Private, Keep Out!

By Dennis M. Kirschbaum, ARM

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Meeting Your Clients' Expectations of Privacy Online

I would not call myself a runner. Yes, I do jog for exercise a few times a week, but to me a runner is someone who competes in races, wears a number, and has the special shorts and shirts purchased at the specialty store in town. So I was surprised when I received my special invitation" for the "Runners Credit Card." Normally, I don't even open such solicitations but this one intrigued me and I opened the envelope.

What interested me was not the low introductory interest rate. Nor was it the fact that the annual fee was waived because of my excellent credit rating. It wasn't even the nice picture on the front of the card depicting a fit athletic looking guy ambling down a green country road. No, what I wanted to know was how they got my name!

I have never run in a race, never subscribed to *Runners World* and I am not a member of any runners' clubs. How did they know? I imagined a person from the credit card company driving around suburban neighborhoods looking for joggers, following them home and then tapping their addresses into a tiny palmtop computer before transmitting them via satellite to the home office. Then I remembered. Two weeks before I had purchased a pair of running shoes from a respectable mail order company. I had tried out the company's website and ordered on the Internet.

I was impressed at how targeted the marketing was. Not a generic sort of thing but a product aimed directly at a personal interest or hobby. Also they had struck while the iron was hot as if they knew that for me a hobby often begins and ends with the first purchase.

Yet it bothered me too. I felt that my privacy had been invaded. This company I had chosen to do business with had sold my name and some information about me and hadn't even asked me if it was ok.

My experience was not unusual. An extensive survey conducted last year by the Federal Trade Commission found that only 14 percent of commercial websites informed customers how they used the personal data they collected. The survey also found that 89 percent of the sites aimed at children collected information from the children visiting the site. And according to a more recent Georgetown University business school survey, 93 percent of websites collect information about consumers.

"Your first responsibility to your clients is to let them know what you plan to do with the information you collect

about them."

Over the last several years, the Internet and e-mail have dramatically changed the way the world communicates and exchanges information. Where once a single letter could take a week to cross the country, now an e-mail message can travel to thousands of destinations around the globe in seconds. And while your organization's ability to get its message out was once limited by the number of newsletters it printed, now everyone who has access to the World Wide Web can interact with your organization from anywhere in the world.

There are also new opportunities to gather information and to learn and interact with your constituency. New interactive websites use technology to collect names, mailing addresses, personal preferences, and even credit card information about clients and customers. And although these new technologies provide welcome service and convenience to clients, with easier access to information comes the potential for misuse.

The Internet is a marvelous communications tool. And unlike the more traditional forms of media it can allow your organization to collect information as well as distribute it. You can track your clients' preferences, buying habits, meeting attendance and history with the organization. But what happens to the information you collect? And what is your legal and moral obligation to your client regarding how you use and store the information you collect?

Legal Obligations

As in most areas that are rapidly evolving, government legislation can not hope to keep pace with changing technology. The federal and state governments are struggling to create legislative and regulatory guidelines that will protect consumers online without dealing a deathblow to the emerging Internet marketplace. Right now, with some restrictions, organizations that collect information about you can use that information for marketing purposes without getting your permission unless they have told you that they will not. Laws vary from state to state and among nations so complying with all the laws can be difficult especially given the global nature of the Internet.

But for many nonprofit organizations, the issue is even more complex. First of all, the nature of the information that you have about your clients may be different. The fact that a client is HIV positive is far more sensitive than the fact that they buy running shoes. And even if you never sell or give out your mailing list, you must consider what may happen if a security lapse results in private information becoming public.

Changing Expectations

What do your clients expect you to keep private? There are no hard and fast rules, but generally clients expect that you will respect and protect their:

- Rights relating to name, identity, picture, and voice.
- Privacy of communication (i.e. that you will not tape phone calls or forward their e-mail messages without permission).
- Employment records, credit history, social security number, financial information, and medical records.

Make a Bold Statement

Your first responsibility to your clients is to let them know what you plan to do with the information you collect about them. This can be accomplished by creating a privacy statement and posting it prominently on your website (for an example of a well written and thought out Privacy Statement see the website of the Software & Information Industry Association. If you sell your mailing list or make it available to other nonprofits from time to time, tell your clients and give them a chance to opt out. If you never give out your list, tell them that too. Just remember that if you change your policy down the road you will need to let everyone on the list know about the change. Also when considering your privacy policy think about who will be using your site. If the site is aimed at children, for example, you need to be very careful if you collect any information at all.

Because laws vary so widely, an attorney should review any privacy statement before it is published or posted on your website.

Nonprofits have a moral if not a legal obligation to protect sensitive information about clients and customers.

Understanding both the law and your clients' and customers' expectations are key to implementing a successful privacy statement. In a world where so much about us is known and can be obtained through electronic databases and reports, clients are demanding to know how you will use any information you collect about them. Communicating your intentions and your need to know up front will go a long way toward protecting privacy and maintaining a good relationship with your clients.

For a more comprehensive look at the risks posed by emerging technologies see: "Risks of the Electronic Age," a new section in the 2nd edition of *Mission Accomplished: A Practical Guide to Risk Management for Nonprofits*. (Mission Accomplished has replaced by *Enlightened Risk Taking: A Guide to Strategic Risk Management for Nonprofits*.)

Components of a Comprehensive Privacy Policy

According to Lauren Hall, chief technology officer at the Software and Information Industry Association, a privacy policy should address the following areas:

Notice

In order to make an informed decision, clients must understand what data is being collected and how it will be used.

Consent

Consent ensures that clients have choices regarding the use of their personal information and have an opportunity to "opt-out" if they wish to.

Access and Accuracy

Clients not only want to monitor what information is collected about them, they also want to ensure that it is accurate. Providing access to individuals to their own data can increase their confidence in the system.

Security

Security relates to how your organization stores, processes, and maintains sensitive data. Having a strict privacy statement is of little value if your employees have unrestricted access to the information or if your server is in an unsecured location. Obviously the more sensitive the information, the greater is your duty to protect it. Also there is a risk of unauthorized hackers breaking into your system. If you host your website in-house, have a thorough security analysis performed by a qualified systems specialist. If an Internet service provider hosts your site, inquire about what kind of security systems they have in place to protect your site from hackers.

Redress

Provide a means for your clients to resolve any privacy concerns that they may have. By responding quickly to complaints, you may prevent far greater problems later on.

Enforcement

Privacy policies are an important first step but need to be followed up with oversight and enforcement. You need to consider how your organization will ensure that all employees and others who have access to data will comply with the policy. For organizations with a sensitive client list or information of a medical or financial nature, third-party oversight may be helpful. There are firms that can provide this oversight and provide certification for your website.

Dennis Kirschbaum is Manager of Information Technology for the Nonprofit Risk Management Center. Questions about this article should be directed to Dennis at (202) 785-3891 or via e-mail.