PERGAMON

Telematics and Informatics 19 (2002) 173–192

TELEMATICS
AND
INFORMATICS

www.elsevier.com/locate/tele

Policies for online privacy in the United States and the European Union

Jared Strauss, Kenneth S. Rogerson *

DeWitt Wallace Center for Communications and Journalism, Sanford Institute of Public Policy, Duke University, Box 90241, Durham, NC 27708, USA

Abstract

This article examines how public and private sector institutions in the United States and the European Union have reacted to public demand for increased and improved online privacy protection. We argue that self-regulatory attempts do not adequately protect privacy online and that legislative intervention, as is happening in the European Union, is not only a good idea for the United States, but may be necessary to secure future online exchange of personal information.

Keywords: Online privacy; Internet regulation; Fair information practices; European Union; United States

1. Introduction

Online privacy is not always a top priority, either to consumers or producers of online content. But, because the misuse of private information can result in serious problems, it will remain on the agendas of policymakers and the public. Though we believe the level of public concern about privacy is significant, it may be of even greater consequence to understand how the protection of online privacy will be addressed by the public and private sectors. This paper will examine how both public and private sector institutions in the United States and the European Union have reacted to public demand for increased and improved online privacy protection.

* Corresponding author. Tel.: +1-919-613-7387; fax: +1-919-684-4270.
E-mail address: rogerson@pps.duke.edu (K.S. Rogerson).

0736-5853/02/$ - see front matter
PII: S0736-5853(01)00012-0

First, we will discuss the demand for privacy protection in both societies. Second, we will discuss an array of public and private sector responses. We argue that self-regulatory attempts do not seem to be adequately protecting privacy online and that legislative intervention, as is happening in the European Union, is not only a good idea for the United States, but may be necessary to secure future online exchanges of personal information. The US Federal Trade Commission (2000) made this same recommendation to Congress in May 2000 in a report entitled "Privacy Online: Fair Information Practices in the Electronic Marketplace", but the administration of President Bill Clinton "threw cold water on [the] proposal. [They] were decidedly lukewarm... and said that the government should continue to rely on the industry to police itself" (Labaton, 2000, p. C1). This does not necessarily mean that legislation such as the EU data protection directive is working perfectly to protect privacy, just that the rationale behind it better addresses concerns about privacy than do alternative programs.

2. Privacy

Privacy online has evolved to mean the processes by which information is gathered and used. Information in this sense has usually meant personal information, i.e., a person's name, address, phone number, family status, social security or other identification number and even more in-depth information like financial and health statistics. The processes associated with privacy issues fall into four broad categories: methods of gathering, storing, analyzing and distributing information. Each process can invade privacy depending on the transparency of the methods used. Finally, privacy issues have been divided into individuals' relations with the public sector and the private sector. It has been notoriously difficult to discover how the private sector (businesses) collect and use personal information. Activities in the public sector (governmental bodies) have been more open.

The collection of personal information is certainly not new. Concerns about consumers' ability to protect their privacy existed well before the Internet, and the growth of World Wide Web has not fundamentally changed discussions about consumers' rights. Yet the Internet accentuates these issues by making data collection and storage easier. The Internet gives web sites (as opposed to brick-and-mortar businesses) access to a much wider audience, allowing them to collect more information from more people. Furthermore, web browsing creates a "data trail" resulting in an unprecedented level of preference tracking. Attaching cookies to a hard drive is like hiring someone to trail a shopper in the mall and report what stores they enter (Berman and Mulligan, 1999). Thus, web sites can access specific behavioral information that traditional businesses could never hope to gather. Finally, data storage has become so inexpensive that more companies can afford to gather more information on more people and keep it for a longer

period of time. Hence, cost concerns are less likely to constrain data-collection practices.

2.1. Privacy in the United States

Although privacy is not explicitly protected by the Constitution, Americans have traditionally considered privacy a valued right. The Supreme Court has included privacy among the "penumbra" of rights implied by the Constitution, and the government has passed laws specifically guarding individual privacy. Historically, Americans have been more concerned with government violations of privacy than with private sector intrusions (Reidenberg and Schwartz, 1996). For example, Congress enacted the Privacy Act of 1974, which regulates how the government can collect information on its citizens. However, no such overarching legislation governs data collection in the private sector. Rather, a few narrow, industry-specific laws, such as the Fair Credit Reporting Act, regulate the private sector.

Fair information principles (FIP) have also guided privacy policy.

> The principles were first developed a quarter century ago when the US Department of Health, Education and Welfare (HEW) studied the best way to take advantage of the growing power of computers without trampling on personal privacy. A task force of the HEW developed a set of five principles that have since formed the basis of privacy-related laws in the US. The FIP have also been codified into the national data protection laws of many industrialized countries (the US is the exception, having pursued a sectoral approach to privacy protection rather than adopting an omnibus privacy protection law) (Givens, 1999).

Also called "fair information practices", these principles influenced the 1974 Privacy Act. While the United States unofficially observes the standards, it has never passed legislation requiring private organizations to follow the guidelines (Givens, 1999). Still, privacy advocates have used these fair information practices as benchmarks for evaluating data collection and privacy protection since 1980.

The international community recognized the benefit of these practices when the Organization for Economic Cooperation and Development (OECD) used them as a foundation for its "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" in September 1980. These guidelines germinated in the 1970s, a period of "intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data" (OECD, 1980). With the increased capacity to gather, store and analyze information, people became more interested in, and in many cases concerned about, how that information might be used.

2.2. Privacy in the European Union

In the member countries of the European Union, the right to privacy is felt just as strongly as in the United States. There are differences, however. Whereas US policy makers have been reluctant to legislate privacy, European countries have done so more frequently and more broadly, attempting to include the private sector as well. This stems principally from the European tradition that the state should play an active role in protecting the citizen from social harm. In 1970, the German state of Hesse passed what is often considered the world's first data protection law (Maxeiner, 1995, p. 95, ft. 9). By 1975, Sweden had adopted national data privacy legislation. But other individual European countries eventually followed suit, such as Germany with its Federal Data Protection Act of 1977 and Britain with its Data Protection Act of 1984 (see Table in Bennett, 1992, p. 59).

Regional organizations were also keeping pace. In addition to the OECD Privacy Protection Guidelines, the Council of Europe adopted the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and, in 1992, the OECD adopted a recommendation on the "Guidelines for the Security of Information Systems". The OECD has now included at its web site a Privacy Policy Generator [1] to help anyone formulate a privacy policy that adheres to OECD guidelines. At the same time, the European Union was preparing for what eventually became Directive 95/46/EC on "The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (Commission, 1995). As it is in the process of being formally accepted by the Member States, this action effectively legislated data protection across Europe.

It is important to note that these actions were not originally intended to include data collected on the Internet, but, in order to make the connection clear, the Council of Europe accepted Recommendation No. R(99)5, "Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways", in February 1999 and the European Commission made sure that it was "compatible with EU directives and actively promote[d] the protection of privacy" (Commission, 1998). Subsequently, in March 1999, "European Union data privacy regulators... served notice that they do not want companies to market Internet software or hardware that collects information about Europeans without their knowledge" (Commission, 1999).

Not only is data privacy regulated throughout Europe, it is also institutionalized. Each EU country has established a data protection commissioner assigned to a ministry or agency. [2] "Those who collect information must register with the au-

[1] See web page at http://www.oecd.org/scripts/PW/PWHome.asp. Accessed: 21 April 2000.

[2] See list at http://europa.eu.int/comm/internal_market/en/media/dataprot/links.htm, providing office and web site contacts. Created: 15 September 1998. Accessed: 5 October 2000.

thority and describe their data protection policies'' (Haufler and Bessette, 2000, p. 10).

The consistent thread running through discussions in both the United States and the European Union is a desire for fair and equitable uses of information. As stated above, these have been articulated in various forms as Fair Information Practices.

2.3. Fair information practices

In a 1999 report, the Federal Trade Commission reiterated the importance of the main elements of fair information practices in five categories: notice, choice, access, security, and contact. [3] The practices are meant to empower individuals by alerting them to data collection and ensuring their ability to control their personal information. These guidelines were specifically designed to be technology-neutral and to apply to all types of data so that they could evolve along with developments in data collection and processing. ''Despite technological advances, and the evolution of an electronic environment based on world-wide information and communications networks, the Guidelines are still applicable today'' (OECD, 1998).

''Notice'' lies at the heart of fair information practice. This element mandates that a data-collecting entity clearly tell the subject exactly what information is being collected, how it is collected, how that information will be used, and with whom it will be shared. Many of these descriptions are particularly important online where collection may not be obvious. Specifically, a web site should explain whether or not it utilizes cookies and for what purpose. Ideally, a site would post its privacy policy in an easily accessible place with a link on its homepage or any other page that collects information. Without notice, a consumer essentially has no idea about the data-collection process, and therefore can exercise no control. Notice is absolutely essential for any of the other fair information practices to be effective.

The second element, ''choice'', allows consumers to actually exercise control over the use of their data. For example, a web user could choose not to receive e-mail from a web site or could ask that the site not share his or her data with another company. There are two main types of choice provisions: opt-in and opt-out. Opt-in requires a site to obtain explicit permission before using a visitor's data (e.g., ''check this box to receive our catalogue''), while opt-out requires users to tell the collector *not* to use their information. Opt-in choices generally afford more protection because they require a conscious decision by the consumer before a collector can use the data. As part of the choice element, the collecting organization should explain the ramifications of not providing data.

[3] ''In 1980 the... OECD expanded on these principles by adopting a set of eight FIP. The principles of purpose specification, use limitation, and individual participation were added.... The OECD principles were adopted by 24 countries including the US.'' See Givens (1999).

"Access" allows individuals to easily review the information that has been collected about them. It also gives consumers the ability to correct inaccurate information. The privacy policy should describe how an individual could request a correction. This element helps consumers monitor data collectors and ensure that their information is kept up to date.

"Security" requires data collectors to protect their gathered information, both during transmission and storage. This means taking reasonable measures to prevent theft, loss, destruction, modification, or unauthorized access. Security is particularly important online where hackers can infiltrate databases.

Finally, fair information practices require that collectors provide subjects with reliable "contact" information. Without the ability to communicate with a data collector, an individual cannot effectively exercise other rights of choice and access. Furthermore, contact provisions may make collectors more accountable by ensuring that consumers have an easy method to submit complaints or questions. On the Internet, e-mail provides a simple means of contact between users and sites.

Fair information practices are the consensus criteria for evaluating privacy protection. They inform and empower consumers and citizens, and they have been recognized for more than 25 years by policymakers in the European Union, the United States and international organizations. Though the United States has not legislated these, they clearly appear in the EU Data Privacy Directive (notice, articles 6, 10, 11; choice, article 7; access, article 12; security, article 16, 17; and contact, article 14). A directive is not a law; it is a "direction to Member States to enact law.... The Data Protection Directive balances competing interests both directly, by mandating certain rules, and indirectly by permitting Member States to legislate accordingly" (Maxeiner, 1995, p. 96). As of April 2001, 11 of the member states have passed data protection legislation and laws are either pending or being discussed in the others (Commission, 2000).

Fair information practices have become accepted criteria for evaluating concerns about privacy protection as well. Though both the United States and the European Union have, in theory, followed these practices, their successful implementation is open to examination.

3. Responses to online privacy problems

Advocates, industry members, and policy makers in both the United States and the European Union have proposed myriad different approaches to deal with online privacy issues. Most potential solutions fit into four categories: laissez-faire, self-regulation, technology, and legislation/government. The approaches vary in their effective implementation and enforcement of fair information practices. Each approach has unique benefits and drawbacks, and, most likely, a combination of methods will be needed to fully address privacy issues. Some are more common in the United States, others in the European Union.

3.1. Laissez-faire

Laissez-faire means "hands-off". Free-market capitalists around the world have championed this approach of minimal government involvement in the marketplace, trusting an "invisible hand" to guide decisions towards the ideal equilibrium of supply and demand. Proponents of applying laissez-faire theories to online privacy believe that no outside action is necessary to produce the level of privacy protection that consumers want (Swindle, 1999). In both the European Union and the United States, laissez-faire is often encouraged as the best way to be profitable in the evolving online world.

The laissez-faire approach appeals to the e-commerce industry because it provides maximum flexibility. This approach's proponents claim that laissez-faire will produce the most ideal privacy practices. They believe that businesses will shape their policies according to consumer preferences, since economic success depends on increasing market share by attracting more consumers. This solution allows web sites to adjust their privacy practices fluidly without concern for fulfilling any static requirements. Supporters of laissez-faire emphasize the rapid-changing nature of the Internet as evidence that all web sites must be able to adjust their practices, including privacy protection measures, quickly and constantly (Singleton, 1999).

Laissez-faire's critics, [4] however, highlight evidence suggesting that businesses are not responding to consumer concerns adequately, producing privacy policies that do not fully address fair information practices. Critics question whether the theory of laissez-faire can actually work, especially if consumers do not have perfect information.

In theory, if consumers value their privacy, they will evaluate sites based on privacy protection and stop using sites that they deem unsafe. As consumers move away from sites that either fail to state their information practices or follow undesirable practices, these sites will fail from lack of usage. Meanwhile, web sites that practice consumer-friendly policies will flourish as consumers seek them out. Commercial sites, particularly those in competition, will try to enhance their privacy practices if they believe that they can attract more customers. Eventually, as consumers expect a higher level of protection, proper information practices will become necessary for entering the marketplace.

If the laissez-faire approach is effective, one should expect to see a trend over time toward better privacy practices, particularly among the most popular sites on the Internet. Consumers are concerned about their privacy and that these concerns affect their behavior toward web sites. Furthermore, privacy apprehension has been well documented over the past several years. Therefore, sites should be well aware of

[4] Critics include advocacy groups such as the Electronic Privacy Information Center, the Center for Democracy and Technology, the National Consumers League, the Consumer Federation of America, the Privacy Rights Clearinghouse, and the US Public Interest Research Group.

consumer attitudes, and, according to the theory, be changing their practices to attract customers. Specifically, more sites should be posting privacy policies, and these policies should increasingly reflect fair information practices.

Evidence shows that successful companies are beginning to recognize the benefits of increasing privacy protection. [5] In addition, studies by the Electronic Privacy Information Center (EPIC, 1999a,b, 1997) and Online Privacy Alliance (OPA, 1999a,b) show an increase in the number of popular sites with privacy policies. While this data cannot conclusively prove that laissez-faire is effective, the empirical evidence suggests that consumer pressure may be affecting business practices. However, while market forces have been increasing the *number* of posted policies, the *quality* of these policies still does not measure up to fair information practices.

Empirical evidence still shows that while more sites may be posting privacy policies, many sites are not addressing fair information practices. In the 1999 OPA survey, of the 94 sites that made some sort of disclosure, 93% at least partially addressed "notice", while 83% gave some element of "choice". Yet, only 50% addressed "access", 51% mentioned "security", and 59% gave contact information. The Georgetown Internet Privacy Policy Survey (GIPPS, 1999) found even worse results. Of their 236 sites that made some disclosure (65% of the total sample), 89% addressed notice and 62% mentioned choice. However, only 40% had access, 46% described security, and 49% gave contact information. Overall, only 13.6% of the sites with policies (only 9% of the entire sample) addressed all five fair information practices. Thus laissez-faire has yet to produce a significant percentage of web sites that adhere to fair information practices.

"Notice" is clearly the most frequently addressed element of fair information practices. Yet, analysis of posted policies indicates that the quality of disclosures is still insufficient. EPIC's 1999 survey found that only 51 sites had privacy policy links on their homepage, and only 35 had similar links on all pages collecting information. EPIC also criticized the quality of "notice", finding that only 58 sites specified why information was being collected. Additionally, EPIC found that at least one site lied about its use of "cookies" and implied that other sites may have been secretly using identifiers. Finally, EPIC concluded that many of the privacy policies they found were confusing, often using complex legal jargon.

This lack of complete and clear privacy policies presents a problem for the laissez-faire approach. The market theory, upon which laissez-faire relies, depends on

[5] A 1998 study at Vanderbilt University found that the most effective way for web sites to develop profitable relationships is through building consumer trust, specifically with stated policies that allow consumer-empowering interaction (see Hoffman, 1998). A different study by Shop.org identified "lack of trust and security issues" as the leading inhibitors of online shopping. Misuses of personal information and violations of privacy are clearly issues that contribute to a lack of trust. The study recommended that e-commerce companies must build relationships of trust a top priority in order to be successful (Shop.org, 1999). Similarly, Ernst and Young (1999) created its Center for Trust Online specifically to help web sites deal with issues like privacy.

consumers' abilities to make choices based on their personal preferences. However, consumers can only make these decisions with reliable, complete information. Thus, when consumers lack full information, their behavior cannot be assumed to accurately reflect their preferences. If policies continue to confuse consumers, market forces will not create the ideal level of protection that theory suggests. In fact, enforcing fair information practices is the best way to harness market forces, because these practices ensure that consumers have the full information needed to make informed choices. The continuing low percentage of sites adhering to fair information practices and lack of complete information indicate that the laissez-faire approach may not work effectively unless an external presence forces their implementation.

3.2. Industry self-regulation

While laissez-faire operates at the level of the individual web site, self-regulation works at a broader industry level through associations of sites. Industry self-regulation, like laissez-faire, allows businesses to be flexible with their privacy practices, suggesting that it is an efficient approach to privacy concerns. Additionally, self-regulation is more pro-active than laissez-faire, providing more oversight of web site policies while allowing industry experts and privacy specialists to tailor requirements. Still, critics argue that self-regulatory efforts have not been proven to effectively implement fair information practices. Specifically, they claim that self-regulation still does not guarantee the quality of privacy policies and lacks effective enforcement mechanisms.

For the past several years, the federal government, industry members, and private associations have touted self-regulation as the answer to privacy concerns. Recognizing both the need for privacy protection and the fast-changing nature of the Internet, government authorities have maintained that the online industry could best solve privacy problems through its own initiatives, without intrusive government involvement. President Clinton advocated self-regulation in his 1997 "Directive on E-commerce", stating

> For electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever appropriate and support private sector efforts to develop technology and practices that facilitate the growth and success of the Internet (Clinton, 1997).

In a 1998 report to the US Congress, the FTC called self-regulation "a more efficient and effective means of creating online privacy protections than government regulation" (Federal Trade Commission, 1998). While self-regulatory schemes benefit from their ability to adapt quickly to consumer demands and commercial needs, they have produced mixed results in adequately addressing privacy issues. Some

tools of self-regulation are seal programs, industry guidelines, privacy organizations, and, more recently, the US/EU safe harbor initiative.

3.3. Seal programs

Seal programs establish criteria for judging privacy practices. Web sites can apply to these programs, and, if a site's privacy policy meets the program's requirements, the site can pay a fee to display the program's seal. The seal indicates to consumers that the particular site adheres to the program criteria, and users can usually click on the seal to view the requirements. If quality seal programs became ubiquitous and easily recognized by web users, seals would provide consumers with a quick and reliable way to verify a site's privacy practices. Most seal programs were initiated in the United States, but have recently begun to provide their seals to European web sites as well.

One popular seal program is TRUSTe (2000), which was launched in 1996 and grew to 100 participants by June 1997. Between 1997 and 1998, TRUSTe launched its Privacy Partnership with the cooperation of major portal sites and enlisted the sponsorship of Microsoft, Netscape, America Online, IBM, and other industry leaders. TRUSTe is currently the largest seal program with about 800 members. Only a few European organizations are members. The online auction house QXL.com was one of the first European companies to become a licensee of TRUSTe. [6]

The Council of Better Business Bureaus launched the BBBOnline (1999) seal program in 1998 and has awarded approximately 250 seals. While BBBOnline has fewer participants than TRUSTe, the program's affiliation with the Better Business Bureau's established brand name makes consumers more likely to trust its seal (Cranor, 1999). AT&T, Dell Computers, American Airlines, and eBay are among BBBOnline's participants.

Some seal programs, many of which are branching out to European companies, justify the reliability of a specific sector on the Internet, but do not address privacy issues. An example is ePublicEye.com (2000), an online service which rates the privacy reliability of online shopping sites. In February 1999 it became the first US-based e-business rating company to localize its services for the French market, working with the French company eBuyClub, and in January 2000 began publishing its services in German and Spanish as well.

Most privacy-oriented seal programs cover fair information practices, requiring their participants to notify consumers how their information will be used, whether or not it will be shared, how to opt-out of sharing or providing information, how to change submitted data, how data is protected, and how to contact the web site. Also, seal programs offer a complaint resolution process in which they act as mediators

[6] See Privacy Policy at www.qxl.com. Accessed: 5 October 2000.

between the consumer and the web site. The programs may also investigate complaints if necessary.

SecureAssure (1999), a new seal program launched late in 1999, takes privacy policy requirements a step further. While other programs allow their participants to share information with third parties as long as they explicitly notify consumers of the practice, SecureAssure strictly prohibits its clients from sharing information or using it for any purpose beyond its primary use. SecureAssure further requires participants to receive explicit, ''opt-*in*'' permission to send promotional materials, whereas the more established seals allow opt-in or opt-out. SecureAssure also provides a conflict resolution process.

Seal programs uphold fair information practices and seemingly offer an efficient, self-regulatory solution to privacy concerns. However, these programs have two major problems: lack of participation and lack of meaningful enforcement. The two most popular seal programs, TRUSTe and BBBOnline, have only 1050 participants combined, an infinitesimally small percentage of the total number of Internet sites. EPIC's 1999 study showed that only 20 of the top 100 shopping sites belong to one of these two programs. While seal programs are relatively new and will undoubtedly grow, they are still not a comprehensive privacy solution.

Furthermore, seal programs lack the means – and perhaps the will – to provide meaningful enforcement of their policies. While both major programs offer a conflict resolution and investigation process, neither can provide much redress in the event of a violation. At worst, the program can revoke the seal, much as an industry association can expel a member. While such an action could produce negative publicity for the violating site, the program cannot apply more direct punishment.

Moreover, TRUSTe has shown a reluctance to take any action in high profile complaint cases. In 1998, the FTC settled a privacy-violation suit with the web company GeoCities. The investigation revealed that GeoCities had been violating privacy standards while they applied for, and were awarded, a TRUSTe seal. TRUSTe made no mention of the violations until after the FTC settled the case (McCarthy, 1999). In another case, in March 1999, Microsoft breached its TRUSTe seal by imbedding trackable unique identifiers in software. TRUSTe skirted the issue, deciding that Microsoft had compromised consumer privacy, but had not broken their agreement (Rotenberg, 1999). Later that year, hackers discovered a loophole in Microsoft's Hotmail security, which left thousands of private user e-mail accounts open to violation. Still, TRUSTe took no action until after the problem became public and even then only hired an outside accounting firm to help Microsoft fix the problem. The Microsoft case raises particular concern since Microsoft is one of TRUSTe's several industry sponsors. TRUSTe's reluctance to punish Microsoft may have stemmed from a conflict of interest.

Still, TRUSTe's reluctance to enforce its own policies against violating participants raises concern about the effectiveness of seal programs. The comprehensive fair information practices that seal programs support are meaningless if participants are not held to their agreements. While TRUSTe's actions may not be indicative of other

programs' willingness to enforce policies, the fact that the most widely used program does not seem to be completely trustworthy indicates that seal programs are not an effective answer to privacy concerns yet.

3.4. Industry guidelines

Industry guidelines aim to set industry-specific standards for related businesses, often through an established association, like the Direct Marketing Association or the Bankers Roundtable. Since these associations obviously have detailed knowledge of their particular industry, they can tailor privacy guidelines for their members. Theoretically, privacy strategies that account for distinct aspects of businesses could be implemented more efficiently and effectively than broad rules made to govern all web sites.

Several industry associations have crafted privacy guidelines and suggestions for their members. The Direct Marketing Association (1999) instituted its "Privacy Promise", committing its members to notifying customers of their ability to opt-out of information sharing and solicitation. The DMA also provides an online handbook to help its members follow the Association's guidelines. In 1999, the Office of Thrift Supervision (OTS) similarly announced a rule requiring its members to post privacy policies on their transactional web sites. The OTS also urged members to tell customers how their information would be used, allow customers to limit the use of information, and ensure that customer information is kept accurate and secure (Thrifts Urged, 1999).

The World Association of Research Professionals, a professional organization for marketing researchers based in The Netherlands, are "encouraged to post their privacy policy statement on their online site" and assure that the policy is easy to find. The association only suggests the action and does not provide any penalties for non-compliance. Yet, as opposed to the United States, there is a fallback. "All research carried out on the Internet must conform to the rules and spirit of the... Data Protection [the EU Directive] and other relevant legislation (both international and national)" (World Association for Research Professionals, 2000).

Unfortunately, most industry guidelines do not fully address fair information practices. In preparation for its 1998 report to Congress, the FTC reviewed nine sets of industry-specific guidelines. The Commission found that all rules urged notice of some (but not all) information collection practices, and most suggested allowing consumers to opt-out of information sharing. Virtually none of the structures mentioned access or security provisions. Even more importantly, the submitted guidelines provided no enforcement mechanisms to ensure the implementation of industry guidelines. Some organizations, like the Magazine Publishers of America, merely present privacy principles as suggestions or best practices without any actual requirement for members to adopt them (Kummerfeld, 1999). While other groups do require its members to follow the industry's established guidelines, they have little

power to enforce this mandate. At the very worst, an industry association could revoke a company's membership in the association, possibly causing some bad publicity for the business. Yet such actions may not harm the wrongdoer very much and provide no redress for abused consumers. Therefore, industry guidelines not only fail to fully address fair information practices, they also lack the ability to provide meaningful enforcement.

3.5. Professional associations

Various private interests have formed professional monitoring organizations other than seal programs to encourage the development of self-regulation. The Online Privacy Alliance, for example, is a group of corporations and industry associations "who have come together to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals' privacy online" (OPA, 1999a). The Alliance tries to advance self-regulation by keeping members informed of privacy developments, providing a forum for debates, and helping web sites develop privacy policies that include elements of notice, choice, access, and security. The OPA includes many major corporations and web sites, including AT&T, eBay, Disney, and Yahoo. Ironically, however, some of the OPA's members, like DoubleClick and Real Networks, have been consistently criticized for their information practices.

Another organization, Global Information Infrastructure (1999), is comprised of global businesses and media companies. It is dedicated to educating businesses on how to use the Internet effectively and fairly. GII has a standard of best practices that includes establishing privacy policies according to fair information practices. Organizations like GII could help encourage effective self-regulation through education of both businesses and consumers.

3.6. Safe harbors

A final area of self-regulation is "safe harbors". This is the area of most interest to relations between the United States [7] and the European Union. Since October 1998, the effective date for the Directive on Data Protection, each has been negotiating for an acceptable method of information exchange. Safe harbors are the tentatively accepted result. Under this agreement, US industry would voluntarily implement the more stringent EU rules for data exchange and, thus, be part of a list of sanctioned entities with whom EU entities can do business.

In March 2000, negotiators from both sides of the Atlantic had reached a tentative conclusion, subject to approval by the EU member states. In July, the

[7] See Department of Commerce web page, which has gathered information on US views of the process. Created: 21 July 2000. Accessed: 5 October 2000. http://www.ita.doc.gov/td/ecom/menu.htm.

European Commission accepted the safe harbors arrangement. Even though both sides are cautiously optimistic, not everyone believes it will work. Not only must the agreement be approved by EU member states, "the Europeans believe that any scheme that is voluntary cannot work without some independent monitoring and investigative capacity and sanctions for non-compliance" (Haufler and Bessette, 2000, p. 14). US privacy advocates also fear that "US companies that participate in the safe harbor pact may have separate privacy policies for the US and European customers" (Thibodeau, 2000, p. 6).

This fear that self-regulation might not work was echoed by the FTC. In its 1999 Report to the US Congress, the organization concluded that self-regulatory initiatives still had not effectively taken hold. The Commission admitted that, despite several years of encouraging private-sector initiatives, only a small percentage of web sites participated in self-regulation programs and the majority of sites had not implemented fair information practices. Despite these findings, the FTC still concluded that industry was making a substantial effort to make self-regulation effective. The Commission further recommended that the federal government should continue to encourage self-regulation instead of drafting legislation or attempting other government intervention measures.

While self-regulation certainly addresses fair information, these measures cannot guarantee the actual implementation of and adherence to fair information practices. Although self-regulation continues to provide a good appearance of working towards better privacy protection, this image is worthless to consumers without meaningful enforcement.

3.7. Technological solutions

Both commercial and non-profit organizations have developed technological measures to protect privacy rights online. These approaches mostly include working with web browser software, either through plug-in applications or with the programs themselves. All of these solutions attempt to give consumers greater control over their information by making sites' collection practices more explicit. Technological measures can be easy for consumers to use, often requiring little effort after an initial set-up. Also, designers can constantly update and upgrade their programs to keep them effective. However, similar to self-regulatory programs, technological efforts cannot enforce privacy policies.

The most comprehensive and promising technological solution currently being developed is the World Wide Web Consortium (1999) Platform for Privacy Preferences Project (P3P). The Consortium (W3C) follows the Internet's tradition of cooperation by bringing together computer-science organizations from around the world to develop common Internet protocols and insure the Web's interoperability. Once implemented, P3P would allow web sites to express their privacy policies in a standard format with standardized language. Like seal programs, P3P would give

web users a quick and easy way to verify the quality of a site's privacy policy without reading through the policy itself. Furthermore, P3P would ensure that privacy statements are clear and understandable. This method of simple certification lowers the "cost" to consumers of being informed about a site's information practices, thus increasing the likelihood that a consumer will make an informed decision about providing information.

P3P could be built into web browsers or browser plug-ins. When a web user visits a site, the browser would automatically find the P3P evaluation and display symbols, sounds, and prompts that reflect the site's privacy practices. The browser would also indicate where the user could find and read the specific policy. Furthermore, P3P can compare a site's privacy practices to a user's personal privacy preferences and automatically take appropriate action to safeguard these preferences. In future versions, the designers of P3P also hope to allow sites to offer visitors a choice of policies. This feature could help sites take advantage of market forces, perhaps by offering trade-offs between select services and higher privacy protection. Such a choice could give consumers even greater control over their privacy and allow them to exercise their preferences more effectively.

The W3C admits that, while P3P provides an excellent tool for keeping consumers informed of sites' information practices, it has no means of verifying whether or not a site actually practices what its policy states. Thus, even with P3P, consumers would need other mechanisms to ensure that stated policies are actually followed and that complaints are being addressed. Another concern about P3P relates to implementation. The W3C is still developing P3P. The designers made their "last call" for comments on their working paper in November 1999. While the W3C encourages the development of P3P prototypes for feedback purposes, the designers do not want to begin implementing the system before it is completed.

In order to make P3P effective, a majority of web sites would have to craft policies using the protocol's standardized language. Given that numerous web sites still lack privacy policies, P3P will probably not become an effective method for protecting privacy for a few years. [8]

Technology certainly offers useful mechanisms for helping consumers protect their privacy. Unfortunately, the most effective and comprehensive of these measures, P3P, is not complete yet. Furthermore, none of the technologies offers a complete solution. They mostly help consumers use privacy policies more effectively, but do not guarantee that the policies will reflect fair information practices. While these mechanisms can certainly supplement other privacy efforts, other measures must ensure policy enforcement.

[8] There are other technological solutions working on a basis similar to P3P. See Enonymous (1999) and AdSubtract (2000).

3.8. Government action

Finally, the government could address privacy concerns through its own action rather than relying on the self-regulatory and technological initiatives of the private sector. Many privacy advocates and legislators have argued that the US Congress should pass legislation requiring businesses to follow fair information practices as has been done in the member states of the European Union. While critics maintain that government action creates burdensome, inflexible regulation and that self-regulation remains the best solution to privacy problems, consistent weaknesses found in current private sector efforts and the apparent success of the EU Directive indicate that government involvement is inevitable and necessary.

In fact, legislative action solves two problems consistently found in self-regulatory efforts: (1) lack of incentive, (2) lack of enforceability, redress, and punishment. While web sites certainly have an interest in protecting their customers, businesses' primary incentive is to appear trustworthy, in order to reduce consumer apprehension and encourage more commerce. Thus, sites are motivated to at least acknowledge privacy and mention some protection practices, but they may not feel compelled to address all fair information practices. Subsequently, the GIPPS study found few sites that fully adhere to fair information practices. However, by legally requiring web sites to follow fair information practices, the government can induce more robust adherence to privacy standards.

Government can enforce privacy requirements more effectively than private entities. Seal programs and industry organizations lack the capability, authority, and, in some instances, the willingness to enforce their standards and hold their members to stated policies. The most severe punishment these groups can administer is to revoke the offender's membership, a rather minor rebuke. Furthermore, private programs give consumers no way to obtain redress for violations. Alternatively, the government can impose financial penalties on deviant sites and guarantee consumers' rights to redress.

4. Conclusion

Should governments know the extent of privacy problems before they legislate, or is privacy important enough to initiate regulation before the problems are clear? The European Union and the United States have answered this question in different ways. Early attempts at legislation in Europe were much broader in scope than those in the United States, including both the public and private sector as well as electronic and manual databases. [9]

[9] "In most countries it was recognized that the principles were the same for the two kinds of administration, but that in the computerized sector the need for legislative intervention was greater in view of the capabilities of the medium. The trend was therefore to adopt general rules for electronic registers and special rules for certain kinds of manual registers" (Hondius, 1975, pp. 21–22).

The public vs. private debate was not as controversial in Europe as in the United States. "Those in favor of a single law applicable to data processing in the two [public and private] sectors pointed out that it is often an arbitrary matter whether a certain service or facility is located in one sector or the other" (Hondius, 1975, p. 22). In fact, there was some argument that the public sector did not need any more control because existing legislation already made its privacy practices transparent. Therefore, rules and laws need be formulated *only* for the private sector.

The rationale for regulation differs in each as well. "US institutions and culture generally favor commercial interest except when national security issues come into play. EU institutions generally are less friendly to commercial interests but at the same time less likely to let national security limit potential commercial benefits" (Haufler and Bessette, 2000, p. 2).

The full success of the EU Directive cannot yet be determined. In principle, both European-based organizations as well as other organizations working in Europe have begun to subscribe to the Directive's privacy protection requirements. [10] And, the legislation seems to have addressed some of the weaknesses in the other approaches.

Some European counterparts to US privacy advocacy groups have been created over the past few years to encourage both the adoption of general privacy practices and the application of the Directive. Interestingly, they are working for even stronger legislative action than has already been articulated in the existing EU Directive. "Save the Web: The Movement to Save Europe's Internet" states, "The Privacy Directive needs to be amended to address the real threats to privacy, and so that prior permission is required only when somebody else's privacy is really threatened" (Save the Web, 1999).

Critics of the legislative approach in the United States generally worry that the legislative/regulatory process is too slow and bureaucratic to effectively govern the Internet and that regulations will become burdensome and unnecessary. These critics alternatively favor more adaptable self-regulation.

However, legislation in the United States would merely require web sites to adopt fair information practices that have existed for almost 20 years and are as applicable today as ever. It is unlikely that fair information practices will suddenly become burdensome or unfair to businesses. Legislation need not dictate exactly how businesses use information; it would only provide a framework for helping consumers make choices. In fact, legislation would not require web sites to do any more than the best self-regulatory programs. Therefore, concerns that regulations will be more burdensome than self-regulation are unfounded. Also, since Congress and the FTC already have the Children's Online Privacy Protection Act (COPPA). [11]

[10] See some of the cases described in Gauthronet and Nathan (1998).

[11] Though parts of this act have not passed muster in the courts, much could be used in future Internet regulation. See COPPA (1998) as a model for regulations, the rule-making process could progress faster than usual.

Finally, legislation does not necessarily mean the end of self-regulation. Laws could work with self-regulatory efforts, like seal programs, harnessing the adaptability of self-regulation and the government's enforcement capability. In fact, a blend of legal, self-regulatory, and technological measures will probably yield the most effective solution.

> Providing a seamless web of privacy protection to data as it flows through [the Internet] will require us to harness the business community's interest in promoting commerce, the government's interest in fostering economic growth and protecting its citizens, and the self-interest of individuals in protecting themselves from the over-reaching of the government and private sectors. It requires us to use all of the tools at our disposal – legislation, self-regulation, public education, and technology (Berman and Mulligan, 1999, p. 557).

References

AdSubtract, 2000. Products. Created: 8 February 2000. Accessed: 12 February 2000. http://www.adsubtract.com/products.html.

BBBOnline, 1999. BBB*OnLine* Privacy Program. Created: March 1999. Accessed: 2 October 1999. http://www.bbbonline.com.

Bennett, C.J., 1992. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Cornell University Press, Ithaca, NY.

Berman, J., Mulligan, D., 1999. Privacy in the digital age: work in progress. Nova Law Review 23 (2), 551–582.

Ernst and Young, 1999. Center for Trust Online. http://www.ey.com/global/gcr.nsf/US/Welcome_-_Center_for_Trust_Online_-_Ernst_%26_Youn ng_LLP.

Children's Online Privacy Protection Act, 1998. Title 15 *US Code*, http://uscode.house.gov (Chapter 91).

Clinton, B., 1997. Presidential Directive on Electronic Commerce. Created: 1 July 1997. Accessed: 12 November 1999. http://www.ecommerce.gov/presiden.htm.

Commission of the European Communities, 1995. The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC, Adopted: 24 October 1995, Official Journal L 281, 12/11/1995, pp. 31–50, Brussels.

Commission of the European Communities, 1998. Protection of Privacy on the Internet: The Commission keeps and Eye on the Guidelines Drawn Up by the Council of Europe and Asks to Negotiate. Created: 27 January 1998. Accessed: 5 October 2000. http://europa.eu.int/comm/internal_market/en/media/dataprot/news/87.htm.

Commission of the European Communities, 1999. EU regulators propose strict privacy policy. Created: 4 March 1999. Accessed: 21 April 2000. http://news.cnet.com/news/01005200339541.html?st.ne.140.-head.

Commission of the European Communities, 2000. Status of implementation of Directive 95/46. Accessed: 20, April 20 2000. http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm.

Cranor, L.F., 1999. Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. Created: 14 April 1999. Accessed: 12 September 1999. http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm.

Direct Marketing Association, 1999. The DMA Privacy Promise. Created: 1 July 1999. Accessed: 2 October 1999. http://www.the-dma.org/library/privacy/privacypromise.shtml.

Electronic Privacy Information Center, 1999a. Surfer Beware III: Privacy Policies Without Privacy Protection. Created: December 1999. Accessed: 7 February 2000. http://www.epic.org/reports/surfer-beware3.html.

Electronic Privacy Information Center, 1999b. Privacy Center Calls for Strong Protections for Users. Created: 27 July 1999. Accessed: 9 April 2000. http://www.epic.org/release/7_27_1999.html.

Electronic Privacy Information Center, 1997. Surfer Beware: Personal Privacy and the Internet. Created: June 1997. Accessed: 7 February 2000. http://www.epic.org/reports/surfer-beware.html.

Enonymous, 1999. Privacy Made Simple. Created: 4 October 1999. Accessed: 12 February 2000. http://www.enonymous.com/default2.asp.

ePublicEye. Accessed: 20 April 2000. http://www.thepubliceye.com/pr19.htm.

Federal Trade Commission, 2000. Privacy Online: Fair Information Practices in the Electronic Marketplace. Created: 22 May 2000. Accessed: 5 October 2000. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

Federal Trade Commission, 1998. Privacy Online: A Report to Congress. Created: June 1998. Accessed: 13 October 1999. http://www.ftc.gov/reports/privacy3/toc.htm.

Gauthronet, S., Nathan, F., 1998. Online Services and Data Protection and the Protection of Privacy, Part 1. Study for the Commission of the European Community, DG XV, December 1998. http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/index.htm.

Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission, 1999. Created: 21 July 1999. Accessed: 12 September 1999. http://www.msb.edu/faculty/culnanm/gippshome.html.

Givens, B., 2000. The Emperor's New Clothes: Privacy on the Internet in 1999. Created: May 1999. Accessed: 13 April 2000. Privacy Rights Clearinghouse. http://www.privacyrights.org/AR/emporor.htm.

Global Information Infrastructure, 1999. The Standard for Internet Commerce. Created: 14 December 1999. Accessed: 9 February 2000. http://www.gii.com/standard/commercestandard.pdf.

Haufler, V., Bessette, R., 2000. Why there is no international regime for information privacy protection. In: Paper presented at the Annual Meeting of the International Studies Association, Los Angeles, California, March 15–18.

Hoffman, D., 1998. Building Consumer Trust in Online Environments: The Case for Information Privacy. Created: December 1998. Accessed: 22 November 1999. http://www2000.ogsm.vanderbilt.edu/papers.html.

Hondius, F.W., 1975. Emerging Data Protection in Europe. North-Holland, Amsterdam.

Kummerfeld, D.D., 1999. Letter to the Federal Trade Commission. Created: 31 March 1998. Accessed: 13 October 1999. http://www.ftc.gov/reports/privacy3/append-e.pdf.

Labaton, S., 2000. White House and agency split on internet privacy. The New York Times, C1.

Maxeiner, J.R., 1995. Freedom of information and the EU data protection directive. Federal Communications Law Journal 48 (1), 93–104 (footnote 9).

McCarthy, J., 1999. TRUSTe Decides Its Own Fate Today. Created: 8 November 1999. Accessed: 10 February 2000. http://slashdot.org/yro/99/11/05/1021214.shtml.

Online Privacy Alliance, 1999a. Background. Accessed: 12 October 1999. http://www.privacyalliance.org/join/background.html.

Online Privacy Alliance, 1999b. Privacy and the Top 100 Web sites: Report to the Federal Trade Commission. Created: 8 June 1999. Accessed: 12 October 1999. http://www.msb.edu/faculty/culnanm/gippshome.html.

Organization for Economic Cooperation and Development, 1980. Explanatory Memorandum. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 9.23.1980. Paris, OECD. http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM.

Organization for Economic Cooperation and Development, Group of Experts on Information Security and Privacy, 1998. Implementing the OECD Privacy Guidelines in the Electronic Environment. Created: 9 September 1998. Accessed: 8 October 1999. http://www.oecd.org.

Reidenberg, J., Schwartz, P., 1996. Data Privacy Law: A Study of United States Data Protection. Michie, Charlottesville, Virginia.

Rotenberg, M., 1999. Testimony and Statement for the Record before the House Subcommittee on Courts and Intellectual Property. Created: 27 May 1999. Accessed: 9 September 1999. http://www.epic.org/privacy/internet/EPIC_testimony_599.html.

Save the Web: The Movement to Save Europe's Internet, 1999. Created: 14 September 1999. Accessed: 5 October 2000. http://www.savetheweb.org/threatpr.htm.

SecureAssure, 1999. Created: 26 October 1999. Accessed: 9 February 2000. http://www.secureassure.org.

Shop.org, 1999. State of Online Retailing 2.0. Created: 19 July 1999. Accessed: 25 January 2000. http://www.shop.org/research/summary.htm.

Singleton, S., 1999. Innovation Versus Privacy. Created: 13 Augest 1999. Accessed: 9 April 2000. http://www.cato.org/dailys/08-16-99.html.

Swindle, O., 1999. Regulation of Privacy on the Internet: Where Do You Want to Go Today? Created: 8 April 1999. Accessed: 9 April 2000. http://www.ftc.gov/speeches/swindle/reston.htm.

Thibodeau, P., 2000. Europe and US agree on data rules. Computerworld 34 (12), 6.

Thrifts Urged to Post Privacy Policies As Part of Transactional Web Sites, 1999. Bank Bailout Litigation News. Created: 16 July 1999. Lexis-Nexis Academic Index. Accessed: 6 September 1999.

TRUSTe, 2000. The TRUSTe Story. Accessed: 9 February 2000. http://www.truste.org.

World Association for Research Professionals, 2000. Conducting Marketing and Opinion Research Using the Internet. Accessed: 21 April 2000. http://www.esomar.nl/guidelines/internet_guidelines.htm.

World Wide Web Consortium, 1999. About the World Wide Web Consortium. Created: December 1999. Accessed: January 2000. http://www.w3.org/Consortium/.