9/25/01 12:53:12 PM

Whose Information Is It Anyway?

by Lynie Arden

Unscrupulous information vendors are willing to sell whatever information about you they can get. At the least that's annoying. At the worst, you could be ruined by identity theft when a criminal takes over your personal information. It's not all that hard to do, considering how many times you're asked for information, how many times you hand it over without question, and how many places it's stored, swapped, and sold. Oddly, most people put themselves in that vulnerable position willingly, being lured to fill out a personal information form with promises of freebies or contest entries. To online information grabbers, it's easier than tempting kids with candy and puppies.

E-commerce is growing rapidly. There are now more than 130 million Internet users in the U.S. alone and market analysts expect that number to rise to 165 million by the end of next year. To reach this growing market, businesses spend enormous sums for market research and advertising -- more than $6.6 billion of it online alone. That spending is expected to outpace the number of consumers getting online, topping out at a whopping $16.5 billion by 2005.

As e-commerce grows, so does the desire to collect personal data. Businesses spent $4.8 billion last year for marketing data with which to target their selling efforts. That's a lot of money and anyone who wants a piece of it seems to be willing to sell you out by grabbing what is rightfully yours -- your personal information.

Who's Got Your Number?

Any Web site with the inclination to do so can track your movements just by using "cookies." It may seem harmless, but to privacy advocates, it smells like Big Brother is coming. Through the use of cookies, operators can see every page you visit and make note of every ad that captures your attention. The practice is known as "profiling," something that gives marketers the ability to know you, in many cases by precise identity, and build detailed profiles that include your tastes, preferences, and activities. This all happens invisibly, of course, but try to imagine someone with a clipboard and a tape recorder following you around on your next trip to the mall. It wouldn't be long before you called a cop.

Individual sites participate in this practice all the time without anyone taking much notice. But someone did blow the whistle on the biggest Web-based advertising company, DoubleClick Inc. It seems the Internet behemoth was using ad-tracking cookies throughout 11,500 sites to track Web users by name and

address as they moved from one Web site to the next. And that was just the beginning. When DoubleClick bought Abacus Direct Corp., a leading direct marketing services company, it was able to merge the information gathered online with a database containing the information on more than 90 percent of American households.

DoubleClick considered this practice just good business, allowing it to better target its online ads, calling the practice "personalization." Consumer advocates called it something else: invasion of privacy. Through the use of cookies, DoubleClick was able to identify Web surfers -- something it claimed it wouldn't do -- by following the trail of cookie crumbs until contact information was left at a site. Sometimes the information was provided as a shipping address so the user could get a package through the mail, and sometimes it was required for registration on a site. DoubleClick built an enormous database of information, collecting more than 100 million files, while wiping out the anonymity of online users along the way.

Not only did DoubleClick disregard the privacy of online users, it added insult to injury by refusing to disclose the names of the companies involved in feeding them consumers' identities, in effect protecting the privacy of the privacy violators.

The Risk of Losing Control

If you're protective about your privacy, you are right to be concerned over how your personal information is collected and used by companies. Suppose that on your last trip to the grocery store, you happened to buy cigarettes for your neighbor or a nice bottle of wine for a dinner date. What you bought was nobody's business, right? Now suppose someone were to take your grocery Bonus Club membership information and sell it to your health insurance provider. Think about it. The ramifications are unsettling. Virtually everywhere you go and everything you buy could be open knowledge to anyone with the cash to buy the information -- not just marketers, but also employers, health insurers, and government agencies.

You may recall the incident in 1998 when a U.S. sailor was subject to discharge from the Navy for "Homosexual Conduct Admittance." The sailor accused America Online (AOL) of violating its own privacy policy by revealing his member profile where he had listed himself as "gay" under "Marital Status."

Then there is the case of medical information. Have you ever tried to sneak a peek at your own medical file? It's just about impossible. Sure, you can request that your records be passed from one doctor to another, but you can't just march into your doctor's office and demand to walk out with your own information. Yet it's estimated that, once you are confined to a hospital, more than 70 people will get to see your "chart." What's more, your insurance company, the HMO, the government and a host of computer hackers now have the capability to open your computer-based medical files. The exposure could cost you your job, any anticipated promotions, even your insurance coverage.

Most databases are full of profile records that are inaccurate or out of date, yet important decisions are being based on that information. Especially in the case of credit reports, errors can cause some real problems, but have you tried to change your credit report information? You may find yourself being treated like an intruder trying to throw a monkey wrench in the system. Sure, it can be done, but it isn't easy and it certainly isn't fast. On the other hand, a subscribing company

PRIVACY OPTIONS
Opt-Out Letter Generator
Stop Junk Privacy Kit
Privacy Features
Privacy Fact Sheets
Privacy FAQs
Privacy Sources
Privacy News

More Ways To Protect Your Privacy!

Privacy Main

SEARCH

can add any information they want to your record and no one even questions it. Yet when you want to view or change your information, it's a different story. After all, you're not the one paying the subscription fee, are you?

Protect Your Information

As long as we choose to surf the Net, we are risking losing control of our information. You can greatly reduce the risks by:

- **Avoiding third parties.** Once your information is passed along, you can consider it completely out of your control. A Web site's privacy policy should clearly state whether your information will be shared with third parties, who and where they are, and how the information will be used. It's not good enough to say "We only share this information with our select advertisers." That just means anyone who has the money to pay for it can have it.
- **Demanding access.** Access to one's own data is at the heart of most privacy laws. Before giving away any information, check the Web site's privacy policy to see if you will have the right to view your personal information and make corrections if necessary. Unfortunately, sites where users can access their own information files are rare. In an ideal online world, Web site users should be able to create their own personal profile, access that profile at any time, revise the information as necessary, and control who sees it. It's your right to make sure your information is accurate and complete at all times.
- **Opting in.** Preferably, a Web site will ask your permission before collecting and using your personal information. It's only polite for a company to ask "May we occasionally send you email promotions?" or "may we keep you up-to-date with monthly newsletters?".
- **Opting out.** At the very least, a site should allow you to remove yourself from any database upon request. It is your information, after all. If that's not an option, don't get involved to begin with. The problem with opt-out policies is that companies can make use of your information until you notify them to stop.
- **Setting limits.** Your personally identifiable information should only be required to transact business or for some other specific purpose. Just because you register to use a particular service does not give anyone the right to use and sell your data any way they wish. Check the privacy policy to learn why your personal information is required and how it will be used. If a site didn't make some effort to provide this basic information, you should consider it an inadequate privacy policy and go elsewhere.
- **Surfing anonymously.** Most Web sites allow access to their home page and at least some additional browsing without disclosing any personally identifiable information. The practice of anonymous browsing is a good indicator of how privacy is being protected on a site. In the real world, you wouldn't expect to be asked for identification before being allowed to enter a store and browse around. Macy's wouldn't have many customers if it did. Only after you have looked around and scrutinized the terms of the privacy policy should you consider filling out online registrations, surveys, or forms.

Some information is also collected from online users surreptitiously with "cookies." It is more difficult to set hard and fast rules about allowing cookies to be used. Generally, sites that have registration or membership, such as Disney or

the New York Times, use cookies to store information on the user's system. But other sites enable cookies for purposes unrelated to registration. You can set your privacy preferences in your browser to disable cookies, but it could be problematic, limiting your ability to sign up for ongoing services or using shopping carts.

In the long run, the most important thing that you need to remember is that it is your information being collected. Take the time to protect it -- and to protect yourself.

Related Information

Privacy Fears Online

Since the beginning of the Internet, users have been concerned about privacy issues, and those concerns are growing more severe. It seems the general public shares Web surfers' concerns. Recently, The National Consumers League (NCL) discovered through a survey that what worries American consumers most is not health care, crime, or taxes. It's loss of privacy.

Other Privacy Features