



claudia
imhoff

Can You Keep a Secret?

Some Companies Can and Apparently Some Can't!

Lately there have been a number of serious breaches of major companies' databases, resulting in big news splashes about customer, financial and medical information being compromised, possibly downloaded and used fraudulently. ChoicePoint and LexisNexis, along with other information providers, have had their names in the press from the news that hackers were able to get at their data. The Wall Street Journal is not where you want to air dirty laundry. Similar breaches spurred the California legislators to pass their notification law in 2002, and the Federal government is now considering a similar law.

On the other hand, commercial gain and governmental investigations are also eroding privacy in ways we would not have imagined five years ago. The buying and selling of customer information is at an all time high. For example, the 1974 Privacy Act, which forbids a governmental agency from secretly collecting information about our citizens unless there is a "proper purpose," does not stop the Justice Department from spending \$63.4 million with the very same ChoicePoint just in the news. Why? It appears that loopholes in the Privacy Act allow federal investigators to tap into databases of personal information collected by these private data brokers. While not illegal, it is a disturbing practice that seems to violate the spirit of the Privacy Act. It appears that customer privacy is under attack from a number of fronts.

One thing is certain. This digital information is of great value to commercial enterprises and governmental agencies alike, and there are dozens of companies willing to sell services that track a person digitally as he or she moves around the Internet, uses credit cards, uses loyalty cards for purchases, fills prescriptions, etc. In reading a number of articles from privacy experts, it appears that business intelligence is squarely in their crosshairs. What should we be doing to prevent a catastrophe or severe restrictions on data usage?

How society will change as the digital footprints erode privacy is unknown. We all love services that save us time and money. I know I get quite aggravated when I visit a Web site and it doesn't remember my login information or when my bank's ATM machines don't recognize that I want the screen information in English. On the other hand, I am affronted or at least uncomfortable when I see the vast amount of "personal" information (former addresses, current neighbors, phone numbers, list of relatives' addresses, ages in family, etc.) that you can get by purchasing a \$4.50 report from ChoicePoint!

Indeed, the information providers struggle with how much they should allow other companies or governmental agencies to use the customer profiles they have accumulated. Civil liberties

and our need for privacy must be delicately balanced with the needs of commercial enterprise as well as national security. It is this balance that is so difficult to find when the advances in technology and utilization of data are expanding at such a high rate.

What to do? Well, there are few suggestions I can make. I am sure there are many others, but these stand out.

- Education and training are badly needed not only in the commercial usage of personal data but also in our governmental agencies' usage. Most organizations – commercial as well as governmental – do not have formal training or education about privacy and the misuse of data. Most, in fact, don't have formal, documented punishments or responses to breaches in privacy.
- New rules and regulations must be established regarding the do's and don'ts of privacy. The Privacy Act should be updated to regulate the new capabilities available today that were not even thought of 31 years ago. It should be extended to cover the private (commercial) data brokers so that our government can't do an end run around the law. Meanwhile, our federal legislators should continue to work on meaningful new privacy protections.
- Everyone should be able to see their own profiles in these databases and be able to change or correct these records. Perhaps it even makes sense for you to be able to delete them from existence if you so choose. The best defense against an inappropriate invasion of your privacy is to understand what is known about you to begin with.

To repeat, the key to a successful privacy policy is a balance between the individual's need for secrecy and the public need to understand who this individual is. The benefits to the individual can be greatly welcomed as long as that fine line is not crossed. It does appear that government-backed constraints will be needed as our technology gets smarter. Until then, we must be vigilant in our usage of this sensitive data, doing everything possible to stop breaches and educating and monitoring internally what is and is not acceptable in terms of the processing of this data. 

Claudia Imhoff, Ph.D., is the president and founder of Intelligent Solutions (www.intelsols.com), a leading consultancy on CRM and business intelligence technologies and strategies. She is a popular speaker and internationally recognized expert and serves as an advisor to many corporations, universities and leading technology companies on these topics. She has coauthored five books and more than 60 articles on these topics. She may be reached at cimhoff@intelsols.com.