

PRIVACY RIGHTS ON THE INTERNET: SELF-REGULATION OR GOVERNMENT REGULATION?

Norman E. Bowie and Karim Jamal

Abstract: Consumer surveys indicate that concerns about privacy are a principal factor discouraging consumers from shopping online. The key public policy issue regarding privacy is whether the US should follow its current self-regulation course (where the FTC encourages websites to obtain private "privacy web-seals"), or whether a European style formal legal regulation approach should be adopted in the US.

We conclude that the use of assurance seals has worked reasonably well and websites should be free to decide whether they have a privacy seal or not. Given the narrow scope and the wide variety among these seals, we do argue that the seals should commit themselves to the key features of a good privacy policy and that an opt-in provision be required. We believe that insufficient evidence exists to propose formal Government mandated Internet privacy regulation.

Introduction

Most people support a right to privacy. Philosophers have provided a number of arguments that justify a right to privacy although there are certain situations where many would agree that privacy rights need to be sacrificed either in order to honor other rights or for the general public good (Etzioni 1999). Until the last decade of the twentieth century, privacy rights focused on the intimate details of one's life—one's right to be silent about one's sexual preference, and one's political affiliation, for example. In addition, there was a general concern about providing government or other institutional authorities with too much information and with government snooping. There was less concern with privacy in marketing.

With the Internet and the development of marketing by e-commerce, privacy issues became more complicated as a result of the new technology. However, philosophers have said less about these new privacy issues.¹ This is unfortunate since concerns about privacy have limited the development of e-commerce marketing. According to Tedeschi (2000) a New York Times report on a survey of Internet users indicates that privacy is the chief reason why people do not shop online and that 92 percent of online households do not trust online companies to keep their information private. Another survey showed that 70 percent of the respondents were more concerned about privacy on the Internet than on any other medium.² Yet

another survey indicated that privacy was the number one issue facing the Internet.³ Indeed, consumer concern is so high that the latest version of Internet Explorer—IE 6.0—has been set so that the default is “No” for accepting third-party cookies. This is in accordance with P3P⁴ standards that are designed to protect Internet privacy.

This paper is concerned with a major public policy issue with respect to marketing in e-commerce. The public policy issue at the focus of this paper is whether the United States should adopt the formal (legal) regulation of privacy in e-commerce that has been adopted by the European Community or whether the United States should allow the self-regulation that is underway to continue. Given the data that is available what should be done next? In particular how much of a role should be left to voluntary self-regulation and how much to government regulation?

Section one begins with a normative question: What are the elements of a good privacy policy? To answer that question we need to answer a further question: Do some types of information deserve more protection than others? For example, should information about one's health be more strictly protected than information about one's buying habits? In order to address these two issues, we will discuss some of the philosophical justifications given for a right to privacy and review some of the occasions where honoring a right to privacy may not be in the public interest. Those considerations will enable us to propose criteria for a morally acceptable privacy policy and for determining if there should be a hierarchy of information to be protected with some information deserving more protection.

Section two presents current privacy law regarding e-commerce in the United States and the European Community. Regulation in the United States is mostly limited to self-regulation through privacy seal programs while the European Union has more extensive government regulation. Our intent in this section is to see how well both voluntary self-regulation and existing government regulation incorporate the elements of a good privacy policy presented in section one.

Section three presents empirical evidence that examines disclosure practices, effectiveness of opt-out options, and registration policies of high-traffic US websites. Some comparative evidence is also collected from the UK where websites are required to conform to EU privacy law. Section four presents our analysis for settling the central public policy issue.

I. The Elements of a Good Privacy Policy

In order to suggest the elements of a good privacy policy we need to be familiar with some of the justifications for a right to privacy in general.

Traditional Philosophical Justifications for a Right to Privacy

Let us start with the position of Immanuel Kant. We endorse Kant's view that persons ought to be treated with respect. One condition for treating people with respect is that we honor their individual autonomy.⁵ What distinguishes us as human beings from everything else on earth is the fact that we have free will or are

autonomous. As O'Neill (1989) has pointed out, Kant believed that autonomy is the ground of rationality and morality.

He [Kant] argues not from reason to autonomy but from autonomy to reason. Only autonomous self-disciplining beings can act upon principles that we have grounds to call principles of reason . . . it [the categorical imperative] is the fundamental strategy not just of morality but of all activity that counts as reasoned. The supreme principle of reason is merely the principle of thinking and acting on principles that can [not do!] hold for all.

Since we are autonomous beings, we are capable of rationality (making laws unto ourselves), responsible decision making and of being subject to the moral law. Freedom, or autonomy, has intrinsic value and we have an obligation to respect freedom and support those values and institutions that contribute to freedom.

Joseph Kupfer (1987) has argued that privacy is a necessary condition for the development of autonomous selves. His argument for that position runs as follows: Privacy is necessary for an efficacious self-concept and an efficacious self-concept is in turn required if one is to be an autonomous self.

Why is privacy necessary for the development of an efficacious self-concept? Kupfer begins with developmental psychology. A child who experiences privacy, secrecy, and perhaps even lying learns that she has some control over her life and a sense of control of one's life is necessary for autonomy. Furthermore, empirical evidence shows that people who are deprived of control over their lives, in nursing homes, prisons, and hospitals, for example, "lose the sense of themselves as origins of thought, purpose, and action" (Kupfer 1987).

Second, privacy also allows us to rehearse changes in life style in the privacy of our own homes to be something we are not. This ability to try on different personas also contributes to a concept of the self that is in control of his or her life.

Yet a third value of privacy to an autonomous self-concept is the fact that being permitted privacy allows one to perceive oneself as trustworthy. This feature of privacy is particularly relevant to the business context. The use of drug tests, two way mirrors, and screening devices, as well as close monitoring by supervisors, provides little or no privacy and conveys the message that one is not trustworthy. The absence of these features indicates a degree of a trustworthiness that in turn contributes to the notion of an autonomous self.

Finally, privacy enables us to choose with whom we share personal intimate information. Our control over with whom to share intimate information helps us to distinguish between friends and acquaintances. As Kupfer (1987) says, "privacy enables us to define ourselves socially in terms of intimate relationships." Thus, a right to privacy is a social good that enables persons to develop as autonomous selves. It is this capacity for autonomy that is the grounds for the moral obligation to respect people.

In summary, a person cannot develop as an autonomous individual unless he or she has some privacy over personal information. To respect a person's autonomy requires that we respect the conditions that make autonomy possible. Thus, we must, at least

to some extent, respect a person's privacy. With respect to marketing in e-commerce, we should impose conditions that make an individual's privacy efficacious.

Rights in Conflict: When Should the Right to Privacy Give Way?

Despite the value of privacy to the development of an autonomous self-concept, we recognize that the right to privacy is not absolute. Before the terrorist attacks on the United States on September 11, 2001, efforts were underway in a number of states and in the US Congress to increase the protection of the privacy rights of American citizens. Since that date, the momentum for such action has understandably slowed. But circumscribing privacy rights to protect us from terrorist attack is not the only limitation we are willing to put on privacy rights.

In the medical field we know that the number of mistakes, especially in the prescription and administration of medication, can be drastically lowered if we had computerized records. And if the databases were national, a physician in one part of the country could have access to your entire medical record. Canada and Germany already have such systems. Privacy advocates are vehemently opposed to the establishment of such a national system in the United States.⁶ Privacy advocates have even found the establishment of a device that contains your entire medical record to be objectionable. This despite the fact, that there are 120,000 preventable deaths per year in American hospitals due to medical error.⁷ We cannot get into the merit of these proposals here, but the fact that they might significantly reduce the number of deaths provides a *prima facie* case for adopting these proposals even if some privacy is sacrificed. Perhaps this is one area where good consequences trumps the right to privacy.

Criteria for a Good Privacy Policy

In 1999, the Federal Trade Commission developed five fair information practices.

1. Notice/awareness: covers the disclosure of information practices, including a comprehensive statement of information use;
2. Choice/consent: includes both opt-out and opt-in options and allows the consumers the choice to trade information for benefits, depending on the value consumers place on the benefits;
3. Access/participation allows for confirmation of the accuracy of information; necessary when information is aggregated from multiple sources;
4. Integrity/security: controls for theft or tampering; and
5. Enforcement/redress: provides a mechanism to ensure compliance; this mechanism is an important credibility cue for online companies, but is extremely difficult to accomplish effectively (Caudill and Murphy 2000).

In 1999, Amitai Etzioni presented a framework for a good privacy policy in his book *The Limits of Privacy*. That book, in turn, developed from a series of discussions

led by the OECD (1980) that included extensive US participation from the FTC and several senior members of the Clinton administration. Duh, Jamal, and Sunder (2002) subsequently adopted the Etzioni framework in the form of five principles that closely resemble those adopted by the FTC although they have interpreted them somewhat differently. Although neither set of principles was defended on normative or ethical grounds, such a defense is readily forthcoming.

Defense of the Criteria for a Good Privacy Policy

Freedom of choice or individual autonomy is a value that is endorsed by both liberals and conservatives. We have already established that privacy is necessary if one is to develop a sense of autonomy. It is also a means of treating people with respect in Kant's meaning of that obligation. We now ask what conditions are necessary if a right to privacy with respect to business transactions on the Internet is to be efficacious and what conditions are supportive of the exercise of individual autonomy. The notice/awareness condition provides information. A person cannot be free to do x, if he or she does not know that x is an option. A person cannot make a decision with respect to how one is being treated if he or she does not even know he or she is being acted upon. If we do not know that our personal information is being used to send us advertisements or is sold to third parties so that they can send advertisements to us, then we are not free to prevent the advertisements from being sent (we are of course free to delete them). The choice/consent and access/participation criteria enable us to exercise our freedom with respect to our right to privacy. These two criteria enable us to make choices about how personal information about us can be used by others. The integrity security condition is designed to protect the decisions we make about personal information. What good would the first three conditions be if people did not respect the choices that we made? The final enforcement/redress condition is similar in that it punishes those who violate our legitimate choices or at least gives redress to us when those choices are violated. The five conditions proposed above make a person's privacy on the Internet efficacious and are all supportive of or involve the exercise of a person's autonomy.

However, the discerning reader may see a gap in our argument. We have admitted that the right to privacy is not absolute and that respecting a person's autonomy involves respecting a person's privacy to some extent. But suppose one argues that some information is more worthy of privacy protection than other information. Suppose further that one argues that the information collected on the Internet in e-commerce is not important and therefore, although some information deserves privacy protection (e.g., medical information), the information collected on the Internet is not deserving of this protection. What can we say to that? Our answer is that we do not think the central moral issue is the importance of the information but rather who has a moral right to the information whatever the importance of it. In taking this position we believe that we are consistent with the view of privacy held by George Brenkert (1981). For Brenkert, privacy involves a relationship among a person A, some information X, and another individual Z. Thus A's right to privacy

is violated only when Z comes to possess information X and no relationship exists between A and Z that would justify Z's coming to know X.

Let us apply Brenkert's definition to a specific issue: Amazon.com and a book buyer are engaged in an economic transaction over the Internet. Amazon needs to know and is justified in knowing information that makes the mutually agreed upon transaction work. Thus, Amazon.com is justified in knowing the shipping address and the credit card information of the buyer. Any reasonable book buyer would agree to make this private information available to Amazon.com. However, in the absence of a policy stating otherwise that the buyer sees, he or she has no reason to believe that Amazon.com has a right to sell or give this information to others or to use the information except for the purpose of successfully completing the transaction. Anything else ought to require the consent of the buyer. Moreover, no other agent is justified in receiving this information from Amazon.com without the buyer's permission. And this is true no matter how trivial the information.

This argument shows that commercial marketing outlets are not justified in using private information for secondary purposes not necessary to complete the transaction and are not justified in selling or giving the information to others without the buyer's consent. The moral issue is not the importance or unimportance of the information but who has a right to know or a legitimate claim on the information.

Application of the Principles

We believe that the five principles are sufficiently justified. Let us apply two of these principles specifically to marketing in e-commerce. We choose these two principles because they are central in the protection of privacy and because there is empirical evidence regarding whether websites that claim they honor these principles really do so. The most obvious moral requirement is that an e-commerce website should have a privacy policy. In the absence of a policy the notice/awareness criterion cannot be met. Second, the policy should be easy to find and easy to read, i.e., not legalistic. To be easy to find, the privacy policy should be clearly stated on the homepage or at the site where personally identifiable information (PII) is collected. Normally the statement of the privacy policy should be one click away to meet the "easy to find" requirement.

To further meet the notice/awareness criterion the privacy policy should describe all the demographic and personal information collected. The Federal Trade Commission did not require that all information be disclosed in order for the notice/awareness condition to be met. In ascertaining whether a privacy disclosure was posted on a site, Commission staff credited *any* disclosure, even if related to only one discrete information practice (Federal Trade Commission 2000). Consistent with Duh, Jamal, and Sunder (2002), we would require disclosure of all such information.

A distinctive feature about computer technology is that a computer code attached to a site (called a cookie)⁸ can collect indirect information about a user as he or she browses the website. Thus, a person who goes to a website for athletic supplies where a cookie is attached will have his or her "hits" at that site and purchases, if

there are any, recorded. Without disclosure in the privacy policy there is no way for the normal user to know that his or her behavior at the website is being monitored in that way. Even more insidious from a privacy standpoint is that a third party can attach a cookie to the website the person is visiting and in that way can gain information and target ads to the person using the site. For example, consider the person who goes to the website for athletic supplies. Suppose Time Warner, which owns Sports Illustrated, has a cookie there. A person interested in athletic supplies may also be interested in Sports Illustrated. Time Warner can now send a special ad to the person who logged into the website of the athletic supplies firm. Time Warner has a number of means of doing this, for example, through an e-mail or a pop-up ad.

As we indicated in the introduction, surveys have consistently shown that people are most concerned about information gathered by the use of cookies, especially the information shared with or collected directly by third parties. In order to meet the notice/awareness criterion *all* information regarding the use of cookies should be contained in the privacy policy. We can illustrate the importance of this requirement by considering the saga of DoubleClick, Inc.

DoubleClick is in the business of serving as a middleman between content-rich websites and advertisers seeking to promote their goods to consumers who frequent those sites. How do they accomplish that technically? Some information can be obtained through the use of cookies. But the information gathered from cookies could be enhanced if DoubleClick and its clients had access to an offline database of personal information. With a planned merger of DoubleClick and Abacus in June of 1999, DoubleClick could have gotten the personal information it needed on 88 million US households. DoubleClick could now match online consumption and behavioral patterns with individual demographic data. This capability is of great interest to advertisers who want to target individual consumers. And advertisers are willing to pay DoubleClick for it.

More precisely, as reported in *USA Today*, DoubleClick can do this through the use of two cookies.

DoubleClick need only tie your cookie to another one placed by a site that ships you something through the mail or one which requires registration. To do that DoubleClick sends a cookie to your browser and gives it a unique ID number. DoubleClick sends the same ID number on to the site that knows who you are. That company then sends back the data that DoubleClick needs to look you up in the Abacus data base. And voila—DoubleClick knows who you are. (Rodger 2000)

As a matter of fact, the merger did not occur—perhaps as a result of pressure from privacy advocates. However, we believe that there are other companies that do engage in the practice that DoubleClick had envisaged in its merger with Abacus. Online data brokers MyPoints, Codigit, 24/7 Media, and Naviant have lined up with offline aggregators Experian, Equifax, Axcion, and InfoUSA.com, respectively. We believe that consumers should know or have easy access to all this information

upon signing into the database. That is why we require that the privacy policy ought to contain this information and be only one mouse-click away.

With respect to the choice/consent criterion, there are two basic strategies here. One strategy, the more permissive, is the opt-out strategy. Here a company website asks a person if they are willing to share their personal information with third parties, usually advertisers. Unless they explicitly say they are unwilling to have the information shared, "opt out," as it were, the company will share the information. With opt-in, the person logging into the site must explicitly agree to have his or her personal information shared—"opt in," so to speak. Unless the person so indicates, the company is not permitted to share personal information. We believe that the opt-in provision is more consistent with respecting a person's autonomy or right to choose. It supports maximum choice, especially since the opt-out provision frequently appears at the end of a long privacy policy document that many never read to the end and therefore never realize they have a choice to opt out. We acknowledge that we are arguing for a higher standard here—one based on ethical considerations rather than on legal ones. This issue will be discussed further in section four.

II. Privacy Law in E-Commerce in the European Union and the United States

In the US there are virtually no government regulations on privacy policies and disclosure in e-commerce or on the Internet. Once a person discloses information at a site or registers at a site there is no limit on what can be done with that personal information so long as no fraudulent actions are involved. In the United States there is no requirement that a site have a privacy policy or that an opt-out option be provided by those sites that do. In addition there are no legally mandated audit procedures nor are the e-commerce sites required by law to have their privacy policies certified by independent auditors.

There are three exceptions to the lack of US regulation of privacy—the health care industry and the financial services industry are governed by the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) respectively. In addition Congress passed the Children's Online Privacy Protection Act (COPPA) that became law in 1998. HIPAA became law in 1996, although the regulations on privacy were not finalized until December 28, 2000. COPPA sets rules for online collection of information on children. Since eBay collects personal information that would be in violation of the law if collected from children, the eBay website specifically limits participation to those over 18. These are important exceptions but can be ignored for our discussion here.

The situation in the European Community is very different. The general principles for privacy regulation are found in the European Directive on Data Protection.⁹ In 1995, the European Union adopted a mandatory rule, binding on all EU countries. The European Union Directive on the Protection of Personal Data required that all EU members amend their data protection laws to comply with the Directive. The

Directive stipulated that personal data must be processed fairly and lawfully and collected only for a specified, explicit, and legitimate purpose. Use of data beyond that stated purpose is prohibited. Data cannot be kept any longer than needed to serve its purpose and the data can be collected only if the person has given his or her consent. There is some fuzziness about what "consent" means under EU law. Some countries, such as France and Germany, define consent in their national law as requiring "opt in," whereas the UK has a more permissive definition which allows consent to be discerned as long as an "opt out" is provided. Given that the US has no law covering most websites, it is generally considered that with respect to privacy laws, the European Community has much stricter (and legally binding) requirements than does the United States.

Privacy Webseals

In the absence of strict national regulations on privacy as in the European Union, an alternative system of self-regulation has arisen in the US. In response to privacy concerns a number of companies have adopted privacy policies and posted them on their websites. But are these policies worth the paper they are printed on? In the absence of government regulation, private firms—including major accounting firms—have adopted seals or other devices to certify that companies follow the policies they have adopted. In addition, the providers do have certain requirements to obtain a seal, but the requirements vary from provider to provider and there is no exact match between any of the provider requirements and our five principles of a good privacy policy. The four most prominent providers of privacy "webseals" are TRUSTe, BBB Online, Web Trust (provided by the American Institute of Certified Public Accountants [AICPA]), and PricewaterhouseCoopers's (PwC) Privacy Seal.

Let us see how the four providers do when evaluated against the Notice/Awareness principle. The four competing providers all require that the privacy policy describe all types of personally identifiable information (PII) collected through the website. The TRUSTe and PwC standards are more demanding here since they also require a disclosure of how that information is collected. All four providers also require that websites disclose how the information will be used and shared. The TRUSTe website requires a website to disclose the use of cookies, indicate whether cookies are linked to PII, explain what data is collected with cookies, explain the consequences of not accepting cookies, disclose if data collected is aggregated with data obtained from other third parties, and identify third parties who are collecting data on the website. The TRUSTe standard is the most demanding one with respect to cookie disclosure. The PwC standard is the least demanding one and requires no cookie disclosure, although one could argue that cookie disclosure would be required under the standard that requires notification regarding what PPI is collected.

III. Testing the Solutions: Do Companies Adhere to Their Own Policies?

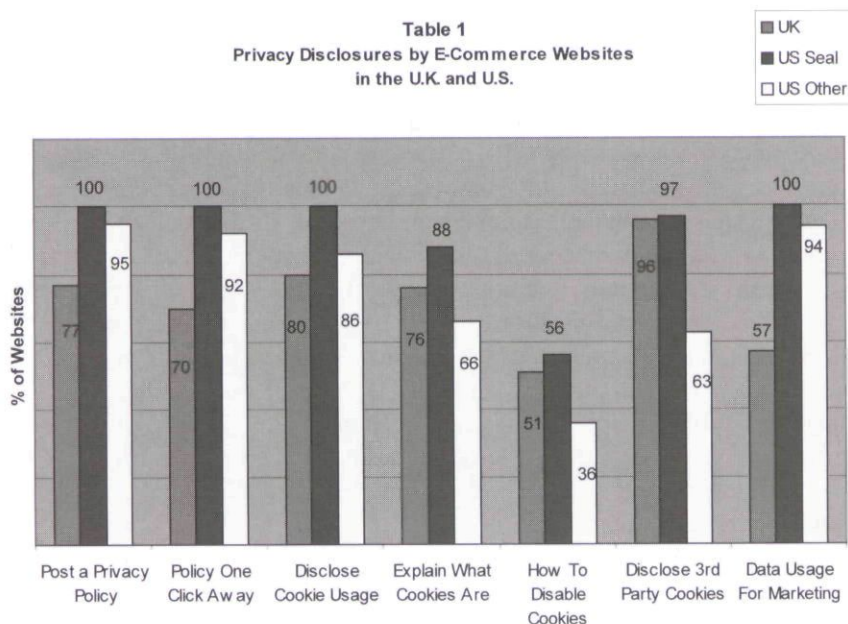
Privacy Policies Disclosure

Since a market has arisen in the privacy assurance area, it is important to see, in the absence of government regulation in this area, how effective these seals or assurances are in protecting the public. This section reports on a pioneering study by Karim Jamal, Michael Maier, and Shyam Sunder (2003) that provides some empirical data to answer this question. Jamal, Maier, and Sunder examined the privacy policies of 100 high-traffic US websites. Jamal, Maier, and Sunder conducted a field study to compare the actual practices of e-commerce websites against their own posted privacy policies. They programmed a web-crawler to identify which websites used their own and/or third party cookies to track the actions of visitors and to compare the observed behavior to the relevant disclosure of cookie usage in the privacy policies. A portion of the disclosure results of the study are shown in Table 1.¹⁰

Jamal, Maier, and Sunder report that out of the 100 selected high-traffic websites in the US, 34 had a privacy assurance seal (30 Trustee, 2 BBB Online, 2 had both Trustee and BBB Online). None had a WebTrust or PwC privacy seal. All 34 websites with an assurance seal (100 percent), and 63 of the 66 (95 percent) remaining sites without a web-seal, disclosed their privacy policy, for an overall disclosure rate of 97 percent of the total sample. Ease of finding the policy (roughly one click away) was 100 percent for those sites with an assurance seal and 92 percent for the other sites in the sample. In a follow up study, Jamal, Maier, and Sunder (2005) replicated the Jamal, Maier, and Sunder procedure on 56 high-traffic UK websites. Results of this comparison are shown in Table 1. Jamal, Maier, and Sunder (2005) were surprised to find that overall (despite stringent disclosure requirements in EU privacy law) disclosure rates in the UK were significantly below those observed in the US sample. In addition, they found it much more difficult to find privacy policies on UK websites. While it is relatively easy to find a privacy policy on a US website, it is generally quite difficult to find a privacy policy on a UK website. After extensive search, Jamal, Maier, and Sunder were able to find a privacy policy on only 77 percent of UK websites. Only 23 percent of UK websites seem to be non-compliant with the law.

Next, we focus on cookies. For the US sample, 100 percent of those with a privacy web seal disclosed cookie usage (see Table 1), 88 percent explain what cookies are and the kind of data they collect with cookies, but only 56 percent of those with a privacy seal explain how to monitor and disable cookies. What about those without an assurance seal? The percentages in all cases were significantly lower. Among the 66 websites without a privacy seal, only two sites did not use cookies, leaving a sample size of 64 who use cookies. Of those 64, 86 percent disclosed their use of cookies, 66 percent explained what cookies are, and only 36 percent explained how to monitor and disable cookies. Again the US study was replicated by Jamal, Maier, and Sunder (2005) in the UK sample. For all three cookie disclosure ques-

Table 1
Privacy Disclosures by E-Commerce Websites
in the U.K. and U.S.



tions, UK website compliance rates (see Table 1) are: 80 percent disclose cookie usage, 76 percent explain what cookies are, and 51 percent explain how to monitor and disable cookies. These percentages were below those of US sites with a web seal, but higher than US sites that do not have a web seal. For all other disclosure issues documented by Jamal, Maier, and Sunder, such as usage of personal data for internal and external marketing and sharing of information with partners, UK websites have significantly lower disclosure rates than US websites, both with and without a seal.

The use of third party cookies creates special challenges to those who seek to protect their privacy, since it is these third parties that create consumer profiles by aggregating behavior across thousands of websites and often sending the annoying "pop-up" advertisements that intrude over what you are viewing. For example, if you are looking through links to special news topics on CNN.com, you are often interrupted by an ad that pops up and takes over the whole screen. In some cases a novice finds it impossible to close the window without exiting from the entire program. The Jamal, Maier, and Sunder (2003) study showed that for US websites, 31 (91 percent) of the sites with an assurance seal and 48 (73 percent) of those without an assurance seal had third parties who placed a cookie on the site. Thirty (88 percent) of those with the seal disclosed the use of third party cookies, while 30 of the 48 without a seal (45 percent) disclosed the presence of third party cookies. Clearly sites with the assurance seal have a better record than those without the seal. However there is still room for improvement for those with the seal. A test of UK websites shows that UK websites are less likely to allow a third party to place cookies from their

site (only 50 percent allow such behavior). In the UK, disclosure rates of the presence of third party cookies are high (96 percent). However, UK websites generally do not provide a link to the privacy policy of the third party collecting data from their website (only 14 percent provide such a link). The Jamal, Maier, and Sunder (2003) results on disclosure by US websites are consistent with a series of studies conducted by the FTC (see <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>), which show significant improvement in privacy disclosures of US websites over time. In addition, the better disclosure practices in the US relative to the UK (which is contrary to our expectations), suggests that demands for formal government regulation of privacy disclosure may be inappropriate. An independent survey of EU privacy practices conducted by Consumers International in 2001 (Hwa 2001) also found very poor compliance rates with EU privacy law. For a discussion of the complexities of EU privacy law and the corresponding low compliance rates in EU countries see Nijhawan (2003). Slowly a consensus is emerging that EU privacy law leads to low compliance and widespread cheating, though the exact cause of this behavior is not well understood.

Formal government regulation should be resisted at least until we understand why UK websites don't follow EU privacy law which requires disclosure of cookies and third party cookies. Passing a law does not seem to necessarily create better disclosure practices (the case of Enron, WorldCom, TYCO, and other recent business scandals illustrates this point in the domain of another heavily regulated field—financial reporting by publicly traded corporations). A complex interaction of private incentives, regulation standards (like our five key privacy principles), and enforcement mechanisms (e.g., pressure by the FTC for better privacy practices) seems to be required to have effective regulation. We comment more on regulatory implications in section four.

Choice/Consent (Opt-In) Practices

The Jamal, Maier, and Sunder (2003) study also tested for the choice/consent standard. The test for this condition involves an examination of opt-in and opt-out policies. BBB Online and Web Trust standards require websites to offer either an opt-in or an opt-out strategy with respect to both its own marketing activities and the sharing of PII with third parties. TRUSTe requires only an opt-out option. PwC's standard is quite vague and requires websites to disclose "if you can prevent information about you from being shared."

Now that we are familiar with the policies of the assurance seal providers, Jamal, Maier, and Sunder tested the effectiveness of these policies using the same 100 high-traffic websites used to test the disclosure policies. Jamal, Maier, and Sunder also compared the stated policies and actual practices with respect to whether the opt-out choices by registrants were honored. Jamal, Maier, and Sunder created 200 identities and registered two times on each web site (with a unique identity each time). In one case Jamal, Maier, and Sunder opted in and thus allowed the website to send commercial messages or share data with third parties. In the other case,

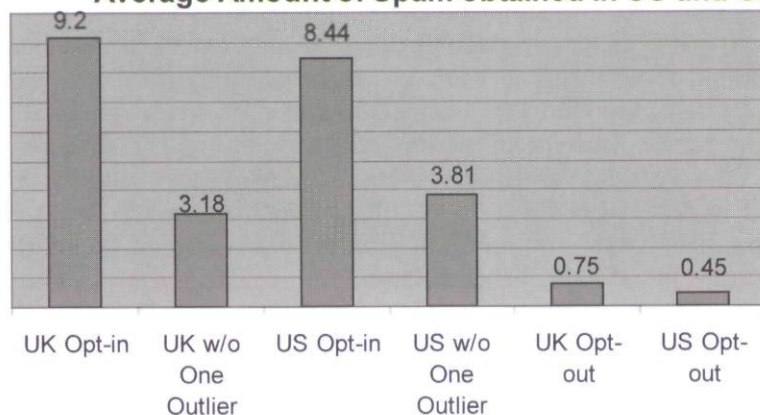
Jamal, Maier, and Sunder opted out and thus *did not* authorize (explicitly forbade) the sending of commercial messages or the sharing of data with third parties. By registering twice, once opting out and once not opting out, Jamal, Maier, and Sunder could monitor the volume of e-mail messages generated. If the opt-out policies worked, there would be far fewer e-mail messages to the opt-out address, compared to the address that did not opt out from the same site.¹¹ Some of the results can be summarized in Table 2.

The key result of Jamal, Maier, and Sunder is that exercising an opt-out option has a significant effect on amount of e-mail received. In the US, failure to opt out leads to each identity receiving an average of 8.44 messages per week over the 26-week duration of the study. In the opt out condition, the average amount of e-mail received falls significantly to an average of only 0.45. The UK results are similar. Failure to opt out leads to an average of 9.2 messages per week, whereas exercising the opt-out reduced the average to only 0.75 messages per week.

In both the US and the UK, most of the e-mails originate from a very small number of websites (outliers). In the US, 48 percent of total messages received after opting-out originate from one site. Five sites account for 92 percent of all messages received. None of these websites has a privacy seal. In the UK the outliers are even more extreme. One site accounts for 93 percent of the messages received from UK registrants. The most charitable conclusion is that their opt-out option is not working. A less charitable reading is that the sites are dishonest with respect to having an opt-out option. Fortunately, the vast majority of websites are honest and honor the opt-out options provided to consumers.

Like the opt-out results described earlier, the opt-in results were also driven in large part by a small group of websites (outliers). In the US, Some 56 percent of all opt-in messages came from a single registration. Again in the UK the results

Table 2
Average Amount of Spam obtained in US and UK



were more extreme. One website in the UK accounted for 66 percent of all opt-in messages received. This suggests that there are some sites that spam-averse users should be careful dealing with.

The conjecture of Jamal, Maier, and Sunder is that once an e-mail address is sold to third-party marketers, the amount of junk e-mail received increases steadily over time, and there appears to be no way to recoup the privacy of the sold addresses.

The study also included the postal service. Those who did not opt out received a total of twenty-seven pieces of mail of which fifteen came from a single registration (free newspaper for three weeks). Opt-out registrants received only two pieces of mail. Although the sample is limited, the opt-out choice worked almost perfectly for postal mail.¹²

As a result of their study Jamal, Maier, and Sunder have concluded that a kind of self-regulation can arise even in the absence of government regulation. But that still leaves open the question of whether government regulation is still needed—to protect us, for example, from the five sites that claimed they had an opt-out policy when they did not. Should government regulation be driven based on an analysis of average behavior (which is good in this case), or be driven by outliers who misbehave grossly in invading people's privacy on the Internet? Is it okay to complain that regulators are being swayed too much by outliers (as we hear these concerns often with respect to financial statement fraud—especially Enron and Arthur Andersen)? That is an issue we address in section four.

Default Registration Practices

The previous two sections on disclosure and opt-in practices suggest that widespread consumer concern about privacy is either unjustified, or fueled only by the actions of a small number of outliers. Unfortunately, there are some additional causes for concern besides disclosure and opt-out practices. Duh, Jamal, and Sunder (2002) did a detailed case study focusing on actual business practices of eBay, which has a very transparent privacy policy that discloses in great detail (and clarity) that the company collects a staggering amount of personal information about members of its "community." This includes a person's name, address, e-mail address, phone number, areas of interest, age, education, income, social security number, credit card number, bank account number, bidding history, feedback from others about transaction experience with a specific person, and many other types of information (disclosure of the types of information collected in eBay's privacy policy is three pages long). EBay also uses cookies, allows third parties to use cookies on its site, and tracks the URL, browser software, URL where a user came from, next URL a user goes to, and the IP address of participants. A personal file retains messages posted on bulletin boards and correspondence with the company. Purchases from cooperating merchants who do their business through eBay's website are reported back to eBay. EBay also discloses in detail all the data it provides to advertisers, telemarketers, partners, members of its community, co-branded third-party suppliers,

and service providers. These third parties may follow different privacy guidelines, which eBay says it neither controls nor endorses.

eBay's registration process automatically sets the default to "yes," which ensures that unless the readers are fully alert in reading all the details, they would automatically, and perhaps inadvertently, agree to have their private information sold or shared with telemarketers and to receive promotional material from eBay. The users have to manually select "no" to prevent having their information sold to telemarketers. Duh, Jamal, and Sunder (2002) propose that one way to summarize eBay's privacy policy would be to say "there is no privacy on the Internet." The reader can confirm these conclusions as we did in May 2004 by visiting the eBay website.

eBay is a licensee of TRUSTe and claims to follow their requirement of notifying users of its privacy policy. Unless a person does not want to be a registered eBay user, he/she must agree with whatever policy eBay adopts. As long as eBay discloses its data collection and data use practices, it is automatically in compliance with TRUSTe requirements. TRUSTe standards focus on disclosure only and not on the actual content of the underlying privacy practices themselves. If the market among auction operators were reasonably competitive, unsatisfied users could go elsewhere. However, the dominant market share of eBay among auction operators suggests that many users have no real choice.

It could be argued that the "TRUSTe" privacy seal gives users a false sense of comfort. TRUSTe standards specify disclosure requirements, but do not set practice standards. Companies with wide variance in quality of actual privacy practices can get a TRUSTe seal as long as they disclose their practices. At first TRUSTe did not revoke a privacy seal from any company, despite some widely publicized scandals involving TRUSTe participants. Most of the scandals involve spyware (where a company such as Microsoft or RealNetworks covertly tracks activity of users), and the sharing/selling of customer information to third parties. However, the 2003 TRUSTe annual report indicates that two privacy seals were revoked—one for failing to honor an opt-out decision and another for selling personal information without consent. Yahoo recently amended its privacy policy to allow it to sell addresses and phone numbers, in addition to e-mail addresses, to telemarketers.

The above analysis of eBay in this section suggests that consumers have valid reasons to be concerned about the privacy of data they supply to operators of e-commerce websites. A clever lawyer can easily insert a disclosure statement that informs the discerning reader that all her activity is being tracked and the information can (and will be) sold to a large number of internal and external "partners." In addition, some of this information is collected covertly, and a serious question can be raised about what it means for a user to give "consent" to be monitored, and for her personal information to be sold to other third parties. New technology provides a staggering array of covert monitoring (and sharing of information) possibilities. Is it okay to use these technologies (and do this sharing) as long as their use is disclosed? While media accounts focus largely on threats from hackers, there is a steady and ongoing threat to consumer privacy from the actions of e-commerce

website operators. Consumer surveys cited earlier in the paper confirm these concerns. This again raises the question: Can websites collect any information they want (overtly or covertly) and then share that information with whomever they like as long as they disclose their practices? Or should the Government (or seal providers like TRUSTe) place some restrictions on them? This is a key regulation issue we discuss in the next section.

IV. What Should Public Policy Be with Respect to Privacy Laws?

To address the public policy issues, we will use the same framework for an argument that we used when justifying the right to privacy in general and in justifying the criteria for a good privacy policy. We maintain that autonomy is a basic value and that honoring autonomy is one way of showing respect to participants in e-commerce and users of the Internet. Furthermore there is a consensus that honoring privacy in e-commerce is necessary for facilitating the autonomy of individual users and thus of showing them respect.

It should come as no surprise that the Federal Trade Commission has recommended increased regulation in this area. In their 2000 report to Congress, the Commission noted that too few business sites met the fair information standards. Indeed less than half met the notice and choice standards. (Federal Trade Commission 2000) For this reason the FTC recommended on a split vote that all consumer-oriented commercial websites that collect personal identifying information be required to comply with the five widely accepted fair information practices. Do we agree?

Since government regulations impose constraints on action, we prefer voluntary action to government regulation whenever voluntary action is efficacious in resolving a problem. The use of privacy seals is an attempt at voluntary action with respect to the protection of privacy rights on the Internet. The experiment by Jamal, Maier, and Sunder provides empirical evidence that sites that have seals are meeting the requirements of their own policies. Their research also shows that having an opt-out policy and a seal does make a significant difference in the amount of e-mail solicitations one receives. Thus, a consumer who is concerned about his or her privacy rights can look for the seal and be relatively certain that the site holding the seal has an easily accessible privacy policy (the equivalent of one mouse click away.) They can also be reasonably certain that the policy will disclose the use of cookies and whether the personal information provided will be used for solicitations and provided to third parties. Finally they can be confident that if they choose to opt out that choice will be respected. All this is to the good.

Moreover as our UK sample has shown, strict legal prohibitions do not necessarily lead to good compliance. In many respects websites in the UK were not as good at meeting the criteria of a good privacy policy as those in the United States—despite the European Union directive on privacy. This fact counts as another reason why the voluntary plan deserves a chance.

However, the voluntary approach through the use of seals does not solve the problem created by rogue behavior. Sites that do not honor the opt-out provision have not lost their privacy seals. We believe that if the voluntary approach is to work, sites that violate their own policies and do not honor the choices of registrants should have their seals revoked.

One of the criticisms of the voluntary approach is that there are no judgments about the privacy policies themselves. This paper has argued that there is a consensus that can be supported by ethical theory that there are some generic universals regarding a good privacy policy. These are captured in our five criteria. Should there be government regulation requiring that all business websites that collect personal information have privacy policies that meet these criteria?

We believe that the autonomy of the consumer is sufficiently protected in a market where there is an opportunity to do business and provide PII that is protected by a privacy policy and an assurance seal. Thus, we would not require all business sites to have a seal. Let the consumer decide if he or she wants to do business with a company that has a seal. However, we are concerned about the widespread disparity among the seals and the lack of clarity surrounding just what the assurances are. Thus, our proposal is not that all business sites that collect personal information have a privacy policy that honors our five principles. Rather we believe that in a world of privacy assurance seals, there are certain conditions that should hold if a seal is to be granted and maintained. It is to these issues that we now turn.

Should opt-in be required if a registrant's personal information is to be used for purposes of non-transaction related solicitations or given or sold to third parties who would make such solicitations. As we have seen the opt-in requirement is a matter of law in the European Union. We believe it should be a requirement to obtain a privacy assurance seal. We believe that an opt-in policy is the policy that is most consistent with facilitating consumer choice. Many users of the Internet are still relatively unsophisticated, the privacy policies tend to be lengthy and hard to understand, the choice to opt out is often at the end of the policy so that consumers would have to read to the end to exercise their choice. Only in a few cases opt-in is the default. Given the importance of a right to privacy and given the facts provided, we believe that opt-in should be a requirement for the possession of a privacy assurance seal. Finally it is also important that these policies be written in plain English that can be understood by the vast majority of Internet users. Legalese should be avoided.

A rebuttal to this position would need to show that the value of the opt-out option is of such great weight that it overrides the right to privacy in this case. But how could such an argument be made. Under an opt-out provision, it would be easier for merchants to sell other people goods and services, but why should that trump a right to privacy? The whole point of rights is to put some limitations on social utility as a trump on individual interests. Ease of selling sporting goods does not rise to the level of preventing a terrorist attack. We see no reason why utilitarian considerations should prevail in this case. This is especially true since no site is required to have a privacy assurance seal.

Another issue surrounds the lack of definitive standards imposed by the seal and variations among the seals themselves with respect to standards. We believe that no seal should be granted unless a privacy policy is in accord with something like our first four principles and unless the seal can be revoked for violations. Beyond that we do not object to the lack of uniformity. The situation has some similarities to the differences in accounting standards between the United States and the United Kingdom. The US is very rule oriented; so long as a firm literally follows the rules the firm's practices are considered acceptable. In the UK, there are fewer rules and what governs is the spirit of the rules. We think that operating from the spirit of a good privacy policy is more important than imposing a detailed set of rules that everyone must follow. Besides the rules that we would impose have real bite. Consider our rule that all good privacy policies meet the choice condition only if they have an opt-in policy.

Although we think this approach is justified by our reliance on autonomy and the working of markets, we recognize that there are some complicated issues where it might be better to have rules. Suppose a person opts-in for the selling of PII to a third party. Should opt-in permission be needed for each vendor or should the opt-in provision be a general permission to provide PII. There is also an issue of scope. Suppose a website that has done comparatively little selling of PII suddenly decides to vastly increase the scope of its selling. Should a new opt-in agreement be required? We think the solution to this problem can be resolved by disclosure. Some websites may request a wide right to provide PII to third parties. If a person opts in to that arrangement, then we do not think the person's privacy rights are violated even if the website expands the scope of its provision of PII. After all the user has given that permission in advance as it were. However, some websites may believe that they will not get sufficient opt-in if the provision to third parties is cast too widely. In such cases, some websites may choose to restrict provision to third parties. In those cases, it seems to us that a change in strategy would require a new opt-in agreement. Consistent with our overall view we are not concerned if some websites have a wide provision and some a narrow provision.

A similar analysis would be applied in cases where a website changes its activity. Suppose a bank that had no real estate loan department or no investment department decided to do so. As a result PII that had been provided to a narrow range of banking clients is now provided to real estate agents and investment brokers. Would this require a new opt-in agreement? In most cases we think it would because in most cases there would be no mention of the real estate and investment business in the original opt-in agreement. However some banks that contemplate expansion in these directions might announce in advance that they are thinking along those lines and therefore would ask for the right to provide PII to an expanded clientele. In that case a new opt-in provision would not be required. These two test cases provide the kind of moral casuistry we would use as we apply our general philosophy and the five principles of a good privacy policy to issues that arise.

In conclusion, we adopt a mixed approach relying on the voluntary use of privacy seals as much as possible. In so doing we recognize that people who register on sites without policy seals may sacrifice their privacy regarding the use of personal information. If a person wants the protection of a privacy seal, he or she should know that certain minimum standards are met. In this section we have tried to outline what those minimum standards are. Although they are minima, we do not think they are insignificant. If our proposal is correct, a person who is truly concerned about his or her privacy can be protected in e-commerce on the Internet. Yet we accomplish this without detailed rules and regulations. These proposals are not ad hoc but are justified by an appeal to moral theory and to values on which there is a wide consensus.

Notes

1. An exception is Charters 2002. Although philosophers have had little to say, much more has been written by those working in marketing and marketing ethics. An entire issue of the *Journal of Public Policy & Marketing*, published in the spring of 2002, was devoted to ethical issues in database marketing. Patrick E. Murphy also published "Privacy in Market Research" in a volume called *Excellence in International Research*, ed. Maureen Sheptstone (ESOMAR, 2001).
2. Boston Consulting Group Study, 1997.
3. Business Week, <http://businessweek.com>, 1999.
4. P3P stands for Platform for Privacy Preferences, which is a project of the World Wide Web Consortium. The project is designed to help users gain more control over the use of their personal information.
5. We recognize that persons' desires and interests conflict and that respecting autonomy does not involve letting people do whatever they want. A further discussion of this issue is beyond the scope of this paper. See Bowie and Simon 1998 for a further discussion of this issue.
6. Katherine Eban Finkelstein cites the ACLU, Phyllis Schafly's Eagle Forum, and the National Coalition for Patient Rights as holding this view. See "The Computer Cure," *The New Republic* (September 14 and 21, 1998 issues).
7. Lisa Belkin cites a 1993 study by Harvard University as the source for these figures. See "How Can We Save the Next Victim," *New York Times Magazine* (June 15, 1997).
8. A cookie works as follows: A user clicks on a site and asks for information. A small computer file with a unique tracking number (cookie) that identifies a specific computer is installed on the user's computer. The firm that placed the cookie there can now track the users of this computer on websites in its network. The firm then stores that information and can send ads to that computer and/or sell information to a third party that allows that third party to send information to the computer.
9. This directive may be found in the Official Journal of the European Communities and accessed at http://europa.eu.int/eur-lex/pri/en/oj/date/2002/l_201/l_20120020731en00370047.pdf.
10. Details on how the investigators accomplished this technically can be found in Jamal, Maier, and Sunder 2003.
11. Again, the details of the experiment can be found in Jamal, Maier, and Sunder 2003.
12. The study also had a phone-call component. Interestingly, especially in light of the recently passed Do Not Call legislation, phone calls were not a problem even if you did not opt out. Telemarketers must have different lists.

References

- Bowie, N. E., and R. L. Simon. 1998. *The Individual and the Political Order*, 3rd ed. (Lanham, Md.: Rowman & Littlefield).
- Brenkert, G. G. 1981. "Privacy, Polygraphs and Work." *Business and Professional Ethics Journal* 1(1).
- Caudill, Eva M., and Patrick E. Murphy. 2000. "Consumer Online Privacy: Legal and Ethics Issues." *Journal of Public Policy & Marketing* 19 (Spring).
- Charters, D. 2002. "Electronic Monitoring and Privacy Issues in Business-Making: The Ethics of the Double-Click Experience." *Journal of Business Ethics* 35(4): 243-54.
- Duh, R. R., K. Jamal, and S. Sunder. 2002. "Control and Assurance in E-Commerce: Privacy, Integrity and Security at eBay." *Taiwan Accounting Review* 3(1).
- Etzioni, A. 1999. *The Limits of Privacy* (New York: Basic Books).
- Federal Trade Commission. 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*.
- Hwa, A. P. 2001. "The Role of Self-Regulation and the Internet." *Journal of Interactive Advertising* 1(2) (Spring).
- Jamal, K., M. Maier, and S. Sunder. 2003. "Privacy in E-Commerce: Development of Reporting Standards, Disclosure and Assurance Services in an Unregulated Market." *Journal of Accounting Research* 41(2).
- . 2005. "Enforced Standards versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the U.S. and the U.K." *Journal of Accounting Research* 43(2): 73-96.
- Kupfer, J. 1987. "Privacy, Autonomy, and Self-Concept." *American Philosophical Quarterly* 24(1).
- Nijhawan, R. 2003. "The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States." *Vanderbilt Law Review* 56(3) (April).
- O'Neill, Onora. 1989. *Constructions of Reason* (New York: Cambridge University Press).
- Organization for Economic Cooperation and Development (OECD). 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available from <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.
- Rodger, W. 2000. "Activists Charge DoubleClick Double Cross." USA Today (February 21), available at usatoday.com.
- Tedeschi, R. 2000. "Sellers Hire Auditors to Verify Privacy Policies and Increase Trust." *New York Times* (September 18).

Copyright of Business Ethics Quarterly is the property of Philosophy Documentation Center and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.