Personal Privacy: The Latest Oxymoron on the Internet

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

The meaning of “personal privacy” has changed over time. Activities that would have been considered an invasion of privacy a decade ago have become routine and acceptable to many in 21st century society. For instance, a social security number, which originally was to be used for one purpose, is now used as an identifying code on many driver’s licenses and other documents. Very recently, keeping a customer’s credit card number on file or photographing a car as it proceeds through a tollbooth or intersection, or creating an electronic signature that can be copied and pasted into other documents would have been considered by many Americans to represent unnecessary and inappropriate invasions of personal privacy.

However, Americans are finding that if they want to conduct business, they must acquiesce more and more to never-before-imaginable invasions of personal privacy. But passivity isn’t the American way: there is growing concern among employees and consumers alike that our society has gone too far in permitting invasions of once-sacred privacy for commercial efficiency, marketing, reducing actions of scofflaws or other reasons.

And then we have the Internet, possibly the greatest single assault to private information. No longer does the expression: “On the Internet, nobody knows you’re a dog” apply. The anonymity one once enjoyed when traveling the information superhighway was fleeting. Internet travelers are increasingly identifiable. With the growing use of forced logons that require providing personal information before you can enter a site; spyware that comes along for the ride, unbeknownst to you, when you download a desired software program and forevermore tracks your use of the Internet; and “cookies” that automatically identify you when you logon to a Web site; computer users are becoming increasingly accustomed to unprecedented intrusions into their personal lives.

Despite these concerns, there remains no comprehensive federal law addressing privacy. Isolated attempts at legislating the issue have resulted in protecting one segment of the population: The Children’s Online Privacy Protection Act, which requires parental consent before identifying information (i.e., full name, home address, e-mail address, and telephone number) can be obtained from children who are under 13 years of age. Across the country, some 465 privacy-related bills have been introduced in 46 state legislatures, but none have become law.

Balancing the needs and rights of your nonprofit against its employees and its clients can be tricky. Creating use policies, educating people on their existence and chastising those who break the policy go a long way towards providing necessary protection.

The Nonprofit Organization

Have you completed a detailed privacy risk assessment as part of your nonprofit’s risk management strategy? Do you know what kinds of personal information your nonprofit collects, keeps and uses? Do you know how much of that material is gathered via the Internet or stored on computer? Do you know which of that personal information your nonprofit discloses intentionally or unintentionally? How secure is that information from

external hacking, internal sabotage, and generally from those not in a need-to-know position within your nonprofit?

A privacy policy statement posted on your Web site can help solidify service-recipient relationships. If the user of your Web site knows that the organization's policy is to safeguard personal information and let the site user determine what information to provide, what gets collected and how it is used, they will feel more confident in providing information about themselves to you. Of course, you have to honor your policy or trust will be broken. Thus, you need to put procedures in place that back up your Internet privacy policy.

Employees

An important component of a nonprofit's policy governing the use of computer equipment is a provision that seeks to dispel any notion or expectation of privacy with respect to use of the nonprofit's systems and equipment. According to a recent survey undertaken by the American Management Association, 78 percent of U.S. companies monitor employee phone calls, e-mails, Internet access, or computer files. Among 1,600 midsize to large companies responding to the survey, 63 percent reported monitoring Internet use, while 47 percent reported storing and reviewing e-mails. While nonprofits may be less likely to monitor equipment and system use by employees, the growing awareness about the risks associated with such use is likely to increase monitoring in the years ahead.

Risks and Reminders About Employee Privacy

- Make certain that employees have no expectation of privacy with respect to their use of technology owned by the nonprofit, or their use of their own computers for business purposes in your facilities.
- Remind employees who express views or make statements that are inconsistent with the nonprofit's policy about the existence and importance of policy.
- While passwords are important to system security, management must be able to access employee files and data. Your systems administrator should keep a securely held record of all passwords in use within your nonprofit, and that record should be available only to the administrator, the executive director, and a backup responsible for your systems.

Clients

Protecting client privacy is an important consideration for every nonprofit. Whether the organization provides emergency shelter for victims of domestic abuse, matches mentees and mentors, or places children in adoptive or foster families, every nonprofit should take reasonable measures to safeguard personal information about clients.

The availability of computer systems has resulted in tremendous improvements in case management. Client information previously maintained in worn file folders can be tracked in a database and readily retrieved by those with a "need to know." A push-pull relationship exists between the need to protect client privacy and the desire to use state-of-the-art technology to enhance efficiency and program management. We must accept that a slight loss of efficiency comes with the need to adequately protect client privacy. By the same token, no system can be completely secure from breaches of privacy and still be functional. Striking the appropriate balance for your organization requires a thorough review of your programmatic needs and technological capabilities.

Risk Management Strategies to Protect Client Privacy

- *Articulate your nonprofit's policy concerning client privacy and instruct all staff on the policy*. For example,"[Name of Nonprofit] is committed to protecting the dignity and privacy of all clients. Staff will keep client information in confidence, disclosing only with full permission to those who have a need-to-know, and not disclosing confidential information through insecure means, such as unencrypted e-mail, fax or wireless telephones."
- *Obtain permission before using photographs or other information about clients for public relations or marketing purposes*. Always obtain a signed photo release form before including photos of your clients in an annual report or on your Web site. One nonprofit faced a costly lawsuit by a client alleging that a photograph of him appearing in a photography exhibition violated his privacy. Exercise extreme caution

when using photos of children for any purpose. For example, if a photo of a child appears on your Web site, no information that could help identify the child should be provided (the name of the school the child attends or the child's name plus the name of the town in which he or she lives). This information could be used by a predator to track down the child in order to victimize him or her.

- *If your nonprofit maintains detailed files that contain highly personal information about your clients, restrict access to these files to those individuals whose job requires them to use the files.* In some organizations highly personal information should be kept separate from information that several persons in the nonprofit may need to view from time to time. For example, monthly progress reports concerning a mentor-mentee relationship may be accessible by several departments within the organization, while the results of the initial intake process, including answers to highly personal interview questions, may not.
- *Keep your systems secure, and let employees know that the need to maintain client privacy is the job of everyone*. Change system passwords on a regular basis (every 60 to 90 days), and keep regular audit trails of information accessed on your database. When telecommuting employees leave the organization, change the access phone numbers into your system to prevent unauthorized entry.

This article was adapted from *Full Speed Ahead: Managing Technology Risk in the Nonprofit World*, published by the Nonprofit Risk Management Center. To speak with a staff member of the Center about any of the topics covered in this article, call (202) 785-3891.