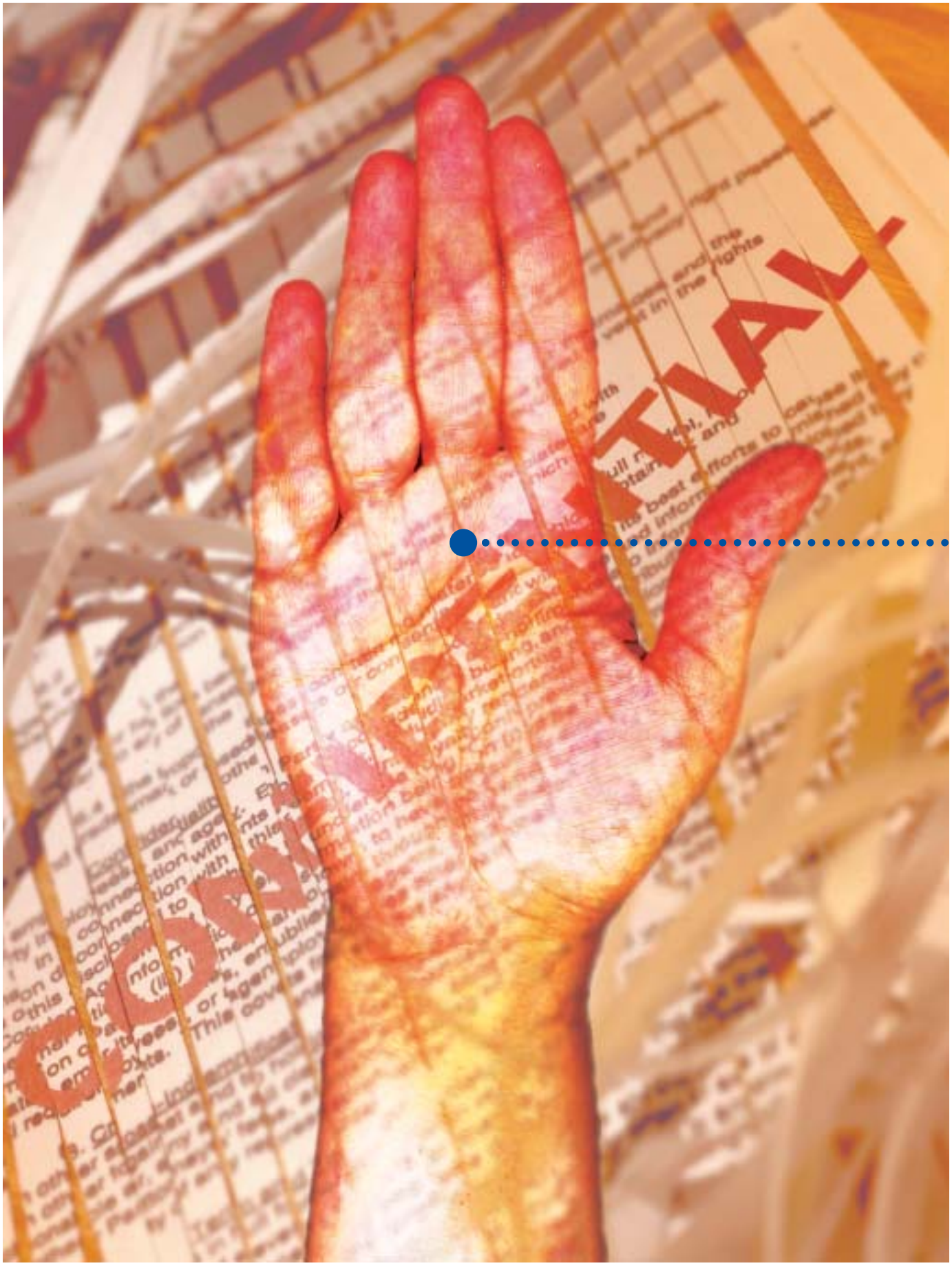

# PRIVACY PROTECTION ON THE INTERNET

By Linda Lee Larson, CPA; Robert K. Larson, CMA, CPA; and Janet Greenlee, CPA

It's Saturday morning, and you're looking forward to a leisurely weekend when you receive an urgent call from the office. Your company has been charged in a $500 million class-action lawsuit for violating customer privacy by selling the names (and other information) of those who have bought goods on your website. Your attorneys say the plaintiffs have a good chance of winning. And you may have even bigger problems with your European Union (EU) customers because of the strict privacy rules in the EU Privacy Directive. Besides penalties, the EU may prevent your organization from even transferring customer data from your own operations in Europe to the U.S.

Sound far-fetched? Well, in the past few years, several organizations have had significant lawsuits filed against them by customers claiming that their privacy was violated. Consumers are becoming increasingly angry when their personal information is used or released without their permission. As a result, new laws and regulations are being introduced that prohibit companies from releasing customer information to third parties without the consumer's express consent.

## CONSUMERS' CONCERNS

**Disclosure:** Consumers are afraid that businesses, including those on websites, will sell personal information to other organizations without their knowledge or permission. In 1999, a California lawyer filed a $500 million class-action suit against RealNetworks, charging that it shared customers' personal financial information with telemarketers in direct violation of its own stated privacy policy.

Prosecution in Minnesota of U.S. Bancorp on similar charges (also in direct violation of its stated privacy policy) led to new U.S. legislation. One section of the Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act) requires that customers of financial institutions must not only be notified before any personal information is disclosed to any nonaffiliated third party, but they must have the opportunity to opt out of any disclosure. But these protections only apply to customers of financial institutions and don't prevent U.S. financial institutions from sharing customers' personal information with their affiliates.

**Security:** Consumers are afraid that businesses and their websites aren't adequately protected against outsiders. In 2000, someone calling himself Maxus hacked his way into the CD Universe website and stole 300,000 credit card numbers. When his attempts to blackmail CD Universe for $100,000 failed, Maxus posted 25,000 of these credit card numbers on his website, leading to untold lost business and mass cancellation of credit cards. The website was promptly shut down.

## HOW IS PRIVACY PROTECTED?

**United States.** In the U.S., the protection of an individual's information is governed by laws, court rulings, and self-regulation. While laws now cover financial institutions, in practice, a consumer's privacy is protected primarily by the goodwill of businesses. Most recent privacy concerns have centered on the Internet.

To address privacy on the Web, several organizations have set up website certifications and privacy seals, and many businesses have posted one or more of these seals on their websites. TRUSTe is by far the most popular Web privacy seal. At year-end 2002, the websites of more than 1,500 organizations displayed the TRUSTe seal, including Netscape, IBM, Yahoo!, Microsoft, AOL Time Warner, Adobe, and Disney. Another popular program is the Better Business Bureau's (BBB) Online Privacy Program (with seals on 706 company sites as of April 2003). The AICPA also has an Online Privacy Program (and

## VOLUNTARY PRIVACY SEALS

**TRUSTe Privacy Seal** (www.truste.org)
A third-party oversight seal program sponsored by a nonprofit organization.

Overall goal: Give consumers control over their personal information online.

Requirements to display TRUSTe seal:

- Post privacy statement on website disclosing
  - Type of information gathered.
  - How the information will be used.
  - How the information will be shared.
- Agree to cooperate with initial and periodic reviews.

Better Business Bureau (BBB) Online Privacy Program (www.bbbonline.org)

- Awards seals "to online businesses that post online privacy policies that meet the required 'core' principles, such as disclosure, choice, and security."
- "Provides consumer-friendly dispute settlement."
- "Monitors compliance through rigorous requirements for participating companies to undertake, at least annually, an assessment of their online privacy practice."

AICPA/CICA WebTrust Program for Online Privacy (under WebTrust) (www.aicpa.org)
WebTrust was developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants "assuring" that e-commerce sites meet the standards of consumer information protection, transaction integrity, and sound business practices.

- The WebTrust Privacy Principle:
  The entity discloses its privacy practices and maintains effective controls to protect personally identifiable information obtained as a result of electronic commerce.
- Meet or exceed the EU Privacy Directives and the Online Privacy Alliance (OPA) Guidelines as of October 1999, and the U.S. Safe Harbor Privacy Principles issued July 21, 2000.
- As of July 2002, the AICPA established a separate Task Force to address Enterprise Wide Privacy issues.

Principle) as part of its WebTrust seal program. (See "Voluntary Privacy Seals.")

But critics have pointed out that organizations sponsoring these privacy seals are largely self-regulated. For example, both RealNetworks and U.S. Bancorp had posted privacy seals on their sites. Although TRUSTe did conduct an audit of RealNetworks once the violations were reported, certifying organizations rely on members' self-compliance.

Another problem is confusion about privacy seals and what they mean. For example, the Better Business Bureau's Online Reliability Program sounds like it might be a privacy seal, but it has nothing to do with privacy protection. Actually, it's similar to the traditional BBB program designed to "help web users find reliable, trustworthy businesses online, all via voluntary self-regulatory programs that help avoid government regulation of the Internet." The BBB program that specifically addresses online privacy is called the BBB Online Privacy Program.

In 2000, the Federal Trade Commission (FTC) issued "Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress." It surveyed two basic groups: a random sample of all websites and the 100 busiest sites. The FTC reported that only 20% of the busiest websites surveyed had implemented all four of the so-called fair information practices—notice, choice, access, and security. Of the most popular U.S. websites, 42% had implemented, at least in part, each of the four principles. The FTC also reported that only 8% of the sites in the random sample displayed any type of privacy seal. The report concluded that privacy legislation in conjunction with self-regulation was needed to ensure consumer privacy. (For details, go to http://www.ftc.gov.)

Industry groups such as the On-Line Privacy Alliance have vigorously lobbied against increased government regulation in this area, claiming that the current self-regulatory environment is adequate. Critics have questioned the ability of these groups to properly monitor the industry and suggest that the privacy seals may be no more than marketing ploys to lull consumers into a false sense of security.

Also in 2000, the FTC voted 4-1 to endorse a new self-regulatory plan submitted by a group of Internet advertising companies called the Network Advertising Initiative. The plan, which took effect immediately, requires Web advertising firms to tell consumers about their Internet profiling activities and to give customers the opportunity to choose whether data regarding their Web activities can be collected. But the plan is voluntary, and not all Web advertisers have agreed to abide by it. Moreover, the FTC realizes that legislation should still be enacted to enforce privacy rules on the Web.

## EUROPEAN UNION DIRECTIVE ON DATA PROTECTION

Applies to all businesses with operations in EU countries and those trading with EU countries. Some believe it may also apply to U.S. websites with EU customers.

Protected information:

- Demographics
- Finances
- Health
- Political Affiliation and Political Opinions
- Race or Ethnic Origin
- Religion

Individual rights:

- To know the protected information possessed by the organization.
- To have erroneous protected information corrected.
- To "opt out" of the distribution of any protected information for direct marketing purposes.
- To "opt in" to allow the distribution of any "sensitive" information.

The complete text of the EU directive is at: http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html

**Europe.** Historically, Europeans have been much more concerned about privacy issues than Americans, and most European countries have enacted very specific and strict laws designed to protect their citizens. European concerns culminated in the EU Privacy Directive, which was passed in 1995 and became effective in 1998.

The EU Privacy Directive has important implications both for companies engaged in e-commerce and for multinational corporations with offices in EU countries. It's based on the idea that collecting and using personal information infringes on the fundamental right to privacy. The directive covers a wide variety of data that might be transmitted during the normal course of business.

Although the directive officially covers only personal data, it defines that to mean "any information relating to an identified or identifiable natural person." (See "European Union Directive on Data Protection," p. 51 for examples.) Organizations that want to trade in EU countries must guarantee that personal information is processed fairly and lawfully; that it's collected for specified, legitimate purposes; is accurate and up-to-date; and is kept only for the stated purpose and nothing more.

Substantial rights are given to individuals regarding the information that organizations possess about them. Individuals must have access to any personal information collected, and any mistakes must be corrected. More important, individuals may prohibit the use of their personal information for marketing purposes.

One recent study suggested that the EU Privacy Directive impacts numerous parts of an organization's records. A partial list of business functions includes human resources, call centers, customer service, payment systems, sale of financial services to individuals and business, personal and corporate credit reporting, as well as accounting and auditing.

Under the directive, transfers of personal data to countries outside the EU can be made only when there is an adequate level of privacy protection unless individuals expressly consent to the transfer. All forms of transmission are covered, including electronic and hard copy. In the EU's initial analysis, the U.S. wasn't listed among those countries seen as adequately protecting the privacy of personal data.

In response to this concern, the U.S. entered into negotiations with the EU to ensure the free flow of information internationally. After Department of Commerce approval, in 2000, the member states of the EU unanimously voted to approve the U.S.-proposed International Safe Harbor Privacy Principles. While not eliminating the EU rules, the agreement establishes a "mechanism, which, through an exchange of documents, enables the EU to certify that participating U.S. companies meet the EU requirements for adequate privacy protection." Almost 250 organizations are now on the Department of Commerce's Safe Harbor List. (See "International Safe Harbor Privacy Principles.")

A major difference between standard practice in the U.S. and EU, including the Safe Harbor Privacy Principles, is in how individuals may opt out. In many cases, before sensitive information can be used or disclosed to third parties, the organization must get permission from the individual in an affirmative or explicit opt-in choice. Sensitive information includes medical and health information, information that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership,

## International Safe Harbor Privacy Principles

(For Compliance with EU Privacy Directive)

| | |
|---|---|
| NOTICE | An organization must give conspicuous notice when it collects information, state how it's to be used, and describe the type of third parties to which the information may be disclosed. |
| CHOICE | Individuals must be allowed to opt out of whether their personal information is used for other purposes by the organization and whether it can be disclosed to third parties. For sensitive information, individuals must be given an explicit opt-in choice. |
| ONWARD TRANSFER | An organization may only disclose to third parties information consistent with the notice and choice principles. |
| SECURITY | The organization must establish reasonable security over the personal information gathered. |
| DATA INTEGRITY | An organization should take reasonable steps to ensure that the personal data collected is accurate, complete, and current. |
| ACCESS | Individuals must have reasonable access to the personal information compiled on them and be able to correct any errors found. |
| ENFORCEMENT | Mechanisms must be established to give individuals recourse if complaints and disputes occur. Penalties must be established for organizations that do not comply with these principles. |

The full text is on the U.S. Department of Commerce website at: http://www.ita.doc.gov/td/ecom/shprin.html.

The Safe Harbor website is at: http://www.export.gov/safeharbor.

or information concerning the sex life of an individual. Under U.S. rules and practices, U.S. organizations often transfer a great deal of this kind of information without getting opt-in or affirmative permission. U.S. organizations with affiliates operating in the EU need to make sure they are following the stricter EU privacy rules.

## WILL TECHNOLOGY PROVIDE THE SOLUTION?

Technological solutions are emerging. The most noteworthy is the World Wide Web Consortium's (W3C) Platform for Privacy Preferences (P3P) standard. The P3P is a standardized method for websites to encode their privacy policies in a computer-readable format. P3P advocates claim that, with such tools, users can more easily control the use of their personal information. For example, if a site wants to collect data for marketing, under the standard the user should receive a warning and the option to leave. Users will also see warnings when encountering sites without privacy statements. Such software tools are designed to give Internet users more control over the amount of personal information they disclose online. (More information about W3C or P3P is at www.w3.org.) Microsoft's Internet Explorer 6 browser was the first consumer software to incorporate P3P.

But P3P will only work if most websites voluntarily participate. In addition, the Electronic Privacy Information Center (EPIC) issued a critical report in 2000 titled "Pretty Poor Privacy," where it called for further improvements in P3P. (The report is at http://www.epic.org/reports/prettypoorprivacy.html.)

Another way to ensure online privacy is with encryption. Encryption is especially important when users give a credit card number online. When it's used, data sent is protected from unauthorized third parties.

More advanced technological safeguards are needed now. A 2001 survey of computer security practitioners found that 40% stated that they had detected outsiders trying to penetrate their network systems.

## THE FUTURE: MORE GOVERNMENT REGULATION?

During the last several years, dozens of bills concerning the protection of privacy have been introduced at both the federal and state levels. Currently, the Online Privacy Protection Act of 2003 (H.R. 69) is being considered by the U.S. Congress. For information on the status of proposed federal privacy legislation, visit EPIC's Bill Tracking Site (http://www.epic.org/privacy/bill_track.html). Various industry groups are lobbying against government regulation of privacy, and, as a result, such federal legislation isn't expected to pass until at least next year.

Even without new federal regulation, the FTC is becoming more active regarding privacy protection on the Internet. For example, several consumer groups, led by EPIC, filed a complaint against Microsoft in 2001. In July 2002, the EU authorities' Internet Task Force issued a strongly worded statement criticizing several features of Microsoft Passport that may violate EU privacy laws. In August 2002, Microsoft Corporation settled FTC charges concerning "the privacy and security of personal information collected from consumers through its Passport Web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services." (See www.ftc.gov/opa/2002/08/microsoft.htm.)

## IMPLICATIONS FOR BUSINESSES

All businesses must now take consumer privacy seriously. This will require investing resources to secure databases and websites. Organizations should also determine if their insurance covers lawsuits that may arise over privacy issues. In the very near future, all organizations with an online presence will need to establish online privacy statements certifying that they comply with legislated privacy standards.

U.S. corporations with operations in the EU must comply with the EU Privacy Directive through the use of the Safe Harbor Agreement. Ignoring these rules might put a U.S. corporation in the awkward position of not being able to access its own records from the EU, either in electronic or hard copy form. While many predict that the U.S. will have strict privacy laws in the near future, for corporations doing business in EU countries, the future has already arrived! ■

*Linda Lee Larson, DBA, CPA, CIA, CISA, is an assistant professor of accounting at the College of Business, Ball State University, Muncie, Ind. You can reach her at LLLarson@bsu.edu or (765) 285-5118.*

*Robert K. Larson, Ph.D., CPA, CMA, is an associate professor of accounting at the University of Dayton School of Business Administration, Dayton, Ohio. You can reach him at Robert.Larson@notes.udayton.edu, or (937) 229-2497.*

*Janet S. Greenlee, Ph.D., CPA, is an associate professor of accounting at the University of Dayton School of Business Administration, Dayton, Ohio. You can contact her at Janet.Greenlee@notes.udayton.edu, or (937) 229-4790.*