Global Business Review

http://gbr.sagepub.com

Guarding Privacy on the Internet

Madan Lal Bhasin

Global Business Review 2006; 7; 137
DOI: 10.1177/097215090500700109

The online version of this article can be found at:
http://gbr.sagepub.com/cgi/content/abstract/7/1/137

Published by:
SAGE
http://www.sagepublications.com

Guarding Privacy on the Internet

Madan Lal Bhasin

Undoubtedly, the government, business houses and employers have a legitimate need to collect data and to monitor people, but their practices often threaten an individual's privacy. Since a vast amount of data can be collected on the Internet, and due to its global ramifications, the FTC had identified 'core' principles of privacy which are widely accepted by leading countries. With the European Directive in force from 1998, 'trust seals' and 'government regulations' are the two leading forces pushing for more privacy disclosures. The need for companies to develop and put into place good privacy policies and/or statements has become more crucial than ever.

Privacy legislation prevalent in the US, the EU, Canada, Japan and Australia is summarized in this article. Privacy laws vary throughout the globe but, unfortunately, the topic has turned out to be the subject of legal contention between the EU and the US. Among the companies given high marks by privacy advocates for making data protection a priority are Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon.

Currently, the only way consumers can stop the collection of their personal data is to 'opt-out' or configure the browser to reject 'cookies'. We have briefly examined various methods (like Carnivore program, W3C Platform for Privacy Preferences (P3P), Encryption, etc.) used by the corporate world. Today, more advanced technological safeguards are needed. For corporations that collect and use personal information, ignoring privacy legislative and regulatory warning signs can prove to be a costly mistake.

Introduction

With the opening of the Internet for commercial activities in 1991, thousands of businesses the world over have hooked up and started doing business online, from establishing a mere presence to using their sites for transactions. The Internet, however, is a public network and doing business online continues to be a double-edged sword. Everyday, more and more companies are opening their information systems to other businesses and to the public to increase sales, and to make shopping, purchasing, and

Madan Lal Bhasin, Head, Accounting Department, Mazoon College for Management and Applied Sciences, Muscat, Sultanate of Oman. E-mail: madan.bhasin@rediffmail.com, madan_0012002@yahoo.co.in

Global Business Review, 7:1 (2006)
Sage Publications *New Delhi/Thousand Oaks/London*
DOI: 10.1177/097215090500700109

service more convenient for their clients. Unfortunately, the more businesses allow access to their services and systems through the Internet, the more vulnerable they are to security breaches. Along with growing concerns about security, consumers are also concerned about their privacy. The potential for violation of privacy in e-commerce has been an issue of significant controversy ever since business on the web began.

According to an estimate by the consulting firm PricewaterhouseCoopers, 'the business world lost US$1.6 trillion to hacker attacks in 2000. The firm based this estimate on a survey of about 5,000 information technology professionals in 30 countries. Viruses launched on the Internet carry out the most financially damaging attacks. The infamous Love Bug of 2000 alone caused an estimated $2.6 billion in damages.' Similarly, the FBI has listed virus attacks and employee violations of company Internet policies among the chief network-related crimes. While the FBI is beefing up its cadre of professional 'cyber crime busters,' some critics claim that the agency itself may violate one of America's most important civil rights: privacy. The accusation arises from the FBI's use of hardware and software to intercept e-mail in a stated attempt to prevent crime and terrorism.

The proliferation of the Internet as an educational and business medium has exacerbated the violation of individual privacy. Today, computers make the collection, maintenance, and manipulation of personal data more possible, faster, less expensive, and more effective than manual methods. A serious concern for individual privacy is growing alongside the growth of e-commerce. In this context, privacy is the ability of individuals to control information about themselves—what and how much is collected, how it may be used, and so on. Three parties may violate the privacy of individuals—government, businesses, and employers. Governments need individuals' information for planning of infrastructure, education and other services, as well as to facilitate law enforcement. Businesses collect consumer information to better target their marketing and service efforts. Employers monitor employees to ensure productivity and enforce corporate policies. Undoubtedly, all three parties have a legitimate need to collect data on individuals and to monitor people, but unfortunately their practices threaten privacy. On the other hand, individuals often feel that too many organizations know too much about their private lives. Therefore, many people try as hard as they can to minimize the amount of information collected about them, or at the least, they demand that their consent to use their personal information be obtained.

Privacy Threats in E-business

Collection of data by businesses about individuals has always invoked issues of privacy. However, online technology increases the concerns, as it allows for faster and easier storage of more data. It also allows for easier manipulation of that data and cross-referencing at unbelievable speeds (Punch 2000). In addition, in the online world, data collection can occur even without the knowledge of the individual, through the use of 'cookies'. 'Privacy is also threatened by the tracking of consumer usage by websites,' say Slyke and Belanger (2003), and 'clickstream data is the term given to data that tracks user surfing habits online.' Finally,

privacy is threatened when individuals' data is shared and/or sold by some companies with other companies without the explicit approval of the individuals.

Consumers are usually afraid that businesses, including those on websites, will sell personal information to other organizations without their knowledge or permission. For example, 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. In another leading case, *ToySmart.com,* an online toy retailer had promised consumers in published privacy policy 'never to share their data with other businesses'. In summer 2000, when the company was declared bankrupt, it tried to pay off debt by selling its customer data to the highest bidder. Despite public protest, a judge refused to block the sale. After the Federal Trade Commission (FTC) intervened, finally, the company agreed to sell the data only to another business that had the same privacy policy as ToySmart's.

Prosecution of *US Bancorp* on similar charges in direct violation of its stated privacy policy led to new US legislation. One section of the Financial Services Modernization Act, 1999, requires that customers of financial institutions must not only be notified before any personal information is disclosed to any non-affiliated 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 do not prevent US financial institutions from sharing customers' personal information with their affiliates.

Similarly, consumers are afraid that businesses and their websites are not adequately protected against outsiders. In 2000, someone calling himself Maxus hacked his way into the *CD Universe* website and stole 3,00,000 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.

Disputes and occasional consumer uproars over privacy issues continue. For example, the web advertising service *DoubleClick* came under fire for its user profiling activities. DoubleClick announced in 1999 that it was merging with *Abacus Direct Corporation*, a leading provider of specialized consumer data. DoubleClick provides Internet network advertising and collects anonymous information on online purchasing and browsing habits through cookies. Abacus Direct specializes in collecting and analyzing consumer data for direct marketing. Paul Krill (2002) points out: 'The companies announced that after the merger they would combine the data gathered by DoubleClick with personally identifiable information from the Abacus Direct databases. The Center for Democracy and Technology organized an electronic mail protect of DoubleClick's practice of tracking the online activities of consumers. This led to a public uproar and filling of lawsuits against DoubleClick. In January 2002, DoubleClick finally announced that it had decided to stop its web tracking service.'

Some of the readers may recall the *JetBlue* episode in 2003, in which the airline ran afoul of customers when it shared flight records with a Pentagon contractor that was building a travel security database. It is also interesting to see how some companies are using privacy to enhance their brand images. The Internet service provider *EarthLink* has run

a humorous ad campaign accusing another unnamed ISP of sharing personal information and promising to be much more discreet.

Undoubtedly, privacy is a major issue for consumers on the Internet. A *Business Week/Harris* poll of 999 consumers in 1998 revealed that 'privacy was the biggest obstacle preventing them from using websites, above the issues of cost, ease of use, and unsolicited marketing,' reported Green, Yang, and Judge. In an IBM Multinational Consumer Privacy Survey in 1999 (Harris Interactive 1999), 80 per cent of the US respondents felt that they had 'lost all control over how personal information is collected and used by companies. 78 per cent had refused to give information because they thought it was inappropriate in the circumstance, and 54 per cent had decided not to purchase a product because of a concern over the use of their information collected in the transaction. Specifically, 72 per cent of U.S. respondents were worried about the collection of information over the Internet.' Another study by *Forrester Research* supports these findings, showing that two-thirds of consumers are worried about protecting personal information online (Branscum 2000). Finally, a recent survey of consumer attitudes towards privacy reported by *Pew Internet & American Life Project* (2000) reveals that 66 per cent of respondents believe that online tracking should be outlawed, and 81 per cent believe that businesses should ask before collecting information about them (opt-in).

In the past few years, several organizations have had significant lawsuits filed against them by customers claiming that their privacy was violated. Consumers, all over the world, 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 in different countries that prohibit companies from releasing customer information to third parties without the consumer's express consent. Until privacy practices are made consistent and all organizations doing business online learn to properly respect individuals' right to privacy, we can expect these disputes to continue. As long as they do, some people will be reluctant to provide personal information online, and e-business will suffer.

Privacy versus Security

Privacy and security are said to be two of the biggest concerns regarding electronic business. In reality, both are major concerns for any computerized environment, including businesses, governments, and individuals. Privacy of data can be thought of as the confidentiality of the data collected by businesses or governments about the individuals using their services. Slyke and Belanger (2003) have defined privacy as 'the ability to manage information about oneself.' Since it is 'willingness' of consumers to share information over the Internet that allows transactions to be made, the consumers' control over 'how much' and 'what' information is shared is the essence of privacy on the Internet.

A security threat is defined by Kalakota and Whinston (1996) as a 'circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse.' Security, then, is the protection against these threats. Under this definition, threats can be attacks on network and data transactions or unauthorized

access by means of false or defective authentication. However, discussion about various forms of security threats, and security technologies and solutions is beyond the scope of the present paper. The primary focus will be on the issue of privacy protection on the Internet.

In other words, security relates to controlling one's environment for protection of data (Hoffman et al. 1999). Consumers, in the context of security, could be concerned with sharing information online because they fear hackers stealing their information. Privacy refers to monitoring the secondary use of information. Consumers, in the context of privacy, could be concerned that once the information is freely submitted to a website, there is diminished or nonexistent control over whether and/or how there is further sharing of that information with third parties.

What is Privacy Concept?

As individuals and businesses continue to use e-business in increasing numbers, an equally increasing amount of information about these individuals and businesses is collected and stored. If the parties involved are knowledgeable about the data being collected and how it will be used, there is not a problem. The problem occurs when users either do not know what data are being collected, or do not know or consent to how the data should be used. The question of the degree to which the privacy rights of individuals should be protected is a leading barrier to global e-business. On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country. For example, privacy laws in the European Union are much stricter than those in the United States, which implies that US companies who want to do business in the European Union must follow the EU standard. However, the issue is not that simple.

In July 2000, the US *Federal Trade Commission* (FTC) identified five core principles of privacy protection that are widely accepted in the US, Canada, and Europe. They are:

- Notice—Consumers should be made aware of an entity's information practices before any personal information is gathered.
- Choice—Consumers should be given the opportunity to consent or deny any secondary uses (uses other than the processing of a transaction) of information. Secondary uses include mailing notices or transfer of data to third parties.
- Access—Consumers should be able to access their personal data and review it without significant delays. Further, consumers should be able to easily correct inaccurate personal information in a timely manner.
- Integrity and Security—The data regarding consumers' personal information should be processed in a fashion so that the data is accurate. Further, the data needs to be kept confidential as it is transmitted, processed and stored by the entity.
- Enforcement—Consumers should have recourse to action, if any, of the above 'core' principles are violated.

Unless businesses fall into certain categories (such as medical or financial institutions),

US law does not require that they abide by any of these. Note that the fourth recommendation is actually two recommendations—ensuring accuracy and ensuring that only authorized people have the access to the data.

Unfortunately, US companies are notorious for not following the very first recommendation. Some do have policies in place to ensure access only on a 'need to know' basis. In 2000, the 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 per cent 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 US websites, 42 per cent had implemented, at least in part, each of the four principles. The FTC also reported that only 8 per cent 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-regulated environment is adequate. Critics, however, 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.

To enforce privacy rules, some companies have established the position of Chief Privacy Officer (CPO). The appointment of such an officer may calm fears of privacy abuse. Regarding the privacy rights of adults, the US government is still willing to allow private industries the opportunity to device sufficient privacy rights policies, but thus far these efforts have fallen short of expectations. As opposed to the US, all EU nations have strict laws that ensure all the above rules are followed in letter and spirit. The US government is facing pressure from privacy advocacy groups and the European Union's (EU) new privacy regulation. As a result, US lawmakers are increasingly 'threatening' the business sector that they may soon introduce privacy regulations if industry efforts are not satisfactory.

Privacy Policy or Statement

Companies that are open and honest in their communications usually adopt privacy policies or statements, and are very clear about how they use collected data discreetly to further corporate growth, efficiency and performance. This is what leads to increased revenue, less litigation from the aggrieved, enhanced reputations for their brands, and more prospective partners willing to enter into lucrative cooperative ventures that require a deep well of trust. Among the companies given high marks by privacy advocates for making data protection a priority, are, to name a few, Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon. Some of these companies—such as Microsoft, which has in the past been plagued by security leaks in its operating system and e-commerce programs—have embraced hard-line privacy stances only after experiencing first-hand the potential damage to

their businesses that privacy breaches can inflict.

One way that consumers have to be knowledgeable about the possible consequences of dealing with a web merchant is the privacy policy or statement. This statement should discuss the privacy policy of the web merchant regarding the data collected and their subsequent use. It should be easily accessible through a link clearly visible on the first page (home page) of the merchant's website. Some companies show this link at the bottom of their home page (in small type) while others show it at the top of their home page. When a company wants to design its own privacy statement, the manager in-charge has to be careful to include all policies to which the company wishes to adhere, and to include them in clear, concise language. The manager must then write the actual statement, have it approved by the company's management (and probably the company's legal department or law firm), and finally, post it on the company website. The content of the statement, of course, will vary from company to company. To promote the use of privacy statements, several online tools have been developed to automatically generate or test privacy statements. For example, Microsoft Corporation has a privacy statement generator at www. Microsoft.com/privacy wizard/, and similarly, the IBM Corporation had its own at www.alphaworks.ibm.com/tech/p3peditor. However, many websites do not even have privacy policies. 'In the 1999 Georgetown survey, only 65.9 per cent of the 361 websites polled had a privacy disclosure,' remarks Dr Culnan (2002).

'Trust seals' and 'government regulations' are two leading forces pushing for more and better privacy disclosures on websites. Trust seals promote privacy in the form of self-regulation by industry, while government regulation takes the form of litigation, forcing companies into better privacy practices. Both trust seals and government regulations are summarized below for the benefit of readers.

Trust Seals

In the US, there are three not-for-profit organizations whose purpose is to guarantee that websites maintain adequate privacy standards. These organizations respond to voluntary invitations of commercial websites to examine their standards. If a website passes the test, they allow the site to use their seal of approval. While such organizations provide e-commerce firms with a mechanism of self-regulation, most of them have not sought such seals of approval. These seals are supposed to instill consumer confidence in the website. Examples of these seals include the Better-Business-Bureau Online (BBBOnLine), AICPA WebTrust, and TRUSTe. A number of other seals also exist on the Internet. For example, there is the VeriSign program, which is mostly for security through encryption and authentication products, or the International Computer Security Association's (ICSA) seal. Table 1 compares some of the requirements for businesses that want to display three of the trust seals.

The AICPA WebTrust seal program was specifically started to address customer concerns about privacy and security on the Internet. It focuses on disclosure of not only what information is collected and how it will be used, but also on business practices of the company. It requires a thorough examination

of the website by a certified public accountant or a chartered accountant.

BBBOnLine, a subsidiary of the well-established Better Business Bureau, administers the BBBOnLine seal, which promotes ethical business standards and voluntary self-regulation. While it promotes the idea that companies using this seal are good citizens, the program does not specifically address privacy and security online. It does require, however, that the company be in business for at least one year before being eligible to receive the seal.

TRUSTe is also administered by an organization that focuses on promoting online privacy. The role of the seal on a company's website is to reassure consumers that the company follows the set of self-regulation rules established by TRUSTe for the collection and use of private and personal information.

To encourage 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. By 2001, fewer than 3,000 e-commerce sites had the seal of approval of any of these organizations. TRUSTe has awarded some 2000 licenses since its 1997 inception, while BBBOnLine has passed out 727 seals since launching last year. WebTrust is considered the most stringent of the three programs. However, due to its costly fees and strict standards, WebTrust had awarded only two seals since 2001. At year-end 2003, the websites of more than 3,500 organizations displayed the TRUSTe

Table 1
Comparison of Some Website Seals

	AICP Web Trust	*BBBOnLine*	*TRUSTe*
Fee?	*Yes (High)*	*Yes (Low)*	*Yes (Low)*
Policies	Website must be examined thoroughly before seal can be affixed.	Website must follow BBB advertising ethics and policies.	Website must agree to site compliance reviews.
Disclosure required	Yes; Business practices, transaction integrity, and information protection must be disclosed.	No	Yes; Easily understandable and easy to find privacy statement.
Consumer redress	Options for redress must be disclosed.	Promptly handle consumer complaints; Agree to binding arbitration; Mechanisms for complaints provided.	Promptly handle consumer complaints; Mechanisms for complaints provided.

Source: Slyke, Craig Van, and Belanger, France (2003), '*E-Business Technologies: Supporting the Net-Enhanced Organization*', John Wiley & Sons, Inc., page 367.

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 Principle) as part of its Web Trust seal program. Several surveys revealed that the public is unimpressed with these seals of approval.

Critics have pointed out that organizations sponsoring these privacy seals are largely self-regulated. Both RealNetworks and US 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. The BBB's 'Online Reliability Program' sounds like it might be a privacy seal, but it has nothing to do with privacy protection. Actually, it is 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". Industry groups, such as the On-Line Privacy Alliance, have vigorously lobbied against increased government regulation in this area, claiming that the current self-regulated 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.

Government Regulations

Various government agencies have been active in the development of Internet privacy policies or principles. For example, the US Federal Trade Commission's (FTC) standard for privacy on the Internet requires that notice be properly given (having a clear privacy statement indicating what information is collected and how it will be used), choices be offered (to opt-out of personal information being shared or used), access be offered (to review the personal information and correct it if there are errors), and appropriate security (protection of the personal information) be provided as elements of a desirable privacy policy (Slyke 2003). Recent public outcries regarding online privacy have accelerated the government's involvement.

Privacy on the Internet is not a new issue. In 1986, the US government enacted the 'Electronic Communication Privacy Act (ECPA)' to protect access and disclosure to certain electronic communication content. In 1993, the government established the Information Infrastructure Task Force to lead the development of the National Information Infrastructure (NII). One of its task forces, the Privacy Working Group, prepared the report in 1995 titled 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information' (visit www.nsi.org/Liberty/Comm/niiprivp.html for details). The task force recommended that the proposed principles for privacy apply to both public and commercial uses of private information. It defined information privacy as requiring respect for individual privacy, disallowing

improper alteration or destruction of information, and ensuring that the information held is accurate, timely, complete, and relevant. The task force also recommended principles for providers and users of information. For providers of information (for example, a consumer shopping on the web), the principles include:

Awareness—Individuals have a personal responsibility to obtain information about which data are collected and how they will be used.
Empowerment—Individuals should have a way to access, correct and technically control their information, and to be anonymous in certain cases.
Redress—Individuals should take action when harm occurs.

Principles for users of information (for example, companies that collect consumer data) include:

Impact assessment—Users of information should evaluate the impact on information providers of using their information.
Only reasonably necessary—Users should only use information that is necessary.
Notice—Users should provide information on why information is collected, what information is collected, which protections are offered, what consequences could result, and what redresses are available to the providers of information.
Security—Users of information should provide security measures to protect the data.
Limited use—Users of information should limit their use to the level of the individuals' understanding of that use.
Education—Users of information should provide education for providers of information and the public in general regarding privacy and collection of data.

Since then, there have been several reports and studies by various governments and agencies worldwide emphasizing the importance of protecting consumer privacy and security of data in the online world. It should be noted that law does not require privacy statements for websites maintained by US operators, but the government has been very active in trying to enforce privacy principles. Slyke and Belanger (2003) have cautioned that 'The FTC has threatened to adopt similar laws to those of the European Union. Federal agencies are forced to be good examples for other organizations regarding the protection of citizens' privacy rights.' As previously discussed, the US government has issued memorandums to all agencies requiring them to follow certain privacy principles, such as not using cookies when inappropriate and disclosing proper privacy statements. The information provided to agencies also includes why the standards were established, allowable exceptions, when the standards should be implemented, and a general discussion of privacy issues. A number of privacy-focused organizations exist, or have recently been developed, for the purpose of dealing with privacy issues. Some privacy-related organizations are: American Civil Liberties Union, Coalition Against Unsolicited Commercial E-mail, Cypherpunks, Electronic Frontier Foundation, Electronic Privacy Information Center, Global Internet Liberty Campaign, Online Privacy Alliance, Privacy Coalition, Privacy International, Privacy Rights Clearinghouse, Privacy Council,

and US Public Interest Research Group. (For more information, visit 'Electronic Privacy Information Center,' at http://www.epic.org/privacy/privacy_resources_faq.html).

Protecting Privacy: Privacy Legislation Scenario

Globalization is a noteworthy factor behind the increased attention being paid to privacy. To do business around the world, companies have had to adapt to local cultures and regulations. On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country. For example, privacy laws in the EU are much stricter than those in the US, which implies that US companies who want to do business in the EU must follow the EU standard. However, the issue is not that simple. Privacy rules, therefore, vary widely throughout the globe, and navigating this thicket of laws is critical to international commerce.

Legislatures the world over have taken notice and tried to minimize invasion of privacy. It is important to state that laws vary significantly among countries worldwide with respect to the protection of citizens' privacy. There are few federal laws in the US forcing websites to protect the privacy of online users. The two laws deal with the financial/banking industry, in which opt-out information must be provided to consumers, and a law protecting the privacy of children. This is why many consumers still fear web-based shopping. We are summarizing below the privacy legislation prevalent in the US, the EU, Canada and Japan. It is expected that a growing number of countries will adopt privacy laws to foster e-commerce.

The United States (US)

In the US, laws, court rulings and self-regulations govern the protection of an individual's information. 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. Privacy laws in the US are significantly more lax, especially with regard to non-government organizations. Further, governments are significantly more limited in the collection and dissemination of private data than are private businesses. Businesses that are not financial institutions or medical organizations are not limited by law. The US approach has been to expect businesses to impose self-regulation on data collection through the Internet. Whether or not this has happened to any significant degree is questionable. The US government, however, has stepped in despite limitations, and the Congress has adopted some laws, as summarized below, to curb violation of privacy.

The Children's Online Privacy Protection Act, 1998

The Children's Online Privacy Protection Act, 1998 (COPPA), which took effect in April 2000, requires online businesses to secure parental consent before collecting personal information from preteen web surfers. The law makes it a federal offense for commercial websites to collect personal information from children under 13 without parental

permission. It also forbids the release of such information if it has already been collected. To collect information from children, site operators must obtain 'verifiable parental consent.' This is a problematic point for businesses: How can the consent be verified online? Some jurists suggested that the presentation of a credit card account satisfies the law, because only adults can receive credit cards. Children, however, can use credit cards without their parents' permission.

Privacy of Consumer Financial Information Act

The Privacy of Consumer Financial Information Act states that a US financial institution must provide its costumers with a notice of its privacy policies and practices. It prohibits a financial institution from disclosing non-public personal information about a consumer to a non-affiliated third party unless the institution satisfies various disclosures and opt-out requirements, and the consumer has not elected to opt-out of the disclosure. Financial institutions include banks, brokerages and insurance companies. A 'non-affiliated third party' is any organization that is not owned by the financial institution and any organization that does not have a business relationship with the consumer.

Please note here that the organization must provide an opt-out option, which means if the consumer does not elect to be excluded, the organization is allowed to transfer his/her personal data to another organization. US privacy advocates have long required opt-in options. With opt-in, as long as the consumer has not opted to allow the transfer of his/her data, the organization is barred from doing so. Countries that are members of the EU enforce opt-in online and offline, because the EU Directive on Data Protection mandates that organizations must receive people's permission to transfer their data to another party.

The European Union (EU)

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. The EU adopted the 'Directive on Data Protection (Directive 95)' in October 1998, which limits any collection and dissemination of personal data. In the EU, a directive is framework law; each member nation may legislate a more restrictive law' but not a more relaxed one. The directive imposes the same rules in all 20 countries of the enlarged EU. These countries have passed laws that reflect Directive 95; some are even more restrictive. The directive provides that no one collect data about individuals ('subjects') without their permission; that the collecting party notify the subject of the purpose of the collection; that the maintainers of the data ask for the subject's permission to transfer the data to another party; and that upon a proper request from the subject, data about the subject be corrected or deleted (see Figure 1: European Union Directive on Data Protection). The directive prohibits the transfer of personal data from EU countries to any country that does not impose rules at least as restrictive as those of the directive.

Companies operating from the EU countries are barred by law from trading with US companies that do not abide by European

Figure 1

European Union (EU) Directive on Data Protection

Applies to all businesses with operations in European Union countries and those trading with EU countries. Some believe it may also apply to US 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-in' to allow the distribution of any 'sensitive' information.
To 'opt-out' of the distribution of any protected information for direct marketing purposes.

(The complete text of the EU directive is available at: http://www.privacy.org/oi/intl_orgs/ec/final_EU_Data"_Protection.html)

privacy laws. To overcome the problem, the US government offered to create a list of US companies that voluntarily agree to obey these laws. This list is referred to as a 'Safe Harbor'. A safe harbor is a legal provision that provides protection against prosecution. Now, European businesses have a protection against prosecution if they deal with US businesses that signed up as members of the arrangement. This arrangement is an official agreement between the United States and the European Union. A European company can look up a US business on the list, which is published online, to see if that business participates. US organizations must comply with the seven safe harbor principles, as spelled out by the US Department of Commerce (see Figure 2: International Safe Harbor Privacy Principles). However, months after the safe harbor was established, very few US companies had signed up—by October 2001, the total was only 102 organizations.

The European Union Privacy Directive has important implications, both for companies engaged in e-commerce and for multinational corporations with offices in EU countries. It is 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'. Organizations that want to trade in EU countries must guarantee that personal information is processed fairly and lawfully; that it is 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

Figure 2

International Safe Harbor Privacy Principles
(For Compliance with European Union Privacy Directive)

Notice: An organization must give conspicuous notice when it collects information, state how it is 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 complied 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 Safe Harbor website is at: http://www.export.gov/safeharbor. The full text is available on the U.S. Department of Commerce Website at: http://www.ita.doc.gov/td/ecom/shorin.html.)

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 EU Privacy Directive impacts numerous parts of an organization's records. A partial list of business 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. All forms of transmission are covered, including electronic and hard copy. In the EU's initial analysis, the US was not listed among those countries seen as adequately protecting the privacy of personal data. Now, almost 250 organizations are on the Department of Commerce's 'Safe Harbor' List.

The United States versus European Union

Transfer of millions of gegabytes of data occurs every day between the US and Europe, and the EU directive gives its member countries essentially 'a global reach' with an attached liability for non-compliance. In this context, Greenstein and Feinman (2000) warn US-based international companies: 'Basically, non-European companies will have to meet the European Union's directive if they want to conduct electronic commerce in Europe or risk legal action.' Thus, international US based companies may be forced to change their privacy practices in response to laws set abroad.

In the US the common approach to privacy regulation has been self-enforcement. When the EU put more stringent privacy regulations in place with a Directive on Data and Privacy in 1995, US companies were reluctant to comply. This reluctance came from the knowledge that customer data represents a valuable resource that can be used not only for direct marketing, but also as a separate source of revenue. Businesses in the US commonly sell customer data to other businesses. Representatives from the US and the EU

have hammered out a compromise called the Safe Harbor Privacy Principles. Seven principles comprise the framework for the Safe Harbor Privacy Principles. These principles outline requirements for how businesses must inform customers about privacy issues and provide options for them with regard to privacy. In addition, the principles dictate in broad terms how customers data should be secured and access granted, as well as how the guidelines should be enforced.

A major difference between standard practice in the US 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 discussed 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, or information concerning the sex life of an individual. Under US rules and practices, US organizations often transfer a great deal of this kind of information without getting opt-in or affirmative permission. US organizations with affiliates operating in the EU need to make sure they are following the stricter EU privacy rules. To understand what is at stake in the critical and tangled dispute between the two, look no further than Daimler Chrysler AG. The giant automaker—the model of the modern multicultural multinational, with one foot planted in Stuttgart and the other in Detroit—deals with an ongoing absurdity. Although the 1998 Daimler-Benz purchase of Chrysler for $37 billion was aimed in no small part at driving international recognition and sales for the combined company's portfolio of brands, information collected about EU customers by the Daimler division (e.g., the demographics of specific Mercedes-Benz car buyers) is generally kept from the Chrysler wing, which might be on the prowl for, say, wealthy German families of four who might be in the market for a Jeep Cherokee. Untold millions of dollars in annual revenues are lost at the iron wall that halts the data flow between the two parts of the company.

Under a 1998 EU directive, organizations in countries that do not match the Union's privacy standards are in most cases prohibited from receiving almost all identification and behavioral data about European Union constituents. With virtually no data protection regulations, the US is one such offender. While the EU and the US seek an agreement, Daimler-Chrysler is cautiously sticking close to the letter of the law. Other US companies echo Daimler Chrysler's approach. For example, Levi Strauss & Company's European headquarters in Brussels deletes consumer-identifying information from e-mail before passing it to the marketing unit in the same building. E-commerce pioneers Amazon.com and eBay have set up websites in some European countries that are completely distinct from their American businesses, in part to keep data in the two continents separate. And to sidestep potential prosecution, online advertising company DoubleClick Inc., buffeted by privacy concerns in the US, does not use information tracking software in Europe.

Jeffrey Rothfeder narrates the Daimler Chrysler approach in his book (2001): 'Merging two distinct work cultures is difficult enough,' says a German Daimler-Chrysler executive involved in the company's privacy initiatives, 'but what is perhaps most surprising is the different effort and attitude among the Germans and the Americans in this company when it comes to the importance of

protecting customer information from being misused or customer privacy from being invaded.' Disdain for the American view of confidentiality sums up the position of much of the EU, whose 20 countries, by and large, have had stringent privacy laws since the end of World War II, with especially rigorous rules in Germany, France, and the United Kingdom. This has led to an intractable distance between the EU and the US on privacy-protection issues, punctured by marathon, ongoing negotiations over the 1998 directive that have shown how pronounced the attitudinal and policy differences are between the two regions.

Canada

Canada passed 'The Personal Information Protection and Electronic Documents Act,' in 2000. The act provides that Canadians have the right to know why a business or organization is collecting, using, or disclosing their personal information, such as name, age, medical records, income, spending habits, DNA code, marital status, etc. They also have the right to check their personal information and correct any inaccuracies. According to the act, businesses must obtain the individual's consent when they collect, use, or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk.

Like members of the EU, Canada established a privacy commissioner. The privacy commissioner is an officer reporting directly to Parliament. Under the act, individuals may complain to the privacy commissioner about how organizations handle their personal information. The commissioner functions as an ombudsman; initiates, receives, investigates, and resolves complaints; conducts audits; and educates the public about privacy issues. He or she has two sets of powers—the power of disclosure, which is the right to make information public; and the power to take matters to the Federal Court of Canada, which can, in turn, order organizations to stop a particular practice and award substantial damages for contravention of the law (Dr Oz).

The act contains a set of fair information principles. These principles are based on the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information. The code was developed with input from businesses, government, consumer associations, and other privacy stakeholders. The act applies to the collection, use, and disclosure of personal information by organizations during commercial activities both with brick-and-mortar and online businesses. Personal information is any information about an identifiable individual whether recorded or not. Organizations include associations, partnerships, persons, and trade unions. The term 'commercial activity' includes the selling, or leasing of donor, memberships, or other fundraising lists.

Japan

Japan also recently passed its first omnibus privacy law, which Professor Alan F. Westin at Privacy and American Business (P&AB) accurately describes as 'a "middle way" between the industry-sector-based privacy laws of the US and the comprehensive data protection laws of the European Union.' It is reported in an article 'Privacy in the Age of Transparency,' published in 2004, as: 'The P&AB offers the Guide to Consumer Privacy in Japan and the New Japanese Personal

Information Protection Law to explain the data-protection climate in Japan and help companies navigate the legislation'.

Will Technology Provide the Privacy Solution?

Currently, the only way consumers can stop the collection of their personal data is to opt out—namely, find the webpage where they can ask the data collector to stop the collection. However, many sites do not do the data collection themselves; they hire companies such as, DoubleClick to do that for them. Consumers then have to find that third party's site and opt-out. To do so, they have to know that the site they visit contracted with the third party, and many consumers are not aware of the third party's role. No one is eager to inform the public about this, either. As we stated earlier, you can also configure your browser to reject cookies. While this sounds like a good option, it is often impractical. Most cookie-hungry sites are designed to disallow you from browsing further if your computer does not accept cookies. It is a conundrum.

A program originally called 'Carnivore', now called DC$1,000, is an e-mail sniffing software that captures data packets passing through Internet service providers (ISPs). To install the box that runs the Carnivore software at an ISP's site, FBI agents must first obtain a warrant, similar to obtaining a warrant for a wiretap. The software then monitors all transmissions coming from or going to a specific IP address they are targeting. Privacy advocates worry, however, that other e-mail messages could be randomly monitored once the software has been installed at an ISP. As Bowman (2001) observes, 'Legislation passed in the Summer of 2001 requires the federal government to reveal how many times law enforcement used DC$1,000, the workings of the approval process to use it, and whether it allowed gathering of any unauthorized information.'

Nowadays, some 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 available 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 complete report is available at http://www.epic.org/reports/prettypoorprivacy.html.

Another way to ensure online privacy is with Encryption—conversion of data into a secret code. When conducting e-business transactions and sending credit card information online, for example, encryption can

protect the user from theft of information that can lead to fraud. The most common foolproof way to prevent someone from reading your e-mail is to use software to encrypt it, thus rendering it incomprehensible to anyone without the decoder (or key). There are two major commercial encryption standards in use: Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME). The PGP is relatively easy to install (available free to non-commercial users, visit www.mcafreesecurity.com/us/products/home.html) and configure, and a widely accepted tool. Like a safe-deposit box, it uses two keys—one 'private' and one 'public'—only its keys are complex electronic passwords. To read a PGP-encrypted message, you need both keys. On the other hand, S/MIME is also available free on the Internet and is included in the Netscape Navigator and Microsoft Internet Explorer browser packages. It is available as a 'plug-in' to most e-mail packages. However, S/MIME is simple to configure and use—with two major exceptions. S/MIME uses a shorter code for its key, making it easier for a hacker to crack, and S/MIME does not rely on public keys; instead it uses third-party authentication relying on digital certificates. These contain the user's name, e-mail address and public key. One advantage of PGP over S/MIME is its acceptance rate. Since PGP is a widely used encryption software package, compatibility is hardly an issue. Additionally, it can be plugged into the most popular e-mail software applications. However, PGP and S/MIME can detect message tampering by using their digital signature features. PGP's digital signature software applies an algorithm (or formula) to the message content that automatically generates a unique code, or digital signature. Thus, encryption enables authentication and confidentiality in communication over computer networks.

The US government has adopted Secure Hash Algorithm (SHA) and allowed its own citizens to use such encryption schemes, but removed encryption techniques from its list of controlled export items only in the late 1990s. 'As a simmering undercurrent to the privacy discussions, the US's stubborn stance against exporting strong encryption software unless American security agencies are allowed access to the keys has added to worries in Europe that some US companies are using data surveillance technology for industrial espionage, giving them an unfair advantage in bidding for lucrative industrial and defense contracts. That possibility (and some Europeans believe there is evidence to support it) has made EU member governments even more antagonistic to giving in to the US on any data protection issue,' asserts Jeffrey Rothfeder. However, the United Kingdom and France still forbid the export, as well as the use of strong encryption software, by their agencies.

More advanced technological safeguards are needed now. A 2003 survey of computer security practitioners found that 40 per cent stated that they had detected outsiders trying to penetrate their network systems.

The Future Scenario and Prospects

Companies are entering an era of information transparency of increasingly activist stakeholders, the growing influence of global markets, the spread of communications

technology, and a new customer ethic demanding openness, honesty and integrity from companies. Consequently, risks to privacy are greater, and safeguarding sensitive information has become more significant, and more difficult to do. Among the companies given high marks by privacy advocates for making data protection a priority are Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon. Some of these companies—such as Microsoft, which has in the past been plagued by security leaks in its operating system and e-commerce programs—have embraced hard-line privacy stances only after experiencing first-hand the potential damage to their businesses that privacy breaches can inflict.

During the last several years, dozens of bills concerning the protection of privacy have been introduced at both the federal and state levels. At present, the Online Privacy Protection Act of 2003 (H.R. 69) is being considered by the US 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). 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.' Microsoft launched a project in 2004 called 'Trustworthy Computing,' under which Chairman Bill Gates has challenged the company 'to be certain that availability, security, privacy and trustworthiness are key components of every software and service product the company develops.'

Although many US companies initially fought consumers' efforts to make companies pay attention to privacy, almost no major businesses today feel they can completely neglect data protection rules. Thus, 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 violation issues. In the very near future, all organizations with an online presence will need to establish online privacy statements or policy certifying that they comply with legislated privacy standards. US 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 US 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 US will have strict privacy laws in the near future, for corporations doing business in EU countries, the future has already arrived!

REFERENCES

Booz Allen Hamilton Inc. 2004. 'Privacy in the Age of Transparency,' *Strategy + Business*, Spring.

Branscum, D. 2000. 'Guarding On-Line Privacy,' *Newsweek*, 135 (23): 77–78.

Bowman, L.M. 2001. 'House Pulls Carnivore into the Light,' *ZDNet News* (23 July): http://zdnet.com/2100-1106-270406.html.

Culnan, M. 2002. 'Georgetown Internet Privacy Policy Study,' McDonough School of Business, Georgetown University, see http://www.msb.edu/faculty/culnan/gippshome.html.

Green, H., C. Yang and P.C. Judge. 1998. 'A Little Privacy, Please,' *Business Week*, 16 March: 98–99.

Greenstein, M. and T.M. Feinman. 2000. *Electronic Commerce: Security, Risk Management and Control*. Boston, Irwin: McGraw-Hill.

Haag, Cummings, McCubbrey. 2004. *Management Information Systems for the Information Age*. Irwin: McGraw-Hill. Fourth edition.

Harris Interactive. 1999. 'IBM Multinational Consumer Privacy Survey,' Study Commissioned by IBM Global Services, October 1999. Available at: http://www.ibm.com/services/files/privacy_survey_oct991.pdf.

Hoffman, D., T.P. Novak and M. Peralta. 1999. 'Building Consumer Trust Online,' *Communications of the ACM*, 42 (4): 80–85.

Kalakota, R. and A.B. Whinston. 1996. *Frontiers of Electronic Commerce*. Reading, Mass: Addison-Wesley.

Krill, Paul. 2002. 'DoubleClick Discontinues web Tracking Service,' *InfoWorld*, 9 January, available at: http://www.infoworld.com/articles/hn/xml/02/01/09/020109hndouble.xml.

Pew Internet and American Life Project. 2000. 'Trust and Privacy Online: Why Americans Want to Rewrite the Rules,' available at: http://www.pewinternet.org/reports/toc.asp?Report=19.

Punch, L. 2000. 'Big Brother Goes Online,' *Credit Card Management*, 13 (3): 22–32.

Privacy Working Group of the National Information and Infrastructure Task Force. 1995. 'Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information,' 6 June, 1995. Available at: http://nsi.org/Liberty/Comm/niiprivp.htm.

Rothfeder, Jeffrey. 2001. 'Every Drop for Sale: Our Desperate Battle Over Water in a World About to Run Out,' Penguin Putnam Inc., Jeremy P. Tarcher.

Slyke, C.V. and F. Belanger. 2003. *E-Business Technologies: Supporting the Net-Enhanced Organization*. John Wiley & Sons, Inc.

Oz, Effy. 2002. *Foundations of e-Commerce*. NJ: Prentice Hall.