



Legal View

by Linda Pickering and
Vanessa A. Ignacio
Lowenstein Sandler PC

A review of Internet privacy issues at the end of the first quarter of 2001 reveals a landscape littered with area-specific privacy legislation and regulation, private litigation, international laws and rules, and numerous bills

If Your Business Has a Website, It Needs a Privacy Policy

pending in Congress. Just about daily, new developments crop up in the area of Web privacy.

All the activity centers around the collection and use of "personally identifiable information." Personally Identifiable Information ("PII") refers to any information that identifies or can be used to identify, contact or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, social security number and credit card information. PII does not include information that is collected anonymously (i.e., without identification of the individual user) or

demographic or aggregated information not connected to an identified individual.

Internet privacy has not seen comprehensive federal regulation - yet. The federal government has stepped in, however, to regulate online privacy in a few narrow areas: children, medical records and financial data. The Children's Online Privacy Protection Act ("COPPA") imposes a complex set of regulations on Web sites collecting PII from children under 13 years of age. The Health Insurance Portability and Accountability Act ("HIPPA") imposes substantial restrictions and penalties regarding the use of medical data. Finally, the Gramm-Leach-Bliley Act ("GLB Act") prevents financial institutions from sharing non-public personal information, such as a customer's loan payment history or account information, with nonaffiliated third parties.

Pressure is building in Congress to regulate Internet privacy more widely. Private lawsuits and complaints have increased as Web consumers remain dissatisfied with current levels of protection for PII and gain more awareness of privacy concerns. Federal Trade Commission (FTC) enforcement actions are on the rise. Business communities are pressuring one another to create and maintain industry-wide standards. In fact, influential technology companies such as IBM, AT&T and Microsoft have added "privacy officers" to their staffs to reinforce their

commitment to online privacy. As part of the self-regulation wave championed by private industry, organizations such as TRUSTe and BBBOnline have developed independent compliance programs that award their "seals" of approval to privacy-friendly sites.

Yet, when the FTC last looked at the use of privacy policies by business, it found many companies still had not developed policies. In a recent flurry of activity, members of Congress have introduced bills targeting, among other things, Internet privacy. As of the end of March, more than a dozen bills relating to Internet privacy had been introduced in the House or Senate. The threat of data collection and use laws on the horizon is a palpable one.

Muddy Waters: What Is the "Safe Harbor"?

Not only must U.S. e-commerce firms keep afloat of the laws, regulations and private actions on this side of the Atlantic, but they must deal with added pressure that is coming from the European Union. While the U.S. takes a targeted approach that includes a mix of legislation, regulation and self-regulation, the EU relies on its Privacy Directive, comprehensive legislation that imposes strict requirements on the collection, use and disclosure of PII by businesses in the EU.

In 1998, the U.S. began negotiating a "Safe Harbor" agreement with the EU in order to ensure the continued transborder flow of personal data. The negotiated Safe Harbor allows U.S.

companies to voluntarily pledge to follow a set of principles regarding the handling of personal data originating from the EU. The Safe Harbor requires that organizations that receive PII from any EU state demonstrate that they provide "adequate" privacy protection, as defined by the EU Directive on Data Privacy. An organization can qualify for Safe Harbor protection by either 1) joining a self-regulatory privacy program that adheres to the Safe Harbor's requirements; or 2) developing its own self-regulatory privacy policy that conforms to the Safe Harbor.

This year's shift in power in Washington may result in the U.S. drifting away from the Safe Harbor. Responding to concerns voiced by the financial services sector, the Bush administration has objected to a set of proposed European Commission privacy rules affecting trans-Atlantic e-commerce. The Commerce and Treasury Departments have said that the proposed rules "impose unduly burdensome requirements that are incompatible with real-world operations." Very recently, an industry coalition including IBM Corp., Ford Motor Co. and Procter & Gamble Co. announced plans for a \$30 million national advertising campaign aimed at easing consumers' privacy fears and pointing out the costs of privacy regulation. For example, the coalition reported that catalog companies would have to raise prices by a total of \$1 billion if they were not free to use customer information for marketing purposes.

Implement a Privacy Policy Now

In all this confusion, one message is clear: Every business that has a Web site should have a privacy policy, and a statement of that policy on the site. Development of company-wide data collection practices, including notice and disclosure of such practices to consumers, is critical to establishing and maintaining consumer confidence and

remaining a viable presence in the online marketplace, regardless of where Congress, the FTC and state legislatures eventually come to rest on this issue.

E-businesses with inadequate privacy policies are subject to attack from several fronts. Although the law in this area is unsettled and developing rapidly (as of this writing, the Bush administration is objecting in part to the EU directive), e-commerce firms should expect that they will at some point be subject to regulations consistent with the FTC report and European Union Privacy Directive. All companies with an online presence must take steps to protect themselves now by establishing appropriate data collection and use practices and implementing a well-crafted privacy policy.

Are All Privacy Policies Created Equal?

Before your company considers surfing over to a competitor's Web site to copy its privacy policy, think again. To develop a Web site privacy policy that makes sense for your business, stop to consider your company's actual data collection procedures. Ask "What information do we collect? For what pur-

pose?" Keep in mind that use of personal information inconsistent with a company's published privacy policy may result in enforcement actions by the FTC and/or state attorneys general, as well as class action lawsuits by private individuals. Clearly, the privacy policy your company adopts must reflect the actual information gathering and dissemination practices of your Web site with respect to personally identifiable information. A privacy policy is fact-specific - no single statement will work for every site.

What Should a Privacy Policy Include?

Once your business has defined its PII use and dissemination needs and practices, you are ready to implement a privacy policy that works for your particular business. But what should an effective privacy policy include? Several important guidelines are available.

In 1998, the FTC filed a report to Congress concerning the fair use and dissemination of personal information. The core principles of a privacy policy as advocated by the FTC include notice, choice, access and security. The four pillars of the FTC recommenda-

Some online-privacy bills introduced in 2001

HR 89 Online Privacy Protection Act of 2001: To require the Federal Trade Commission to create regulations to protect the privacy of personal information. Sponsor: Rep. Rodney P. Frelinghuysen (R-NJ)

HR 112 Electronic Privacy Protection Act: To prohibit the making, sale or use of an information-collection device without proper labeling or notice and consent. Sponsor: Rep. Rush D. Holt (D-NJ)

HR 237 Consumer Internet Privacy Enhancement Act: To protect the privacy of consumers who use the Internet. Sponsor: California Rep. Anna G. Eshoo (D-Atherton)

HR 347 Consumer Online Privacy and Disclosure Act: To require the Federal Trade Commission to create regulations to protect the privacy of personal information collected from and about individuals on the Internet. Sponsor: Rep. Gene Green (D-TX)

HR 583 Privacy Commission Act: To establish the Commission for the Comprehensive Study of Privacy Protection. Sponsor: Rep. Asa Hutchinson (R-AK)

tions seek to: 1) give consumers notice of an e-commerce firm's information practices; 2) allow consumers choice with respect to the use and dissemination of information collected from or about them; 3) give consumers access to information that has been collected about them; and 4) make certain that the data collector takes appropriate steps to ensure the security and integrity of any PII collected.

The following is a closer look at each of the four main elements of a privacy policy:

- **Notice** - The core of an effective privacy policy is notice. The consumer needs to know the information practices of a company in order to make an informed decision as to what personal information the consumer will disclose. Web sites should inform visitors in a clear way what information is collected and how it will be used. For example, inform visitors if your site collects cookies. The policy should also inform the consumer whether the information is disclosed to third parties as well as whether other entities, such as advertisers, are collecting information through the Web site.

- **Choice** - A comprehensive privacy policy informs consumers of what choices they have regarding the collection, use and dissemination of their personal data. Web sites typically employ "opt-in" or "opt-out" provisions. With an "opt-in" system, a Web site may retain or distribute a visitor's information only if that person explicitly grants the site permission. Conversely, with an "opt-out" provision a Web site may use information unless a site user affirmatively opts-out of such use.

- **Access** - Privacy policies should provide consumers reasonable access to the information collected and allow an opportunity to review information and correct inaccuracies.

- **Security** - Reasonable measures should be in place to protect the security of the information collected.

An effective self-regulated privacy policy will include aspects from the FTC guidelines, the policies of the seal organizations and the principles of the EU Privacy Directive. Such a comprehensive policy will help keep legal issues at bay, raise customer confidence levels and expand business opportuni-

ties. Note that U.S. organizations that certify to adhere to the Safe Harbor must state so in their published privacy policy statements.

The Fifth Element- Enforcement

It is important to understand that when companies claim they are abiding by privacy practices and then fail to do so, they may be liable for fraud and subject to action by the FTC as well as by private parties. Businesses must adhere to and enforce their stated privacy practices and policies. The threat of FTC action, private lawsuits and enforcement of the EU Privacy Directive - not to mention potential public relations disasters - require that careful attention be given both to the design of information practices as well as implementation and compliance with those practices.

Linda Pickering is of counsel and Vanessa A. Ignacio is an associate in Roseland-based Lowenstein Sandler's Internet & Technology Group.

Reprinted from the May 2001 issue of COMMERCE magazine.