



Exchange Rate: Privacy Concerns
infectionvectors.com
August 2007

Overview

How much is your personal information worth to you? At home, we may take great care to ensure that data is protected: from door locks and home security systems to strong passwords, phishing filters, and disk encryption. We assign both tangible and intangible values to our privacy and identity. When giving that data to hospitals, retailers, and credit agencies, we take a (presumably) calculated risk – what return does relinquishing the data provide? Those same groups have to make a risk calculation in order to justify collecting the data as well. This paper examines a few of the forces driving the price of privacy data.

Legislative Branch

Privacy legislation is in many ways much more a definition of the enforcement for a data loss than it is the way to protect sensitive data. That makes sense since enforcement is the most important piece of privacy data protection as it gives tangibility to data losses. Laws that require fines and assess accountability take a concept that is nebulous for a corporation (i.e., personal information valuation) and assign it a “real” value: money. Once it has value, it can be managed. Rather, the risk assumed by collecting data can be weighed against the expense of not collecting the data and still trying to complete the business mission.

Navigating the threat tree for data collection (once a record is accepted as having privacy implications) involves understanding exactly how much collection will cost (including the expected costs of compromises). Possibly, a manager decides that data costs more than it is worth to a particular initiative. But that would assume that the manager has not only the cost of a loss in front of her, but also the cost of additional protection – to mitigate the cost of a compromise.

Roots

To properly evaluate any type of data (with respect to how much the data is worth), it is valuable to know precisely what qualities increase a piece of information’s price to a purchaser. Consequently, knowing why data is valuable to an attacker can help reduce the value of the information and reduce the likelihood of compromise.

Well-known services like Debix and Lifelock¹ remove the value of personally identifiable information. They require credit-issuing agencies (such as banks) to receive

explicit approval prior to opening new accounts. It is the equivalent of password protecting a logon – a Social Security Number is no longer valid on its own as identification.

In a nutshell, the theories include:

- Reduced “street” price = reduced attacks/smaller distribution of stolen data
- Increased cost of processing (i.e., decrypt it, decode it) = reduced distribution/increased time to track down thieves

Those methods are fine for individuals, but would a company be willing to buy this type of insurance for every one of their customers? That would certainly create some good will, but would it reduce liability for data losses? Not under current laws.

Truncated

Privacy rights, from a consumer standpoint, have a well-established history. In the healthcare world, the doctor-patient privilege is taken for granted, as it the case for attorney-client privilege in the legal realm. HIPAA² and IRS restructuring³ actions have extended these privilege sets beyond the doctor/lawyer space as well. These rights are often invoked to shield an individual or corporation from embarrassment or liability. In that regard, there could be some monetary value placed on the information, but it is subjective at best.

The nature of numerous court cases surrounding privacy rights has been to help identify when data is actually protected. In addition to the “type” of data (the “what”), the state of the information is also considered (the “when” and the “why”). Using very specific, concrete definitions promotes the debate over “exceptions” to protection. Definitions like that provided by the US DoD⁴ allow for context to dictate what is personally identifiable, requiring privacy protections. Beyond evaluating each piece of information in a vacuum, the aggregation of data test is required. For instance, if one’s name appears in a table called, “Active,” which resides in a database entitled, “Dental Customers,” that is accessed through a health insurance issuers web site, it may be gleaned that the individual is a participant in a particular plan. The seriousness of the compromise is generally a reflection of how many individual records were jeopardized, and even then in terms of the “betrayal.” When a health insurance organization (or say, the Veterans Administration) loses records, the role of the data holder could be a damage multiplier. But, let us consider how laws are to be written and enforced. Should the nature and number of records be considered when evaluating the protections required for the data? In US federal parlance, the term “system of records” has been applied to large, searchable databases.

How about individual CRM applications like Microsoft Outlook contact lists? If one gets an email, stores all the contact info from the signature lines, do I have a system of

records? It is certainly indexable, contains identifiable information, and would be pretty large (over 25 records for sure).

To an affected individual, the value of one personal record is not tempered by whether thousands of other records were also disclosed, and businesses will undoubtedly have to deal with that when considered the true costs of protecting databases.

Vectored

The type of assessment that is required for personal information does not seem too difficult. Legislation, in many cases, spells out exactly what is and what is not considered “private.” That being the case, we can identify a series of questions that point to privacy assurance measures and where disclosures take place:

Prior to fielding any new application or system:

- Was an assessment completed?
- Were countermeasures enacted to meet the requirements of the assessment?

After a compromise (hopefully, never needed):

- Was privacy data compromised?
- Was compromise a result of data misclassification?
- Was compromise a result of ineffective safeguard?

If systems are allowed to go online without any review of what they collect (and what business need that data is matched against), it is unlikely that adequate safeguards will be taken. Consider all of the places that the data is in jeopardy without specific security measures: while being typed into the browser window, in transit from the browser to the web server, in storage on the server, in backup copies of the server’s contents, in processed form once queried, any reports (electronic or printed) that analysts make. Companies have a responsibility at each stage:

Stage	Storage	Responsibility
Browser	User Machine	XSS issues resolved, any plug-in is safe, due diligence against phishing, authentication
Transit	Network devices	Encryption
Server	Database	Encryption, Authorization
Backup	Disk/Tape	Encryption, physical security
Reports	Paper	Physical security
Reports	Electronic	Encryption, Need-to-know

This very simple view of data collection reveals the potential costs for any private information that is collected. What are missing from the table are the persistent costs: the data must be protected as long as it is held (as very little personal data loses value over time) and any breach will result in notification costs. In some cases, these costs are well-

known⁵; in other cases they will require collaboration between technical and non-technical administrators.

Even the least cynical among us would probably agree that the value the individual places on their personal data is higher than the average hospital, corporation, or credit bureau places on it. But that view may not be accurate. Refined enforcement policies and open discussions about remediation efforts are critical to creating a common calculus for data valuation. People have the ability to rally for tougher punishments for lackadaisical data handling, if they are willing to pay the price (in terms of security measures on the corporate side) for stronger assurances that their data is safe. The same type of calculations take place for the corporate risk manager, who is now charged with knowing exactly what resides on the media in the server farms.

References

1. Debix and Lifelock information can be found at the respective web sites:

<http://www.debix.com> & <http://www.lifelock.com>

2. Full text of the HIPAA can be found at:

<http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf>

3. Internal Revenue Service Restructuring Act of 1998, Public Law No. 105-206 (H.R. 2676) (22 July 1998):

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ206.105

4. DoD exemption, DoDD 5400.11r:

<http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf>

From the text, the protections do not apply to records: "C1.3.1.3.5. Maintained by the contractor incident to normal business practices and operations."

5. It may be especially interested to clients in the health sector to review the Final Enforcement Rule from 2006 for HIPAA:

Department of Health and Human Services, 45 CFR Parts 160 and 164, HIPAA Administrative Simplification: Enforcement; Final Rule. "Federal Register." Vol 71 No 32, 16 February 2006.

<http://www.hhs.gov/ocr/hipaa/FinalEnforcementRule06.pdf>