VOL.4 NO.1
Management Accounting Quarterly
Fall 2002

Privacy Protection: The Safe Harbor for E-Marketing

By George Benjamin Thompson, J.D., and Lynda S. Hamilton, J.D.

The United States is urging Internet businesses to adopt Safe Harbor Principles developed by the Department of Commerce in order to align with the European Union's strict Internet requirements and foster the free flow of commerce.

Clients, be they buyers or sellers, demand privacy and confidentiality in their business transactions. They insist that their rights to privacy cover the use, transmission, and storage of personal information, including but not limited to their credit card numbers, addresses, telephone numbers, and buyer preferences. Those who sell goods and services through the Internet had best comply with both government regulations and market forces. Otherwise, consumers will distrust the information technology on which e-commerce depends, and suppliers will not continue to enjoy burgeoning sales.

Breach of privacy comes in many forms. For example, in early 2000, the theft of credit card account numbers from the e-business CD Universe shocked the Internet community. A computer hacker broke into a secure area of that business's server and gathered information on thousands of accounts, demanded a ransom for the return of the account numbers, and published a large portion of the stolen accounts on the Web.[1] In July 2000, the e-business Toysmart.com attempted to sell its database of consumer information that had been accumulated from Internet customers. In its privacy policy, Toysmart.com had promised visitors to its website that customer data would never be shared with another company.

The U.S. Department of Commerce, long an advocate of industry self-regulation, has developed a voluntary set of Safe Harbor Privacy Principles that are compatible with the European Union's regulatory scheme for data privacy. If your company sails into this "Safe Harbor," you can assure your clients, customers, and suppliers that you shelter their personal information from abusive manipulation and distribution.

Market Perspective on e-Commerce Privacy

Although global e-commerce grew to $111 billion in the last decade, privacy protection problems threaten its continued success. A survey by Georgetown University illustrates the large amount of personal information that websites collect from visitors. For example, 92.8% of the sites in the sample collected at least one type of personal identifying information (e.g., name, e-mail address, postal address), and 56.8% collected at least one type of demographic information (e.g., gender, preferences, zip code). At the same time, only 65.9% (238) of the 361 sites in the sample have posted even

one type of privacy disclosure, a privacy policy notice, or an information practice statement.[2]

Recently, the Electronic Privacy Information Center (EPIC) conducted a survey reviewing the privacy practices of the 100 most popular shopping websites. According to the survey, one of the questionable uses of data collection online involves profile-based advertising, also known as online profiling. This technique is used to collect information about online behavior of Internet users and to facilitate targeted advertising. Profile-based advertising relies on "cookies," identifying tags that are stored on the computer of a person who visits a website. These cookies are often placed on computers without the knowledge of individuals when banner advertisements appear.[3] EPIC found that 86 of the e-commerce operations used cookies, and only 35 of the sites had no profile-based advertisers operating on their pages, while 18 of the top shopping sites displayed no privacy policy at all. It was also found that the privacy policies available at many websites are confusing, incomplete, and inconsistent. EPIC concluded that the current practices of the online industry provide little meaningful privacy protection for consumers.[4]

The EPIC survey also raised questions about the ability of e-businesses to self-regulate. For example, only 19 of the top 100 sites were part of an industry self-regulation program, such as TRUSTe or the Better Business Bureau Online. Only 23 of the top 100 offered an opt-in policy, which requires a company to gain consumer permission before any collection or use of personal information. Most U.S.-based sites use opt-out policies, which allow companies to make use of information as they wish unless a consumer notifies the firm that they do not want their personal information collected or used. The Pew Research Center survey, however, indicated that U.S. consumers favor opt-in policies, with 86% of Internet users favoring "opt-in," 54% thinking that tracking is a harmful invasion of privacy, and 27% finding tracking to be helpful. Opt-in policies mirror the types of consumer protections reflected in European Union regulations.[5]

At the same time, the survey concluded that marketers were using new and more sophisticated techniques to track consumers on the Internet. Methods such as profile-based advertising are a sharp departure from traditional business practices, which allowed companies to advertise products and services and still permit consumers to retain some privacy. Predictive software can build a "digital silhouette" to trace a user's habits on the Web.

The next movement in telecommunications seems to be wireless Internet access. Marketers are already trying to use location-finding technology (knowing the location of a cell phone, such as with 911 calls) to market directly to a consumer's hand-held Internet device. EPIC concluded:

"In the online world, every consumer inquiry about a product and every ad viewing may quickly become incorporated into a detailed profile that will remain hidden from the consumer. On balance, we think that consumers are more at risk today than they were in 1997 [when the first EPIC survey was done]. Anonymity, which remains crucial to privacy on the Internet, is being squeezed out by the rise of electronic commerce. Industry backed self-regulation has done little to protect online privacy. We believe that legally enforceable standards are necessary to ensure compliance with Fair Information Practices. And new techniques for anonymity are necessary to protect online privacy."[6]

U.S. Privacy Policy

In matters of e-commerce, however, the U.S. government has maintained a "hands-off" approach to regulation, instead relying on private industry to take the steps necessary to make e-commerce successful and to provide adequate protection for Internet consumers. One of the most visible private-sector efforts toward protection of consumer data was launched as TRUSTe,

an independent, nonprofit privacy organization founded in 1997. TRUSTe's mission is to promote privacy policy disclosure, informed user consent, and consumer education concerning privacy and security on the Internet. The founders of the organization, the Electronic Frontier Foundation and the CommerceNet Consortium, hoped that building consumer trust would accelerate growth of e-business.[7]

Following the lead of U.S. government policy, TRUSTe's philosophy, as stated on its website, is that "government regulation of the Internet would likely be more rigid, costly to implement, and difficult to repeal than an industry-regulated, cost-effective program such as TRUSTe's. Because the Internet is still in its early growth stages, we believe it's too early to impose regulation without understanding the full impact it would have on growth…the government has already shown its willingness to step in quickly if websites don't self-regulate privacy on the Internet effectively."[8]

To help consumers feel more secure, TRUSTe issues its "trustmark" award to websites that comply with established privacy principles, oversight, and consumer resolution processes. A displayed trustmark (see TRUSTe logo) signifies to online users what personal information is being gathered, how it will be used, with whom it will be shared, and whether the user has an option to control its dissemination. Based on such disclosure, users can make informed decisions about whether or not to release their personally identifiable information (e.g., credit card numbers) to the website.[9]

The TRUSTe program has drawn the support of many highly recognizable e-businesses, including America Online, Compaq, Excite, Intel, and Microsoft. During the first year of its existence, many major websites joined TRUSTe's plans, including Yahoo!, Infoseek, and CNET. In October 1998, all major portal websites joined in the Privacy Partnership campaign, an effort to raise awareness of privacy issues. This campaign includes more than 800 sites to-date.[10]

Nevertheless, a recent U.S. government study indicates that industry efforts to promote privacy have not been very effective. In late spring 2000, the Federal Trade Commission surveyed hundreds of major e-commerce sites and found that nearly 90% of the sites voluntarily posted their privacy policies. Only 20% of the sites, however, met basic FTC standards of "fairness" for protecting consumer privacy. The biggest concern of the Commission was the failure of websites to give consumers access to personal information collected by the websites themselves. Although the Commission acknowledged the efforts of private-sector initiatives in limited privacy protection, the survey results became the basis of the FTC's request to Congress for the authority to regulate Internet privacy.

Privacy Policy Across the Pond

In the European Union, strategies to protect the privacy of consumer data have been quite different because the demand for personal privacy is much greater than in the United States In 1995, the European Union's governing body passed Directive 95/46/EC, a directive on the protection of personal data, in an effort to protect the privacy of individuals in Member States using the Internet. By providing strong protection for consumers, the E.U. directive was designed to promote the free movement of personal data among nations of the European Union, increase consumer confidence due to heightened security of data, and help facilitate the growth of e-commerce in Europe.[11] Creation of "dot EU" domain name designation would allow consumers to have confidence that a website has met the demanding privacy criteria of the E.U. and provide businesses with marketing leverage in attracting buyers.

One of the protections of the directive is the regulation of the transfer of personal data to countries outside the E.U. The directive requires Member States to ensure that personal data is only transferred to countries outside the E.U. when its continued protection is guaranteed. When the directive took effect, the European Commissioner for the Single Market, Mario Monti, remarked, "The entry into effect of this directive is good news for both individual citizens, who will enjoy safeguards concerning data held on them, and economic operators, who will benefit from the free flow of information and the boost to consumer confidence."[12]

Perhaps, but it was bad news to U.S. businesses that favored a hands-off approach on data privacy. The difference in philosophy can be traced to the importance placed on personal privacy in Europe. After World War II, most European countries established policies to pro-

tect personal data through constitutional provisions. Article 8 of the European Convention on Human Rights includes the right to privacy.[13] The Data Privacy Directive, founded on these strong privacy policies, attempts to provide consistency in data privacy regulation. Specifically, the directive grants a number of important rights to Internet users. Those rights include receiving information from subsequent data users about where the data originated (where such information is available), the identity of the organization processing data about them and the purposes of such processing, a right of access to personal data relating to him/her, a right to rectification of personal data that are shown to be inaccurate, and the right to opt out of allowing their data to be used in certain circumstances. Further, some sensitive data, such as an individual's ethnic or racial origin, political or religious beliefs, trade union membership, or data concerning health or sexual life, can only be processed with the explicit consent of the individual, subject to a number of exemptions for specific cases such as consent of the data subject or where there is an important public interest (e.g., for medical or scientific research) where alternative safeguards have to be established.[14] Case law of the European Court of Justice provides that all citizens of E.U. nations are protected by the directive, regardless of the state of implementation by Member States.[15]

The most compelling protection given by the directive may be the prohibition of data transference to non-E.U. countries. According to the directive, data concerning individuals from E.U. nations should only be transferred to a non-E.U. country if it will be adequately protected there. Non-E.U. countries are not required to apply the same controls as the E.U., but alternative protections must be adequate as to safeguards and application of rights. Therefore, the ability to block individual data transfer is a major concern for businesses in the United States, where no governmental guarantees exist to protect the transfer of personal data over the Internet.[16]

Development of the Safe Harbor Principles

At present, the E.U. and U.S. recognize that protection of privacy is a significant stumbling block for future e-commerce growth and integration between their markets. Businesses in the United States are not legally required to provide enough protection for personal privacy to meet the safeguards of the E.U. directive. Because of the chilling effect on U.S. businesses that may occur if the directive is strictly enforced, several groups have come forward with compromise positions to avoid conflict between E.U. and U.S. e-commerce rules. The most significant effort to bridge the gap between U.S. and E.U. data privacy policies has been the Clinton Administration's Safe Harbor Privacy Principles. In April 1999, the U.S. Department of Commerce issued the Proposed Principles as guidelines for U.S. e-businesses to meet the privacy protection guarantees of the E.U. directive. If a business upheld the seven principles found in the proposal, the Department of Commerce argued that the requirements to allow data transmission from E.U. Member States were met. The Seven Safe Harbor Principles include:

Notice—requiring an organization to clearly and conspicuously inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

Choice—requiring an organization to offer the opportunity to "opt out" of the use of personal information, or "opt in" to the use of more sensitive personal information (e.g., race, religious beliefs, medical information.)

Onward Transfer—limiting disclosure of personal information to firms that follow the Safe Harbor Principles or their equivalent.

Security—requiring organizations to take reasonable measures to guard against loss or disclosure of personal data.

Data Integrity—calling for only processing personal information relevant to the purposes for which it was gathered.

Access—requiring that individuals must have reasonable access to personal data to correct or amend that data.

Enforcement—providing for clear and readily available

mechanisms to provide remedies to individuals and sanctions for noncompliance.[17]

On July 27, 2000, the European Commission adopted a decision determining that the U.S. Safe Harbor Principles provide adequate protection for personal data transferred from the E.U. U.S. companies have the option to participate in the safe harbor plan but are bound by the Principles once they join the list of safe harbor U.S. businesses.[18] The compromise relies on self-certification by U.S. companies that they are in compliance with the Principles. Because the E.U. government has concerns over the self-certification issue, and because of the perceived weakness of consumer protections in the Principles, the E.U. has reserved the right to reopen the matter.

At present, private businesses that do business in Europe and want to comply with the Safe Harbor Principles can develop their own policies of adherence. Some e-businesses are hiring Big 4 accounting firms to audit privacy practices for consumer confidence, and law firms are organizing safe harbor departments to help U.S. companies comply with the Safe Harbor Principles. Others may become certified with a privacy oversight firm, such as TRUSTe's new E.U. Safe Harbors Privacy Seal Program.[19] It links a registration form to the Department of Commerce, conducts quarterly monitoring and seeding of privacy practices, and provides online and offline Alternative Dispute Resolution. Companies that are certified are entitled to place the TRUSTe E.U. Safe Harbor Privacy Seal on their logo and Web pages, indicating that they are approved to do e-commerce with customers and suppliers in Europe.

In conclusion, it appears that the U.S. and the E.U. want to implement compromise safe harbors, as they call it, across the pond to foster the growth of e-business while assuring Internet consumers that their privacy will be adequately assured. Private companies remain free to choose how they will protect the private personal data of their clients and may demonstrate privacy assurance through certification under privacy oversight groups such as the TRUSTe Safe Harbor Privacy Seal approved by the Department of Commerce. ■

George Benjamin Thompson, J.D., is director, School of Economic Development, and director, Coastal Rivers Water Planning and Policy Center, College of Business Administration, Georgia Southern University, Statesboro, Ga. He can be reached at benjyt@gasou.edu.

Lynda S. Hamilton, J.D., is professor of Legal Studies at the School of Accountancy, College of Business Administration, Georgia Southern University. She can be contacted at lhamilton@gasou.edu.

1 *Wall Street Journal Interactive Edition*, "CD Universe Is Hit by Hacker Who Released Credit-Card Data," January 10, 2000, www.interactive.wsj.com.
2 Georgetown Internet Privacy Policy Survey (visited Sept. 18, 2000), www.privacyalliance.org/resources/gipps_execsummary.shtml.
3 *Ibid.*
4 Electronic Privacy Information Center, "Surfer Beware III: Privacy Policies without Privacy Protection," December 1999 www.epic.org/reports/surfer-beware3.html.
5 *Ibid.*
6 *Ibid.*
7 TRUSTe, "The TRUSTe Story" (visited Sept. 18, 2000), www.truste.org/about/about_truste.html.
8 *Ibid.*
9 *Ibid.*
10 *Ibid.*
11 Council Directive 95/46/EC of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281).
12 Directorate General XV, "Directive on personal data protection enters into effect " (visited Sept. 18, 2000), europa.eu.int/comm/internal_market/en/media/dataprot/news/925.htm.
13 Data Protection Working Party Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on September 7, 1999, europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp26en.htm.
14 Council Directive 95/46/EC of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281).
15 Directorate General XV, "Data protection: Commission takes five Member States to court" (visited Sept. 18, 2000) europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm.
16 *Ibid.*
17 United States Department of Commerce, "International Safe Harbor Privacy Principles" (visited Sept. 18, 2000), www.ita.doc.gov/td/ecom/shprin.html.
18 Directorate General XV, "Commission adopts Decisions Recognizing Adequacy of Regimes in US, Switzerland, and Hungary " (visited Sept. 18, 2000), europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm.
19 www.truste.org/about/about_eu.html#Top