

PRIVACY ON THE WEB: AN EXAMINATION OF USER CONCERNS, TECHNOLOGY, AND IMPLICATIONS FOR BUSINESS ORGANIZATIONS AND INDIVIDUALS

Eric C. Turner and Subhasish Dasgupta, Ph.D.

Individual privacy concerns significantly affect consumer willingness to engage in electronic commerce over the Internet. This article explores privacy concerns associated with the implementation of new information technology and introduces a new concept termed the “information technology privacy cycle.” This article also examines individual privacy on the Web, including technologies employed for collecting and protecting information on the Web, and the success of legal and technical remedies. Also assessed is the future potential of technology-based solutions through a focused examination of the Platform for Privacy Preferences as well as a discussion of the practical and theoretical implications for business organizations and individuals.

ERIC C. TURNER *is at the Management Science Department at George Washington University in Washington, D.C. He can be reached at turnere@frb.gov.*

SUBHASISH DASGUPTA, Ph.D., *is at the Management Science Department at George Washington University in Washington, D.C. He can be reached at dasgupta@gwu.edu.*

IN 1997, DAVID CHAUM, FOUNDER OF DigiCash, identified three technical barriers to the continued widespread adoption of electronic commerce on the Internet, including ease of use, access to the hardware needed to participate, and privacy.¹ Privacy concerns remain a significant inhibitor preventing more extensive use of the Internet for conducting business-to-consumer (B2C) E-commerce. Privacy pertains to the protection of information about individuals, transactions, or organizations. Web user information is a valued commodity that provides business organizations

with a means to more effectively target and segment its market. Sellers of information goods find it advantageous to segment their markets based on observable characteristics or revealed consumer behaviors that can be used to increase profits.² Recent revelations about the controversial information-gathering capabilities and sharing policies of firms conducting business over the Internet have heightened public interest in privacy. In 1999, DoubleClick Inc. became a target of privacy advocates and lawsuits for collecting and selling information on individual Web surfing habits merged with

Information technology will continue to redefine organizational practices and business models with respect to privacy.

information from other databases to identify users by name and create online customer preference profiles.³ RealJukeBox was identified as tracking information, including name, e-mail address, musical preference, and the number, format, and quality of recordings stored on user hard drives and selling it for profit. In 2000, U.S. Bancorp paid a \$7.5 million fine to settle one lawsuit, agreed to stop sharing customer account information, including credit card numbers, account balances, and Social Security numbers with unaffiliated, nonfinancial third parties to settle yet another suit, and still has several other privacy lawsuits pending.⁴ Users of the Internet are subject to increasing amounts of unsolicited and unwanted e-mail marketing material from companies that in some cases they have not had a previous business relationship. Negative reaction to these practices serves to constrain the growth of Internet E-commerce by damaging the trust necessary for encouraging a reluctant public to shop online. A year 2000 poll shows that 63 percent of U.S. online users who have never made a purchase were very concerned about the use of personal information and 92 percent not very comfortable with having their information shared with other organizations.⁵

In response to public concern, various countries have implemented varying degrees of privacy legislation designed to regulate how companies access and utilize information on potential customers. The United States to date has had a relatively business-friendly, minimal-intervention approach encouraging organizations to provide self-regulated privacy protections. By contrast, the European Union (EU) has taken a pro-consumer approach with stringent regulations banning the use of personal information until consent is received. The perceived failure of U.S. regulatory initiatives to address the concerns of a majority of the Web population indicates that perhaps a technology-based approach to addressing the privacy problem offers promise. The effective mitigation of privacy issues will improve consumer willingness to shop on the Web, thus improving revenue for online business initiatives and facilitating future growth in the international E-commerce marketplace. Information technology will continue to redefine organizational practices and business models with respect to privacy.⁶

This study of privacy focuses on the concerns associated with the collection of informa-

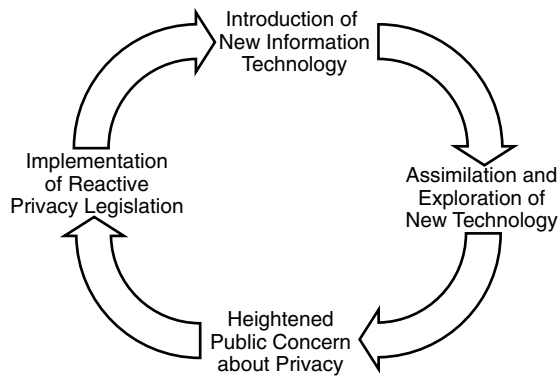
tion from individuals, knowingly or unknowingly, based on voluntary Internet usage as opposed to privacy issues arising from the intentional hacking or gaining of unauthorized access to information sources or repositories for criminal or malicious use. Research conducted by Straub and Collins³ provides a comprehensive discussion of the privacy implications of unauthorized access to personal information resulting from a security breach. Privacy issues arising from organizational monitoring of employee e-mail, Internet and telephone usage are also not specifically addressed within the scope of this article.⁷ This article examines the issue of organizations collecting, monitoring, mining, and in some cases distributing what some consider personal information based on the behavior of individual users of Web sites. The following sections address the definition of privacy, the nature of individual privacy concerns, and how these concerns manifest themselves in B2C E-commerce on the Internet. We briefly discuss various regulatory approaches taken and examine the specific technologies used to monitor Web usage and protect privacy, including the Platform for Privacy Preferences (P3P) initiative. We assess the advantages, disadvantages, and future potential of technology-based solutions using the P3P initiative as a vehicle to examine the potential of privacy-enhancing technologies and implications for business organizations and the individual.

PRIVACY

Definition of Privacy

Although there is no universally accepted definition, privacy can be articulated as the need to secure for the individual "the right to be left alone" or as the "state or condition of limited access to a person."^{8,9} A classic definition describes privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.¹⁰ Three key elements of information privacy include separateness, restricted access, and beneficial use. Separateness is defined as the ability to describe the boundaries and ownership or access rights to information. Restricted access refers to the ability to protect the identified data, and beneficial use implies that only data owners or parties explicitly authorized to receive the information are able to benefit from its use.¹¹

EXHIBIT 1 The Information Technology Privacy Cycle



The Information Technology Privacy Cycle

Historically, the rapid introduction of new information technologies with enhanced capabilities for surveillance, storage, retrieval, and communication of personal information sets off a cyclical chain reaction of events that is conceptualized as the information technology privacy cycle (see Exhibit 1). An information technology privacy cycle begins with the introduction of new technology that augments the ability of individuals and organizations to collect data about people and their behavior.¹² As more organizations begin adopting, assimilating, and exploiting the technology, public concern starts to emerge and the technology is perceived as a threat to individual privacy.¹³ In turn, this heightened public anxiety puts increased pressure on governments to react, generally resulting in the passage and implementation of new privacy laws and regulations. Inevitably, new information technologies are developed that beginning another information technology privacy cycle that continues to repeat itself as new information technologies are introduced. This concept is illustrated in the sections below.

Privacy in the Information Age

The advent of mainframe data processing in the 1960s provided mostly large organizations with a means to obtain, store, and manipulate information in a centralized manner that up until that time was not possible.¹⁰ As mainframe computer technology was assimilated into mainstream business and governmental organizations, users of the technology began exploiting the massive computing and storage capabilities to create databases of information

on individuals, much of it considered personal. The explosive growth of the multibillion dollar direct marketing industry, for example, was facilitated by the availability of large commercial databases compiled from public information, including motor vehicle and real estate records, telephone and other directories, or from responses supplied by consumers on warranty cards and other surveys. The new capabilities also allowed profiles of individuals to be created to assist firms in credit decisions. The resultant public anxiety led to the passage of the Fair Credit Reporting Act in 1970 and the Privacy Act of 1974, which defined the rights of individual citizens and outlined the U.S. Government's responsibility for protecting the personal information it maintains.¹⁴ Although this legislation has been in place for approximately 30 years, fair credit reporting and government release of information remains a concern of consumers today.

Privacy in the Network Age

Continued technological breakthroughs in the mid-to-late 1980s, including the personal computer, workstations, and communications networks, enabled even broader diffusion of database management, marketing, and telemarketing tools. Individuals and small organizations now had the computing capability to manipulate and store information that before required access to a mainframe. Further, new networking capabilities provided the ability to more easily distribute and share information with other organizations and individuals. The resultant resurgence in the public's interest in privacy led to the passage of two additional pieces of legislation that addressed network age privacy issues not covered in the Fair Credit Reporting and Privacy Acts. The Electronic Communications Privacy Act (ECP) of 1986 prohibited unauthorized interception and alteration of electronic communications and made it illegal for online services to disclose personal information without a warrant. The Computer Matching and Privacy Protection (CMPP) Act of 1988 regulated the use of computer matching of federal records subject to the Privacy Act except for legitimate statistical reason.¹⁴ The collection, storage, and distribution of sensitive information continued to raise public apprehension regarding the accuracy of information, the ability of entities to safeguard and protect the distribution of information, and how the information would be used. A 1992 survey indicated that 76 percent of the

EXHIBIT 2 Privacy-Related Characteristics of Various Technology Eras

Era	Characteristics	Capabilities
Information age	Centralized mainframe computing/storage	Compilation, manipulation
Network age	PC workstations, LAN/WAN distributed computing/storage	Compilation, manipulation, communication
Internet age	PC browsers, platform-independent, network computing/storage, Web services	Compilation, manipulation, communication, workflow
Mobile age	Laptop, PDA, cell phone, wireless, mobile services	Limited compilation and manipulation, global communication and positioning

public felt they had lost control over how information about them was circulated and used by business organizations.¹⁵

Privacy and the Internet

Continued advances in information technology in general, and the growth in the use of inter-networking technologies specifically, further facilitate the collection, distribution, and use of personal information. The Internet provides individuals and organizations convenient anywhere-to-anywhere connectivity with unprecedented 24/7 access to a vast array of information across geographical boundaries. As predicted by the information technology privacy cycle, exploitation of Internet technology is now creating heightened public apprehension about its privacy implications. Although the United States recently passed new online privacy legislation, including the Children’s Online Privacy Protection Act (COPPA), provisions in the Gramm-Leach-Bliley Financial Modernization Act (GLB) and the Health Insurance Portability and Accountability Act (HIPAA), these laws are applicable to relatively narrow types of information and particular industry sectors. [Exhibit 2](#) outlines the privacy-related characteristics of the various technology eras, including the burgeoning mobile computing era not addressed in this article.

Understanding Web User Privacy Concerns

Detailed examination of the nature of individual user privacy concerns provides useful insights into potential remedies. A 1998 survey examining scenarios and privacy preferences suggests that Web users can be statistically clustered into three primary groups based on their attitudes about privacy.¹⁶ Privacy fundamentalists (17 percent) are described as unwilling to provide any data to Web sites and are very concerned about any use of data. The pragmatic majority (56 percent) are concerned about

data use but could be made comfortable by the presence of privacy protection measures such as laws and privacy policy statements, and the remaining respondents (27 percent) are categorized as marginally concerned. Similar results from a separate study conducted in Germany in 2000 not only identify the privacy fundamentalist (30 percent) and the marginally concerned (24 percent), but also describe two distinct subgroups within the middle tier delineated as identity concerned (20 percent) and profiling averse (25 percent).¹⁷ These two subgroups differ in the nature of their privacy concerns based on whether information requested includes identifying information such as name, address, or e-mail, or focuses on interests, hobbies, or health habits, respectively.

The most pervasive individual Web privacy concern stems from secondary use of information, defined as personal information collected for one purpose and used, subsequently, for a different purpose.¹⁸ Studies suggest that (1) users are more willing to provide personal information when they are not identified, (2) some information is more sensitive than other, and (3) the most important factor is whether or not the information will be shared with other companies. Further, users overwhelmingly disliked unsolicited communications and any form of automatic data transfer.¹⁶ Most consumers want to be informed about what information is being collected from them, how the data will be used, and whether their information will only be used in an aggregate form. Users are less likely to perceive business practices as privacy invasive when they perceive that information is collected in the context of an existing relationship, is relevant to the transaction, will be used to draw reliable and valid inferences, and they have the ability to control its future use.^{18,19}

Attempting to measure a consumer’s willingness to trade consumer benefits for a relaxation of privacy interests, one study found that user perception of what constitutes fair infor-

There is a gray area between when information sharing is an invasion of privacy and when it is in the public's interest to know.

mation practice diverges across uses and that information collection practices acceptable in one setting may be unacceptable in another setting. That is, perception of whether personal information collected for credit, insurance, employment, or direct marketing purposes was beneficial or privacy invasive varies based on the purpose.²⁰ Research also shows that users frequently act in a manner inconsistent with their privacy preferences, willingly providing more information than their self-reported privacy attitude would indicate.²¹ These inconsistencies suggest that attitudes and behaviors about protecting personal information are negotiable based on the situation, type of information requested, conditions set forth on how the information would be used, benefits provided in exchange for the information, and the extent to which the information would be shared.

Are User Expectations of Privacy on the Internet Unreasonable?

It should be noted that privacy on the Web is not a one-sided issue and some people question where we should draw the line between public, proprietary, shared, and private information. Some point out that the Internet is decidedly and purposely a public medium and that anyone who uses it, by choice, forfeits some measure of individual privacy, much like walking or driving down a crowded street. Additionally, they contend that when choosing to do business with a particular entity, whether online or not, any information gathered with respect to that transaction rightly belongs to the proprietor that invests resources into compiling the databases and mining the information.²² The Direct Marketing Association estimates that restricting the use of consumer information will result in a 3.5 to 11 percent increase in retailer costs, reduce services to rural and inner-city consumers, and make it more difficult for smaller businesses to compete.²³ Further, the current credit system, including the ability to conveniently use ATMs, make credit card purchases, and finance large purchases of homes and automobiles could not exist without a mechanism to share information on credit histories. Indeed, there is a gray area between when information sharing is an invasion of privacy and when it is in the public's interest to know. For example, to what extent is the protection of an individual's privacy more important than securing potential law enforcement or national security interests? Still

others maintain that protecting privacy in cyberspace amounts to hiding and suppressing information, restricting access, and inhibiting the free flow of information or censorship, often forcing people to make bad decisions and reach inappropriate conclusions.²⁴ One interpretation of a reasonable expectation of privacy on the Web concludes that the technologies supporting online shopping and personalization are morally permissible, but that the monitoring of consumer habits and centralization of information is not.²⁵ Privacy is an ethical as well as a business strategy issue.²⁶

Self-Regulation and the Privacy Policy Statement

In 1991, the President of the Association for Computing Machinery (ACM) expressed support for fair information practices; a doctrine including the principles of notice, choice, access, and security; and urged observance by all organizations that collect personal information.²⁷ Subsequently, U.S. industry has attempted to avoid legislative restrictions on the use of personal information by promoting self-regulation. In 1998, then Vice President Gore asked the Commerce Department to work with the Federal Trade Commission (FTC) to encourage companies that build profiles about individuals to implement effective self-regulatory practices, including adopting fair information practices.²⁸ An FTC report in 2000, however, concluded that U.S. self-regulatory approaches were ineffective in safeguarding consumer information, marketing techniques employed to profile customers were increasingly intrusive, and congressional legislative action was warranted to protect consumer privacy online.²⁹

The self-regulatory approach adopted by the United States is in direct contrast with the government-mandated approach adopted by the European Union (EU). Under the EU's 1995, and the subsequent 1997, Directive on Data Privacy, the burden is placed on companies and organizations — not individuals — to seek permission before using personal information for any purpose.³⁰ Similar approaches have been adopted in other countries, including Australia, Argentina, Canada, Hong Kong, New Zealand and Taiwan. The EU Directive states that specific personal information cannot leave the European Union unless the recipient country of this information complies with the laws in the EU Directive.⁴ In July 2000, however, the United States negotiated a safe harbor agreement with the EU Commission, wherein U.S. companies

Although broader privacy legislation is being debated within the U.S. Congress, it is likely that strong business interests will hamper regulatory approaches in the United States.

can voluntarily self-certify to adhere to a set of privacy principles loosely based on the fair information practices developed by the Commerce Department and the EU Commission. The primary difference under safe harbor is the ability of U.S. companies to administer self-enforcement versus enforcement by the European Commissioner or other agencies for compliance with the explicit rules of the EU Directive.³⁰ This safe harbor agreement continues to be a point of contention in ongoing global trade and commerce discussions.

A 1999 Georgetown Internet study indicated that nearly two thirds (65.7 percent) of commercial sites had developed and posted privacy policies or information practice statements.³¹ Because the survey was conducted three years ago, the percentage of commercial sites that currently have privacy policy statements has likely increased. The problem is that the content, accessibility, and scope of these privacy policies are inconsistent, companies can readily and easily change their policies without notice; and in most cases, there is no legal means to ensure that posted policies are followed. Although broader privacy legislation is being debated within the U.S. Congress, it is likely that strong business interests will hamper regulatory approaches in the United States. In general, legislative approaches tend to temporarily lessen public outcry and offer some relief; however, the characteristically slow implementation process ultimately fails to keep up with the fast pace of technology introduction and as such does little to increase consumer confidence and improve user trust. Further, the resulting regulation tends to negatively affect the ability of business organizations to function, effectively impeding efficient, legitimate, business, or statistical use of information. Trust is an integral prerequisite in consumer willingness to participate in B2C online commerce and privacy regulation is severely limited in its ability to improve user trust.³²

TECHNOLOGY AND PRIVACY

The issue of who has control over personal data and how this data is used needs to be addressed at a global level in order for the Internet to develop into a trusted, widely acceptable international marketplace for the exchange of goods and services. The U.S. self-regulatory approach and existing legislation governing information use has not effectively addressed the majority of American individual

Web user concerns, let alone international concerns. This suggests that perhaps technology, although widely implicated for enabling companies to employ privacy invasive practices, could play a significant role in protecting privacy, particularly because of its ability to cross international political, regulatory, and business boundaries, much like the Internet itself.

Technologies for Monitoring Web Usage

The primary technology for collecting information on an individual's activities over the Internet has been the Web "cookie." Cookies are digital information sent from a Web server and stored on the hard drive of an individual's computer by the browser software or network application. Cookies were designed to address the problem of statelessness inherent in the Hypertext Transfer Protocol (HTTP).³³ Because a browser does not stay connected to a server, but instead makes a connection, sends its request, downloads the response, and makes a new connection to send another request, it severely limited the functionality of Web services and complicated application development. Web cookies provide a solution to this statelessness by allowing for continuity in the interaction between the browser and the Web server. The cookie has proven to be the most reliable, robust, and network friendly means to provide needed state functionality on the Web, although this functionality can also be provided by embedding state information in URLs, using hidden fields in HTML forms, or using the client's IP address.³³

Web cookies can be classified into two general types: session and persistent.³⁴ The session cookies last only as long as the browser session with the server. However, persistent cookies remain stored on the hard drive of the client computer until they reach an expiration date or are deleted. Persistent cookies can be used to store information useful to both the user and the Web site, including account names, passwords, and past navigation streams. This cookie information is exchanged using the packet header and can be used by the Web site to eliminate the need for users to log-in, set user preferences based on past behavior, and to customize or personalize user experience.³⁵ The persistent cookie also has more significant privacy implications because storage of navigational streams and log-in information could be used to monitor and track user browsing behavior and linked to any personal information provided. Persistent cookies can also be shared

Monitoring browsing activities in and of itself is not considered by most Web users to be privacy invasive; however, it is the ability to then link these activities back to an individual that has most consumers and privacy advocates alarmed.

by a third-party Web host and used to track activities at a particular Web site or as a user moves from site to site.

Web bugs are hidden images that can be covertly added to any Web page; e-mail, or Microsoft Word, Excel, or PowerPoint file and used to collect information about user behavior. Web bugs send messages back to a server indicating its location, including the IP address of the computer, the URL of the page, the time the Web page or document was viewed, the type of browser used, and the previously set cookie value. Web bugs can be used to determine if and when a Web page, e-mail message, or document is opened, the IP address of the recipient, and how often and to whom information is forwarded and opened.³⁵ Web bugs can also be used to associate a Web browser cookie to a particular e-mail address and read previously set cookie values. Thus, a source server with a very small or invisible window could be added to any Web site or Web-enabled file and used serendipitously for a variety of tracking, surveillance, and monitoring activities.³⁴ Monitoring browsing activities in and of itself is not considered by most Web users to be privacy invasive; however, it is the ability to then link these activities back to an individual that has most consumers and privacy advocates alarmed.

Registration and billing, and observation are two main ways for a company to gather personally identifying consumer information.³⁶ Popular Web sites or sites that offer free services, such as e-mail accounts or stock quotes, often require a visitor to register by supplying demographic information before access to use the site is granted. In addition, online purchasing requires disclosure of credit card and billing information, including name, phone number, and address. A 1999 study found that more than half of surveyed Web sites were collecting personal identifying information and demographic information on users that connected to that site.³¹ That some users willingly give away identifying information in exchange for desired services is consistent with the assertion that personal information may be negotiable. It is also clear that most users who voluntarily provide personal information in one context have little or no understanding of how the information could be used to monitor their Web behavior. Identifying information can also be obtained without permission by exploiting security holes in browsers, operating systems or other software, including the creative use of ActiveX controls, Java, JavaS-

cript, and VBScript code to retrieve information from the user's computer.³⁷ Technology-based means for ascertaining the identity of users continue to evolve, and the increasing complexity of operating systems, network, and application software and their interfaces promises to continue to provide ample vulnerabilities.

The capability of companies or individuals to access information via monitoring, sharing arrangements, acquisition, or voluntarily, combined with the growing sophistication and maturity of tools for matching and aggregating disparate data sources, are at the heart of individual privacy concerns. Sophisticated data mining tools that employ advanced statistical techniques allow organizations to perform analyses to uncover a great deal of information about Web site users, some of it considered personal and beyond what the user has knowingly agreed to provide.¹² This information is a tremendous asset not only to the visited Web sites allowing for customization and personalization, but is also of great value to advertisers or other online or conventional retailers. The high value of information has created great incentive for the information broker industry and made it increasingly difficult for users to control what, where, when, and how information about them is distributed and used.

Technologies to Protect Privacy on the Internet

One of the first technologies available for protecting privacy on the Internet was the *anonymizer*. Anonymizers provide the ability to sanitize packet headers passed from the client to the server. Early versions consisted of software that would act like a proxy server, intercepting all communication between the browser and the server and removing all information about the requester. Current versions use Secure Sockets Layer (SSL) technology for sending URL requests, establishing an encrypted communications tunnel between the user and the anonymizer proxy, and routing traffic through a number of proxy servers.³⁸ This firewall-like technology disguises a user's IP address, similar to most Internet service providers, and supplies users with dynamic IP addresses every time they log on. Software tools are also available that provide a pseudonym proxy for logging on to Web sites, giving users consistent access to registration-based systems without revealing personal data.³⁹ These tools provide a means to protect the net-

Common browser defaults are set to accept all cookies and most users are not aware or sophisticated enough to change the browser defaults.

work identity of the computer; however, there are also negative performance and reliability consequences. In addition, some specialized proxy servers can be used to intercept and alter information between client and server.⁴⁰

There are other technology-based solutions available for protecting privacy, including tools for filtering HTML allowing users to block certain URLs, anonymous re-mailers for sending and receiving e-mail messages, and software for managing Web cookies.³⁸ Cookie managers are used specifically to counter the placement of Web cookies on user hard drives. Most browsers have a parameter that can be set to either inform users when a site is attempting to install a cookie, allowing users the option to accept or decline it, or to prevent any cookies from being installed. However, common browser defaults are set to accept all cookies and most users are not aware or sophisticated enough to change the browser defaults. Users also have the capability to go in and delete cookies from their browsers. There are other software products and services that provide cookie management capabilities, allowing individuals to view, block, control, and remove existing cookies. Web bugs, however, are generally not affected by this so-called cookie crusher software technology.³⁴ The overall market penetration of these technology-based privacy protection tools has been rather minimal, indicating that most users are either unaware of their existence, question their effectiveness, find them too complex or bothersome to use, or are not concerned enough about privacy to employ them. A 2000 study indicates that only 5 percent of Internet users have ever used anonymizers, 10 percent have set their browsers to not accept cookies, and 56 percent do not know what a Web cookie is.⁴¹

THE PLATFORM FOR PRIVACY PREFERENCES (P3P)

In April 2002, the World Wide Web Consortium (W3C) developed its first release of a standard, the Platform for Privacy Preferences (P3P v.1). P3P offers a means for a Web site to provide server-side machine-readable privacy policies that Web browsers could use to automatically compare with the privacy preferences directed by the user.⁴² It provides a framework to describe categories of information and how that information can be used in standard computer-readable format based on the eXtensible Markup Language (XML). P3P is touted as enhancing user control by putting

privacy policies where users can find them, in a form users can understand, and, most importantly, enabling users to act on what they see.⁴² A user initiates contact with a Web site by requesting privacy policy information for that site through a P3P-compliant agent in the browser that maintains the user's privacy preferences. The notice of privacy practices or privacy policy of the organization would be sent by the P3P-compliant Web site as a first response in a standard predefined format using a formalized description of privacy practices written in a P3P Preference Exchange Language (APPEL).¹⁷ The agent would then compare the policy of the organization's Web site with the stored prespecified privacy preferences of the user. The user agent could then either automatically accept the Web service if it met the users' preferences or inform the user of any exceptions and give the user a choice on how to proceed.

The Potential for Success of the P3P Standard

A study examining the privacy practices of Web extensions found that privacy policy statements generally lack candor, provide loopholes, use technical jargon and legalese, and are difficult for most users to use effectively.⁴³ Additionally, an organization can get the majority of users to accept its privacy policy by simply making it the default or the response that is provided if no user action is taken.⁴⁴ P3P offers an interesting technology-based solution to the current inconsistencies of Web site privacy policies and the overwhelming use of "opt-out" practices of most Web sites. The capability to push privacy policy information to the user in a standard format should offer an ease-of-use improvement to the current process requiring that the user actively search for pertinent Web site privacy policy information. Additionally, the use of a core set of information practice disclosure formats should assist user awareness and understanding of privacy policy information.

The assessment of critics of P3P v.1 is that the standard provides benefits that are skewed toward the providers of Web services and developers of Web software.⁴⁵ They point out that Web servers are under no obligation to accept consumer preferences, leaving consumers with little choice but to either lower their standards and accept the server's behavior, or not use the site. Although earlier drafts of P3P included the ability of a Web site to post multi-

P_{3P}
requires an organization to make a nontrivial investment of time and resources to implement and maintain P3P-compliant Web services.

ple policy choices on its server with which a browser could negotiate, the complexity of the negotiation phase led to its removal in the current specification.¹⁷ P3P critics also point out that the specification does not make a recommendation on standard default P3P settings, and that describing privacy preferences can be complex and beyond the technical capabilities of most potential users.⁴⁵ Broad P3P adoption will likely be dependent on the development of third-party tools that allow users to easily develop browser privacy settings and to interpret privacy policies of Web servers. Some question the motive and credibility of the W3C, which consists primarily of large corporations that pay the relatively expensive membership fees, suggesting that member organizations and their representatives have little incentive for developing strong privacy protection measures that negatively affect their ability to collect valuable consumer information. This article maintains that although the P3P does not provide a cure-all for user concerns, it does provide a standard means for accessing Web site privacy policies offering a functional enhancement for most Web users and providing an interesting basis for examining privacy-enhancing technologies.

CAN PRIVACY-ENHANCING TECHNOLOGIES IMPROVE USER TRUST

Most technologies employed to protect privacy on the Web are user-controlled, user-based initiatives that diminish organizational participation in the user trust interaction. P3P, however, requires an organization to make a nontrivial investment of time and resources to implement and maintain P3P-compliant Web services. Web users should interpret this action as a signal that the organization is proactively addressing public privacy concerns and thus offering enhanced customer service. Early adopter organizations should be able to tout support of privacy-enhancing technologies such as P3P as a competitive advantage and use it as a vehicle to improve user trust. Because P3P is an extension of the privacy policy statement, it does not provide a means for monitoring or enforcing a company's adherence to its stated policy. Thus, another important factor in improving user trust will be the extent to which the organization can shape perception and engender belief that the information contained in its policy statements accurately reflects the organization's information collection and sharing practices. This

is particularly true in the absence of more stringent privacy laws or regulations.

Implementation and adoption of P3P-based products will likely follow the adoption and diffusion characteristics of other information systems technologies, as characterized by Roger's S curve plotting the number of users against time.^{46,47} Thus, implementation will initially be slow, with only the most innovative and risk-taking organizations and individuals using the technology. As others observe the benefits that the early adopters derived from the technology, the apparent risk is reduced and they will also begin to adopt it. P3P implementation, like other standards-based privacy enhancing technologies, should also exhibit positive network effect characteristics in that the value of the technology to both the user and the organization is increased the more widely it is used. Conversely, if a small or negligible number of Web sites or users choose to implement P3P, its overall value would also be negligible. P3P implementation will require a significant capital investment and impose significant switching costs on browser vendors, stand-alone software, and compliant Web sites. Most organizations that implement privacy-enhancing technologies exhibiting network effects with corresponding high switching cost characteristics generally benefit from products based on open standards. However, a company with a strong market position, such as Microsoft in the browser market, can use proprietary standards to control the technologies' implementation.³⁶ Similarly, it would be expected that the most popular sites will resist becoming P3P-compliant or implement late in the adoption cycle as dictated by market forces. These sites will have little or no incentive to make it easier for users to examine their information collection and sharing practices and plenty of incentive to use and sell valuable personal information obtained. Even when these organizations do implement the standard, they will likely have privacy policies that allow extensive use and sharing of personal information, forcing P3P users to either alter their preference to use the site or not use the site. The extent to which this stance has minimal market risk, organizations may be able to overlook P3P implementation altogether.

A majority of Web users are concerned about use, particularly secondary use, of their personal information. However, they rarely read Web site privacy policy statements and are usually unaware of existing technological remedies. As such, privacy-enhancing technologies

Privacy-enhancing technologies, such as P3P, that offer the ability for easy user customization and choice, should significantly improve user trust.

such as P3P can offer significant ease-of-use and usefulness improvements by reducing search time to find relevant information and standardizing the access and language of privacy policies. This should result in an enhanced capability to compare competitive Web site policies and foster better user understanding of organizational privacy policy information. A key factor in individual user acceptance will be how P3P is implemented in vendor stand-alone software or the browser. If it is easy to configure and use, and offers increased usefulness, user market demand could be a factor in driving its rapid adoption and acceptance in the marketplace.⁴⁸ The notion of privacy varies across individuals and situations; thus, a one-size-fits-all approach to the issues would be suboptimal for all stakeholders, including individuals, business organizations, and governments. Privacy-enhancing technologies, such as P3P, that offer the ability for easy user customization and choice should significantly improve user trust.

SUMMARY

Privacy concerns are having a direct effect on individual trust and purchase behavior on the Web. This article offers some insight into and practical information for both organizations and individual users participating in B2C E-commerce. We use the concept of the information technology privacy cycle as a framework for predicting user and legislative reaction to new technologies. We examine technologies used by organizations to monitor Web usage, and technologies available to users to protect their privacy. Although P3P implementation was specifically discussed, the principles in this article would be applicable to any privacy-enhancing technology with similar characteristics. Areas for potential future research include empirical studies of the individual user acceptance and organizational adoption of privacy-enhancing technologies, such as P3P. ▲

References

1. Chaum, D., David Chaum on Electronic Commerce: How Much Do You Trust Big Brother, *IEEE Internet Computing*, November/December 1997, pp. 8-16.
2. Bakos, J. and Brynjolfsson, E., Bundling Information Goods: Pricing, Profits, and Efficiency, *Management Science*, 45(12), 1613-1630, December 1999.
3. Straub, D. and Collins, R., Key Information Liability Issues Facing Managers: Software

- Piracy, Databases and Individual Rights to Privacy, *MIS Quarterly*, June 1990, pp. 143-156.
4. Joss, M., Do You Need a CPO?, *ComputerUser*, June 1, 2001, available at <http://www.computeruser.com/articles/2006.1.2.0601.01.html>.
5. Business Week-Harris Poll, Results printed in *Business Week*, March 20, 2000, issue.
6. Payton, F., Ecommerce: Technologies That Do Steal!, *Decision Line*, March 2001, pp. 13-14.
7. Sipior, J., Ethical Management of Employee E-Mail Privacy, *Information Systems Management*, 15, 41-48, Winter 1998.
8. Warren, S. and Brandeis, L., The Right of Privacy, *Harvard Law Review*, 4:5, 193-220, March 1890.
9. Schoemann, F., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, 1984.
10. Westin, A., *Privacy and Freedom*, Atheneum, New York, 1967.
11. Toscana, P., Taming the Cyber Frontier: Security Is Not Enough!, 2001, available at <http://www.usertrust.com/news/taming-cyberspace.html>.
12. Mason, R., Culnan, M., Ang, S., and Mason, F., Privacy in the Age of the Internet, in G. Dickson and G. DeSantis (Eds.), *Information Technology and the Future Enterprise: New Models for Managers*, Prentice-Hall, Upper Saddle River, NJ, 2001.
13. Clarke, R., Information Technology and Dataveillance, *Communications of the ACM*, May 1988, pp. 498-512.
14. Davis, J., Protecting Privacy in the Cyber Era, *IEEE Technology and Society Magazine*, Summer 2000, pp. 10-22.
15. Louis Harris and Associates, Inc., Harris-Equifax Consumer Privacy Survey 1992, Equifax Inc., Atlanta, GA, 1992.
16. Ackerman, M., Cranor, L., and Reagle, J., Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences, *Proceedings of the ACM Conference on E-Commerce*, Denver, CO 1999.
17. Grimm, R. and Rossnagel, A., Can P3P Help to Protect Privacy Worldwide?, *ACM Multimedia Workshop*, January 2000.
18. Culnan, M., How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use, *MIS Quarterly*, September 1993, p. 341.
19. Baker, J., Personal Information and Privacy, *Proceedings of the First Conference on Computers, Freedom and Privacy*, J. Warren, J. Thorwaldson, and B. Koball (Eds.), IEEE Computer Society Press, Los Alamitos, CA, 1991, pp. 42-45.
20. Westin, A., Domestic and International Data Protection Issues, in *How the American Public Views Consumer Privacy Issues in the Early 90's — And Why*, Testimony before the Subcommittee on Government Information, Justice and Agriculture, Committee on

- Government Relations, U.S. House of Representatives, U.S. Government Printing Office, Washington, D.C., 1991, pp. 54-68.
21. Spiekermann, S., Grossklags, J., and Bettina, B., E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior, *Proceedings of the ACM Conference on Electronic Commerce EG'01*, October 2001.
 22. Gordon, H., Roth, S., Lieberman, S., Zeller, A., and McConnell, A., Customer Relationship Management: A Senior Management Guide to Technology for Creating a Customer-Centric Business, available at <http://www.the-dma.org/library/publications/customerrelationship.shtml>
 23. Direct Marketing Association White Paper, The Impact of Data Restrictions on Consumer Distance Shopping, March 2001, available at <http://www.the-dma.org/library/whitepapers/>.
 24. Artz, J., Protecting Privacy in Cyberspace: Just Selfishness or Is It Immoral?, Presentation at George Washington University Seminar Series on the History of Recent Science, Washington, D.C., March 2001.
 25. Lin, D. and Loui, M., Taking the Byte out of Cookies: Privacy, Consent and the Web, *Computer and Society*, June 1998.
 26. Mason, R., Four Ethical Issues of the Information Age, *MIS Quarterly*, June 1986, pp. 143-156.
 27. White, J., President's Letter, *Communications of the ACM*, 34(5), 15-16, May 1991.
 28. Swire, P., Privacy Excerpt from "Towards Digital eQuality: The U.S. Government Working Group on Electronic Commerce," 2nd Annual Report, December 1999, www.ecommerce.gov.
 29. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, Washington, D.C., May 2000.
 30. Consumer International, Privacy@net: An International Comparative Study of Consumer Privacy on the Internet, January 2001.
 31. Culnan, M., Georgetown Internet Privacy Policy Study, Washington, D.C., 1999, <http://www.msb.edu/faculty/cunannm/GIPPS/mmexs>.
 32. An up-to-date summary of pending privacy legislation can be found at the Center for Democracy and Technology Web site located at <http://www.cdt.org/legislation/107th/privacy/>.
 33. Kristol, D., HTTP Cookies: Standard, Privacy and Politics, *ACM Transactions on Internet Technology*, 1(2) 151-198, November 2001.
 34. Berghel, H., Cyberprivacy in the New Millennium, *IEEE Computer Magazine*, 34(1) 133-134, January 2001.
 35. Harding, W., Cookies and Web Bugs: What They Are and How They Work Together, *Information Systems Management*, Boston, 18(3), 17-25, Summer 2001.
 36. Shapiro, C. and Varian, H., *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business School Press, Boston, MA, 1999.
 37. McGraw, G. and Morrisett, G., Attacking Malicious Code: A Report to the Infosec Research Council, *IEEE Software*, September/October 2000, pp. 33-41.
 38. Electronic Privacy Information Center, Surfer Beware III: Privacy Policies without Privacy Protection, Washington, D.C., December 1999, <http://www.epic.org/reports/surfer-beware3.html>.
 39. Gabber, E., Gibbons, P., Kristol, D., Mataias, Y., and Mayer, A., Consistent, Yet Anonymous Access with LPWA, *Communications of the ACM*, February 1999, pp. 39-41.
 40. Berghel, H., Hijacking the Web: Cookies Revisited: Continuing the Dialogue on Personal Security and Underlying Privacy Issues, *Communications of the ACM*, April 2002, pp. 23-28.
 41. Pew Internet and American Life Project, Trust and Privacy Online: Why Americans Want to Rewrite the Rules, August 2000, http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.
 42. P3P 1.0: A New Standard in Online Privacy, <http://www.w3c.org/P3P/>.
 43. Martin, D., Smith, R., Brittain, M., Fetch, I., and Wu, H., The Privacy Practices of Web Browser Extensions, *Communications of the ACM*, February 2000, pp. 45-50
 44. Bellman, S., Johnson, E., and Lohse, G., To Opt-In or Opt-Out? It Depends on the Question, *Communications of the ACM*, February 2001, pp. 25-27.
 45. Hochheiser, H., Principles for Privacy Protection Software, *Proceedings of the Conference on Freedom and Privacy*, 2000
 46. Bakos, J. and Kemerer, C., Recent Applications of Economic Theory in Information Technology Research, *Decision Support Systems*, 8, 365-386, 1992.
 47. Rogers, E., *Diffusion of Innovations*, 4th ed., The Free Press, New York, 1995.
 48. Davis, F., Bagozzi, R., and Warshaw, P., User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science*, 35(8), 985, August 1989.