2. FEATURE: SAFEGUARDING INTERNET PRIVACY: AT WHAT COST?
By Wayne W. Eckerson
Director of Education and Research
The Data Warehousing Institute

*************
SUMMARY: Safeguarding Internet privacy has become the issue du jour in Washington, DC, with hundreds of privacy bills pending in the U.S. Congress. Yet, in their rush to protect consumers’ right to privacy, legislators and privacy advocates need to be careful not to ram through laws that could curb the kinds of personalized services that customers want vendors to provide. Once the government establishes basic privacy regulations, it then needs to trust the power of a free market and a democratic society to secure online privacy for Internet users.

* Privacy Paranoia

As keepers of customer information, data warehousing professionals need to tune into the ever-widening debate over Internet privacy. Not that the debate makes any sense, mind you. It seems that the illogical euphoria that fueled Internet stock prices to stratospheric levels has mutated into a feverish paranoia over Internet privacy.

It reminds me of ancient Internet history (about three years ago) when most people were afraid to use credit cards to pay for goods online. That fear was largely irrational since the same people never had a tinge of remorse about giving complete strangers (i.e. customer service representatives) their credit card numbers over the phone. Now, most people are perfectly comfortable allowing their favorite e-tailers to store their credit card numbers online to expedite future transactions.

But Internet privacy has just entered the paranoia maelstrom. Many people— even those staking a good portion of their retirement income on Internet stocks—are now pushing for restrictive privacy laws that could undermine the potential of the Internet to improve the ways we communicate and do business. It is no surprise that government officials are perhaps the most paranoid. Few officials understand technology, and many quake in trepidation over the Internet’s libertarian exuberance.

Fearful of losing control of what they do not understand, government officials do what they do best: legislate. Currently, there are more than 300 privacy bills pending in the U.S. House and U.S. Senate, and there is a swarm of state attorneys general vying to clamp down on the Internet, if the federal government fails to take action.
* Electronic Versus Paper Junk Mail

But this fear makes little sense. Today, companies routinely sell customer lists and information to almost any buyer and make a fortune in the process. And what do companies do with these lists? They send mountains of junk mail to masses of people and generate millions of unsolicited phone calls that invade our personal space, raise our blood pressure, and annoy the heck out of us.

Despite the vast amount of information that we can collect about people via the Web, junk mailers generally know more about us than online vendors. Companies that rent lists can also tag purchased names with demographic, psychographic, and credit rating data. They can also apply statistical algorithms to these records to predict our purchasing behavior and anything else, for that matter. Talk about Big Brother!

In contrast, online vendors today generally lack the expertise, tools, and processing power to capture, analyze, and act on the gigabytes of clickstream data that flow across their Web servers each day. In fact, most online marketers today create email campaigns or Web cross-sell offers from information that Web visitors volunteer about themselves through online registration forms.

Someone correct me here, but I think we are barking up the wrong tree. We should focus more attention to develop tighter restrictions on paper-based junk mailers and telemarketers than to try to regulate the Internet. Although junk mail and Web banner ads can annoy us, they are much easier to get rid of than paper-based junk mail which clogs our landfills and pesky telemarketers who never take “no” for an answer.

The Internet privacy debate seems like a big smokescreen to avoid tackling the real issues. It seems to me that the U.S. Postal Service would take a big hit if we clamped down on paper-based junk mailers, and big telecommunications companies, with their high-paid lobbyists, would suffer if we clamped down on telemarketers. Whose interests are we protecting here?

* The Role of Privacy Rights

Before you accuse me of concocting a conspiracy theory, let me be clear: I think privacy rights are important to a smooth functioning democratic society.

For example, I do not want to give sex offenders the right to “opt out” of having to disclose when they move into my neighborhood. I do not want insurance companies to find out that I have been browsing Web pages on
debilitating diseases, such as AIDS, diabetes, multiple sclerosis, and so on. I do not want my favorite e-tailer to break its promise and sell my profile information to appease creditors in a bankruptcy proceeding.

In short, I generally agree with the Federal Trade Commission’s guidelines about Internet privacy. In general, those guidelines state that every company should post and adhere to a privacy policy, give users the ability to access the personal information that companies possess about them and give users some choice on how these data are used.

Yet, even these guidelines, if taken too far, will undermine the Internet’s potential to simplify our personal and professional lives. Face it: People flock to the Internet because it makes it easy for them to find and share information, purchase goods, and obtain service and support without leaving their homes or offices. But some proposed privacy policies may choke the free-flow of information which makes the Internet such an attractive medium for conducting business today.

* Downsides to Restrictive Privacy Policies

For instance, large corporations oppose restrictive opt-in proposals because they prevent companies from providing the kind of unified customer service and support which customers are screaming for. Specifically, some proposed privacy regulations would make it difficult for business units with separately branded products to share customer information without first getting each customer’s permission.

This would make it even more challenging for companies to create a "360-degree view" of customers than it is today. There is no quicker way for a company to lose customers than to shuttle them endlessly between departments and voice mailboxes when they call up with a question that cuts across internal product, organizational, or geographical lines. The customer wants to deal with one company, not 20 or 30 separate fiefdoms.

Customers also want other conveniences, even if it means that companies must share customer information. For example, many financial services customers would like to receive a monthly statement that integrates their bank accounts, mortgages, investments, and insurance information on a single statement. Some customers are already demanding such service, even though they purchased these services from different companies. Or, they want to complete a travel profile and itinerary once and pass it automatically to airlines, rental car agencies, and hotels so they only have to fill out their schedule once for every trip. In addition, according to surveys, a majority of customers also want to receive targeted offers and promotions for the things in which they’re
most interested. Most people--especially Americans--love a bargain or special deal and want to be notified about it. They expect companies to know who they are, what they’re interested in, and how to contact them but they don’t want their privacy to be invaded.

* The Case for Free Market Regulation

Given these attitudes, the goal of privacy regulation should be to protect users' basic right to privacy without hamstringing companies from using the Internet to improve customer service, support, and satisfaction. To do this, I believe the government should set basic privacy standards for the Internet and let the market police itself thereafter. And it will, for three reasons:

A. The Market Weeds Out Untrustworthy Players

First, researchers have discovered that the key to Web site stickiness is trust, and a key element in developing trust is a well-constructed privacy policy as well as good old-fashioned customer service. That’s according to Bain & Co. consultants Frederick F. Reichheld and Phil Scheffter in their article titled “E-Loyalty: Your Secret Weapon on the Web,” (Harvard Business Review, July-August, 2000.)

“When customers do trust an on-line vendor,” the authors write, “they are more likely to share personal information. That information enables the company to form a more intimate relationship with customers, offering products and services tailored to their individual preferences, which in turn increases trust and strengthens loyalty. Such a virtuous circle can quickly translate into a durable advantage over competitors.”

In short, online companies that build trust through continuous mutually beneficial interactions will succeed. Companies that violate users’ trust will lose customers and eventually fail. Thus, the free marketplace will reward companies that respect and protect customers’ privacy and punish those that do not.

B. New Technology Minimizes the Impact of Spam and Banner Ads

Second, the marketplace is developing and deploying technology to deal with some of the less desirable outcomes of Internet marketing. For example, many email programs now have a feature that automatically routes junk email to a special folder or right into the “recycle bin.”

Also, increasing numbers of Internet service providers (ISPs) subscribe to Internet junk mail watchdogs, like mail-abuse.org, which filter messages from known or alleged "spammers." As more ISPs subscribe to
such services, spammers will become inundated with their own “bounced” messages and find it uneconomical to continue their practices.

In addition, Web advertising is foundering somewhat because most people ignore Web banner ads more than other types of advertising. Consequently, banner ad rates have plummeted during the past year. Most Web advertisers now seek new arrangements in which they only pay for ads that produce click-throughs or purchases, rather than page impressions.

C. E-Marketers Balance Profiling and Privacy

Finally, the companies most capable of becoming demonic Internet Big Brothers have taken stops to adhere to strict proposals for regulating Internet privacy so they don’t have to rearchitect their systems later. Companies like Engage, Mat&logic, and various other Internet advertisers learned a big lesson when competitor DoubleClick was “publicly lynched” this past year when it engaged in business practices that many perceived Internet users perceived would undermine their privacy.

Most e-marketers now advocate the most restrictive form of permission marketing, known as “opt-m.” They have also erected a dividing wall between “known” data and “anonymous” data. They do this to avoid DoubleClick’s mistake of attaching name and demographic data to anonymous Web “cookies.” This prevents e-marketers from identifying Web site visitors before they’ve decided to register or identify themselves.

But this does not stop e-marketers from doing their jobs, which is to provide advertisers with individuals (or “eyeballs” in Web parlance) who are most likely to be interested in their products. To do this without violating users’ privacy, e-marketers analyze voluminous amounts of anonymous clickstream data culled from dozens of their own or partners’ Web sites. Using statistical techniques, they develop generic (and anonymous) “cookie profiles” that contain a surprising number of demographic attributes, such as gender, location, and income.

But rather than target specific cookies—which is a definite no-no--these e-marketers watch the behavior of individuals who surf a Web site in real-time and try to match them to one of their generic profiles. Once they make a match, the e-marketer then delivers a banner ad or promotion to the Web site visitor that is appropriate for the profile they match. Or at least, that’s the goal. This takes a lot of sophisticated technology, analysis, and processing horsepower and few, if any companies, can do this today.

* Conclusion
For the three reasons above, I believe a **free** market in an active democratic society can adequately **regulate** Internet privacy, once a baseline set of policies and regulations has been implemented. Why? Because businesses desperately want to avoid doing anything that infuriates customers and causes revenues and profits to flee to the competition.

Today, there is too much economic disincentive for companies to ignore customers’ privacy concerns or provide substandard service and support. But the key here is that customers need to make their wishes known--quickly and loudly--because companies will either have to listen or lose **their** customers. This is why a democratic society and free press are so important. They keep communications open, interactions fluid, and businesses honest.

On the other hand, expansive government laws and regulations create the opposite effect. They tend to rigidify the issues and stultify communications, which makes it difficult for companies and customers to engage **in** a healthy, ongoing dialogue. Regulations do not readily accommodate technological advances, which can change the fundamental rules of the game.

**In the end,** too much regulation--especially when pushed through **in** an emotionally charged environment--ultimately means that everyone suffers and no one really wins.

Wayne W. Eckerson is **the** Director of Education and Research at The Data Warehousing Institute. He can be reached at **mailto:weckerson@dw-institute.com.** Wayne welcomes your reaction to this and other articles printed in **FlashPoint.**