Discussions in the Privacy Debate

by Nick Nicholas, Return Path

Consumers have begun expressing a high degree of concern about privacy and how their personal information is used. In one survey, privacy was the second most frequently voiced concern by consumers. Education was the only issue consumers thought was more important than privacy; the lack of privacy was more worrisome than the economy or crime!

Marketers should be concerned about the fact that consumers are declining to do business online because of privacy issues. In a recent study of those who had not purchased goods or services online, 90% said concerns about privacy was the main reason they had not done so. Clearly, online marketers must address these issues in order for their businesses to reach their potential.

The most effective way to address consumers' privacy concerns is to write and implement a strong privacy policy. A good privacy policy must cover at a minimum the four elements of fair information practices identified by the Federal Trade Commission: notice, choice, access and security.

The notice principle requires stating what information is collected, how information is gathered, for what purposes the information is gathered, by whom the information is collected, and with whom the information is shared.

The choice principle provides consumers with an opportunity to choose whether their personal information is used for purposes going beyond those specified in the notice provisions. This includes internal secondary uses such as marketing to customers if the information was collected to complete a transaction, and external secondary purposes such as disclosing data to other organizations.

The access principle allows consumers to review any personal information about them which is in the possession of a company, and also permits consumers to correct any mistakes they find.

The security principle requires companies possessing personal information to make sure that unauthorized parties do not gain access to this data. In addition, companies must make sure that the integrity of this data is maintained and is not altered, deleted or otherwise corrupted.

Although the enforcement principle is not explicitly part of the FTC principles of fair information practices, this principle is implicit. The enforcement principle mandates the creation of an effective mechanism for ensuring that a company's privacy practices are in accord with its privacy policies. This is especially important because the Federal Trade Commission has stated that it will take enforcement action against companies whose privacy practices do not follow their privacy policies.

Canada and the countries of the European Union have identified additional principles of fair information practices, and a privacy policy can be strengthened by addressing these additional principles. For example, the secondary use principle permits data to be used only for the stated purposes for which it was collected; any use beyond the stated purposes requires the explicit permission of the consumer. An organization can invoke the secondary use principle with language in the notice provisions of their privacy policies.

The accountability principle requires a company to acknowledge responsibility for the personal information under its control

and to designate someone who is responsible for ensuring that the company abides by its privacy policies. Appointment of a chief privacy officer is an effective way to comply with the accountability principle. The openness principle imposes an obligation to make an organization's privacy policies and practices easily accessible and to provide a mechanism for providing specific information to consumers upon request.

Simply addressing each of the principles of fair information practices is not sufficient. The principles should be applied in such a way that consumer privacy is enhanced, not diminished. For example, it is perfectly acceptable to draft a notice provision stating that the personal information of consumers may be shared or sold at the discretion of the company collecting the information. Such a provision is likely to heighten a consumer's privacy concerns rather than ease them.

A privacy policy should be easily understood. Too often privacy policies are drafted by attorneys using dense, legalistic language which does little to facilitate understanding by consumers. Although privacy policies have legal implications, they are also mechanisms for conveying important marketing messages. An effective privacy policy will strike a balance between a marketing document and a legal notice. To be most effective, a privacy policy should be no longer than a single page.

A frequent mistake is making a privacy policy difficult to find. A link to a company's privacy policy should appear on the home page of its website. Ideally, every page should include a link to the privacy policy; at the very minimum a link to the privacy policy should appear on each page where personal information is collected.

Finally, a privacy policy should not be thought of as a document set in stone. Privacy policies are evolving documents which should be reviewed once every six months and updated to reflect the latest best practices.

Writing a good privacy policy is not a simple matter, but it is easy compared with the difficult part of developing an effective privacy program: implementing the policy. As long as a company "says what it does, and does what it says" it will reduce the challenges of managing an effective privacy program.

It's not just a slogan, it happens to be true: privacy is good business! Businesses that effectively address the privacy concerns of consumers will not only earn their trust but their business as well.

Nick Nicholas
Chief Privacy Officer
Return Path, Inc.
(212) 905-5500
nick.nicholas@returnpath.net