal churn rates of more than 6 percent."

[ii] Alessandro Acquisti, Allan Friedman, and Rahul Telang. "Is There a Cost to Privacy Breaches? An Event Study," Proceedings of the International Conference of Information Systems (ICIS), 2006.

[iii] See Ryan Singel, "Security Researcher Wants Lube Maker Fined for Privacy Slip," Wired's 27b-6 blog, July 10, 2007, http://blog.wired.com/27bstroke6/2007/07/security-resear.html