



## **Planning the right privacy policy for you and your visitors**

*Author: Jon Garon, Dean, Hamline University Law school*

Over the past few months, demands for increased privacy regulation have taken center stage as increasingly private transactions move to the Internet. According to The New York Times, the Clinton Administration plans to impose privacy regulations on health care information in the waning weeks of his presidential term. Companies are faced with renewed pressure to update privacy policies as tracking technologies change and consumer concern grows.

Privacy policies are not generic and must be tailored to the industry and to the activities promoted at the Web site. Nonetheless, there are certain basic principles that all policies should follow.

### **Elements of the policy**

Any business Web site that gathers demographic information is well served to adopt a comprehensive privacy program. The FTC has identified five core components of such a program. They are: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." These five steps do not limit the ability of a company to collect demographic or market data. Instead, the policy serves to reflect the activities in an accurate manner.

- Notice. The notice should be written in plain English, for quick consumer understanding, designed to explain the types of data that is collected by the Web site and how the information might be used. This should include who is collecting the data, how the data will be used and what choices the consumer has regarding this data. Post a highly visible link to the privacy policy Web page on the Web site home page, using large fonts, contrasting colors and other features that make the required link to the policy stand out.
- Consent. The policy should allow users to choose whether or not to provide the data. For most business organizations, the decision not to provide personal information should not eliminate the person from participation in at least some of the Web site's services. For some activities, such as chatrooms and listservs, the ability to monitor and control the users require that personal contact information be collected by the organization. If information is being collected only for control purposes, then the policy should explain how the information would be used, as well as how the use of the information will be limited.

- Access. Access refers to the user's ability to review the information provided and insure that it is correct. The FTC states that to be meaningful, "access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients."
- Integrity. Business organizations generally recognize the value of the data they have collected in their membership lists. The value of this data is directly proportional to the security of that information and the accuracy of its content. Outdated, inaccurate information should be destroyed. Reasonable steps should be taken to protect the confidentiality of the data. And to the extent that data is used for demographic study, personal identification should be removed from the statistical profiles. In many instances, for example, use of zip codes provide all the geographic specificity necessary for a business's study of usage and trends. Using names and addresses to study the neighborhood living habits will slow the process while risking the confidentiality of individual privacy as multiple participants to the study share the data. Increasingly, the public is voting with its feet by refusing to associate with sites that sell individually identifiable information to commercial trackers.
- Enforcement. The FTC does not actively advocate that privacy policies be enforced through operation of law. Outside the arena of children, such enforcement has not been statutorily granted. Nonetheless, the FTC can take action against intentional violations of a posted policy by treating those acts as deceptive trade practices. The preferable enforcement mechanism is through membership in a trade association that verifies the credibility of the privacy policy. Third party enforcement relationships can be established with organizations such as the Better Business Bureau Online, Entertainment Software Rating Board, TRUSTe or the DMA Privacy Promise.

The privacy policy must also be tailored to the particular company and industry. Information may be treated differently if required for particular uses rather than voluntarily given as part of customer surveys or transactions. Those differences should be stated in the privacy policy. For example, Web sites with chatrooms generally require personal information on the posting parties so that the rights of others in the chatrooms can be protected. Customers who understand their choices cannot accuse a company of being misled, and are often much more highly satisfied because they received what they expected. Customers are also willing to give personal information when it is to receive a service they value.

A comprehensive privacy policy, once adopted, will have the force of contract against the company publishing the Web site, unless its terms limit the scope. As a contractual right for the user, the policy will have some legitimacy; as an altruistic statement ignored in operation, the policy could result in significant liability.

## **Enforcement of privacy policies**

Following the guidelines of the FTC provides only the first step in creating a valid privacy policy. No matter how well intended, a privacy policy provides no protection to a company or the public unless it is followed. To the contrary, failure to follow a policy once adopted and published to the public may result in liability for breach of contract or for allegations of deceptive trade practices. For example, GeoCities, a popular Web site for virtual communities, was forced to settle with the FTC after being accused of deceptive trade practices. The FTC received complaints from GeoCities members who were receiving unauthorized solicitations despite a privacy policy that stated "[GeoCities] will not share this information with anyone without your permission."

In addition to FTC action, companies face tremendous public pressure to comply with their stated disclosure policies. Companies like Microsoft, eToys.com and Amazon.com have come under intense scrutiny for misuse - and sometimes merely aggressive use - of the detailed customer information. The first lesson is that the policy must be drafted with enforcement in mind. An absolute guarantee is probably unwise. "Never" is a long time in the Internet age, so a promise that data will never be shared - no matter how well intentioned - is probably unwise. "Never" may also imply a guarantee against inadvertent disclosure, hacker attacks and future business transactions. These are guarantees that few, if any, businesses are willing to make.

A company must also know what it has agreed to do. If a business has outsourced its Web site to a third party host, then Web site traffic information, demographic information and personally-identifying information may have been sold as part of the contract between the business and its Web site host. The privacy policy must be accepted and respected by a company's ISP, data storage provider, software designers and anyone else who has access to business' data as a result of a professional relationship with that company. Every agreement with third parties should include an express provision obligating that party to enforce the privacy policy as it exists now and as it may be amended.

Another lesson is that things change. Include a statement in the policy that it may change from time to time, advising the consumer to review the privacy statement page on a regular basis. Similarly, while it is courteous and good business practice to put a notice on a Web site that announces changes to policies, do not make this notice a contractual obligation or make it a condition of the new policy going into effect. Good intentions do not always result in good deeds, and no company has been taken to task for doing more than it promised.

Changes to the company must also be anticipated. Proposed mergers between companies with differing privacy policies may give rise to regulatory challenges. Similarly, bankruptcy courts are beginning to balance the creditors' interest in assets of the corporation with the stated privacy rights of the consumers in the database. In a bankruptcy proceeding involving Toysmart.com, the FTC, 40 states' attorneys general and counsel for TRUSTe wrangled over the rights involved in the customer data. Ultimately, the settlement required that the data only be sold as part of a going concern sale of the Web site rather than as a separate asset.

A good privacy policy includes clear, effective notice to the public regarding the activities at the Web site and equally clear obligations that the Web site publisher can reasonably manage. When both the user and publisher of the site can understand the policy, it is a success. If not, it is time to revise the policy.