

7

Cookies Invading Your Privacy

Henry Pham and Cuong (Kevin) Than

Introduction

According to CNN, in May of 2000, Microsoft and Yahoo rushed to repair a security flaw in their e-mail web services. Crackers, individuals that try to gain unauthorized access to a computer system with malicious intent, were exploiting a bug in the system that allowed them to use stolen cookies from the victim's computer to gain access to their e-mail accounts (dictionary.com 2004). Crackers would send fake e-mails, tricking users to click on links in the e-mail. Once a user has clicked on the link, the necessary cookies were sent to the cracker, allowing the cracker to login into the user's e-mail account using the stored cookie (Stenger 2000). Although the crackers did not collect the information, this shows how much information cookies can contain and what can happen if the information stored in the cookies is exploited for malicious purposes. Presently, cookies are more commonly used for marketing in developing and personalizing the content and appearance of websites. For example, marketing companies gather information from cookies so that they can target ads specifically to the user (Cisna and Peng 2000). Cookies have various advantages and disadvantages that are often confused due to the lack of knowledge about the technology. The controversial ethical issue surrounding them is whether the benefits outweigh the drawbacks with respect to privacy issues. Until all concerns are dealt with and settled to a satisfactory level, possibly through governmental regulations, the use of cookies will remain a controversial subject.

Cookies are created by websites to store information, such as the user's name, address, social security number, passwords, and anything else the user may send to the server. Logically speaking, cookies are small text files that reside on the user's computer (Privacy Compliance

Resources). Contrary to the belief of many, cookies cannot retrieve information from your hard drive, read information from other cookies, plant viruses, track movements from one site to another, or steal credit card numbers without permission (Cattapan 2000).

Cookies were originally conceptualized to identify the online user's computer so that the site that planted the cookie would:

- 1) Not have to constantly ask for the user's name and password
- 2) Learn more about the user's interests by monitoring the user's most frequented sites
- 3) Provide the basis for sending personalized offers and advertising (Bayan 2001).

There are two types of cookies: session and persistent. Session cookies are stored only temporarily on the user's computer until her or she close the website, after which the cookies will delete themselves. Persistent cookies, on the other hand, remain on the hard drive for long periods of time. When people think of cookies, they usually think of persistent cookies. On a positive note, cookies cannot automatically collect personal information about the user. The only information that is stored is the information that the user has provided to the server. The downside is that the information one provides is stored for long periods of time, and it may or may not be encrypted. Since their introduction, the function of cookies has evolved and the technology's future uses seem to have unlimited potential. This may or may not cause an increase in ethical problems.

Advantages of Cookies

Depending on who you talk to, people either consider cookies to be positive facet of the Internet or are completely repulsed by their inception due to their insensitivity to privacy concerns. Typically, it is the corporations, online merchants, and marketers that see the benefits of cookies. For example, many supporters believe that the use of cookies will improve electronic commerce efficiency on a large scale. When there are no prior records saved from visiting an e-commerce site, people must make each purchase unconnectedly, thus creating an inconvenience for the consumer. However, with the presence of cookies, information can be saved from previous visits to a specific site, making transactions more efficient and less inconvenient. With cookies, customers have the luxury of avoiding having to repeatedly fill in information that they have provided during a previous visit. Another marketing function that cookies serve is to help personalize advertising based on gathered information:

There is no other competing technology that does what a cookie does, with so little associated cost. Since it is just programming (to send a text file to the client; the file itself is not an actual running program), the only real cost to the producer is the cost of the programmer's time for building it in, and little time is required (Cisna and Peng 2000).

Cookies can also deliver value to consumers by personalizing websites for convenient access and use. For example, Netscape's personalized websites employ cookies for members to only utilize the information that they want while steering them away from unwanted information (Cisna and Peng 2000). Personalization of websites has become a necessity for companies to compete in the increasingly large e-commerce market. It has been estimated that the initial cost of a personalization system is around \$150,000 and the final cost can reach several millions of dollars, after other costs such as labor are included (Cisna and Peng 2000). Cookies can accomplish the goals of personalization systems with increasing cost-reduction incentives. With a large and ever expanding online, the use of cookies will continue to be widespread although is also likely to remain controversial:

E-commerce sales transactions were estimated at \$25.8 billion in 2000. Online advertising expenditure and revenues have also exploded. In 1996, \$267 million was spent on Internet advertising; in 1999, companies spent over \$4.6 billion on Internet advertising... An average American's profile is on twenty-five to one hundred commercial databases (Shimanek 2001, p. 455).

From 1996 to 1999, online advertising increased a staggering \$4.3 billion. With the growing prominence of online advertising comes the importance of cookies to companies. After all, cookies allow efficient marketing that is leveraged through online profiling. Anyone can see why marketers, online merchants, and corporations rely on cookies for, but where does this leave consumer opinion and privacy rights?

Disadvantages of Cookies

The biggest concern for the opponents of cookies is privacy. Many people are against the use of cookies, but are not fully educated about the technology's dynamics. One misconception is that cookies can somehow cause damage to a person's computer. Some believe cookies can transmit viruses, but the reality is that cookies cannot function like a virus (Cisna and Peng 2000). The most basic negative aspect of cookies is that they allow entities to track people while they browse the web, which is a problem for those concerned with their privacy. Internet user have the option to reject cookies by setting their computers to do so automatically or by using cookie specific software. On the other hand, a web user is severely limited in what he or she can do online by accepting cookies. Another problem for the user is that they can result in junk mail and pop-ups for the users. Although these marketing tools are widely used and are quite effective for the companies, they are annoyances to the average user that are hard to avoid.

How to Protect Yourself

Although blocking cookies is possible, often times doing so will render the site inoperable. There are many sites that people browse every day, including MSN.com, Yahoo.com, and Amazon.com among many others, that require the use of cookies. Disabling cookies will not allow one to login to these sites, use their e-mail services, or shop in their online stores, thus forcing people to enable cookies. Users that are

more wary of their privacy are probably concerned about what they can do to protect themselves. Users can do a number of things, including installing an adware program, deleting the cookies, or accepting only some of the cookies offered. Adware programs are good tools to use to delete cookies, as they will often detect cookies that are commonly used to track web browsing. Deleting cookies on a daily basis may also be helpful. This can be done through the browser's settings, or by browsing to the cookies' folder and manually deleting them. Another helpful option is to set your browser to only accept cookies from the originating website, meaning the browser will only accept cookies that are associated with the website the user is currently viewing, and rejecting cookies from the all other websites. The last option, besides blocking cookies altogether, is to change your browser's settings to warn the user before accepting cookies. Although useful, it may be difficult to understand the Internet jargon and understand what it is one is accepting. Blocking cookies these days may be useless depending on the websites you frequent, but this does not mean that there are no alternative solutions. In addition to the options mentioned above, a person can browse through an anonymizer, which will mask his or her identity. Cookies have become almost essential when browsing websites, but where do we draw the line from utilizing a technology to make our lives more convenient to the amount of privacy we want?

Privacy Concerns

The fear of privacy invasion is by far the most important problem because individuals want to be able to search the web without being tracked and want to know that their private information is secure. When information is collected about a person through cookies, it is compiled with personal information that the user voluntarily gives up when filling out forms to create online profiles. These profiles are used by companies for their own purposes but are often sold to a third party without the user's knowledge. For example, a study of more than 70 online job sites has shown that job seekers provide their information for job searches but little do they know that their profile is being sold, often without notification, to third party vendors for marketing purposes (Vijayan 2003). Because cookies have many disadvantages for the consumer and many advantages for commerce, the split between these two sides has set the stage for privacy issues that have increasingly become an ever growing concern.

Many corporations have started solely as Internet commerce companies, while many are taking advantage of this growing market in addition to their traditional operations. Although, e-commerce is growing at an extraordinary rate, it would be larger still and growing at a rate that's even faster if consumers had a satisfying sense of security and privacy. Privacy is important to consumers because it is their nature to want to know how their personal information is being handled and used. If the consumers already know or have just now found out the way companies utilize cookies, it is understandable why the consumers feel their privacy has been violated. As mentioned before, companies use this technology to gather information and then combine that information with additional information gathered by other means or received from other companies to create profiles. These

derived profiles are then used for the direct benefit of the companies that developed them or sold to third parties for a profit. Author of "Four Ethical Issues of the Information Age," talks about how profiling violates privacy when he states:

You or I may have contributed information about ourselves freely to each of the separate databases but that by itself does not amount to giving consent to someone to merge the data (Mason 1986).

Supporters and Opposition

A common theme has surfaced, placing the corporations, yearning for a self-regulated online market, on one side with the consumers, seeking a market that is more regulated and geared towards needs of feeling safe while online, on the other side. Caught in the middle of this controversy is the government, which has to decide how much, if at all, it should intervene and regulate. Of course, it would not make any sense for the government to interfere if self-regulation is proven to work. However, so far it has not. Now, the government must figure out if self-regulation will work in due time or if it is necessary for the government to implement codes and guidelines.

Companies that depend on e-commerce support self-regulation because it is the easiest way for them to efficiently run their business. The more they have to abide by privacy codes, the higher the costs. This business attitude creates a certain bias, which is one of the many reasons why policies need to be in place. Self-regulation has resulted in many companies establishing privacy policies. However, although many companies have privacy policies, the policies are not enforced and/or are inadequate. There must be a solution ensuring that the companies act responsibly!

On the other side, when spending money on products and/or services online, consumers should be entitled to as many rights to be upheld by the company offering the product and/or service as possible. If it was up to the consumers, they would seek the maximum amount of security, and thus it would be difficult, if not impossible, for a company to run efficiently and remain profitable. Therefore, a compromise between the sides will be necessary for our Internet market to be efficient and for the consumers to receive their privacy rights. How will the parties come to a compromise? Will the government need to step in?

Before discussing the policies, or lack thereof, in the United States, we would like to discuss how the European Union has dealt with this matter. The European governments have been more proactive in preparing for a high technology future and, thus, are likely to be better prepared to deal with privacy problems as they arise. With the consideration of how the EU has implemented its guidelines, we will propose an example of a policy that could be used in the US to better serve the public's right to privacy online.

EU Regulation

The European Union (EU) has the strictest regulations on cookies, and it is time that the U.S follows. With the United States being a leader in the technology sector, it has the responsibility to help lead foreign

nations in building guidelines, but yet it has not done so. Foreign nations have already begun to move in the direction of the EU, and are making advances in data protection. On December 11, 2003, the EU passed regulations stating that websites had to meet considering the use of cookies.

Provisions to the directives that were to be met by members of the EU can be found in the "EU directive on Privacy and Electronic Communications 2002." These guidelines consist of the website informing the user, that is, making sure the user is aware cookies are being used and what the cookies are being used for. Also, the website must provide a way to opt-out of the cookie (Cookie Law). More formally speaking:

The Directive also suggests that the methods for giving information and either offering a right to refuse a cookie or requesting consent should be made as user friendly as possible but that this can be done once for use during a particular connection but also covering any further use that may be made of such devices during subsequent connections (Cookie Law).

To restate, the directive is making a push to have websites inform the user that a cookie is being used, in as clear a fashion as possible. The directive also notes that this consent only needs to be given once during a single connection, and for any future connections.

Another piece of information required, is the website informing the user on the purposes of the cookie.:

Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user (*Office Journal of the European Communities 2002*, p. 7).

Any member states involved have to inform the user or subscriber of the uses of the cookies. The information must be provided in a "...clear and comprehensive..." manner. But, the site must also allow the user "the right to refuse such processing by the data controller (*Office Journal of the European Communities 2002*, p. 8)."

This leads to the next requirement of the directive, the right to opt-out. Users or subscribers must be given the option to opt-out at any time, meaning that the website must offer a way for the user to decline the cookies. To meet this requirement, a website can offer a ticker box or provide information on how to block the cookies.

Provisions 20, 21, and 26 state that websites must conform to strict guidelines in regards to cookies and personal information. Though there are more provisions that guide security measures, this paper will only focus on those that directly affect cookies and their use. These provisions state what type of data can be obtained by a server, how the data must be handled, and the security measures that must be applied to the servers.

Provisions 20 and 21 of the directive, suggest that service providers should take appropriate measures to ensure the safety of data. This also extends to the means in which the data was collected, i.e. the data being transferred through the medium is secured. The provision also mentions that the user must be informed of any existing security risks, as well as any risks that may exist after a security breach has occurred. It also notes that service providers must inform users on how to protect themselves and their data. The provision further states that the service provider must take any measures necessary to ensure the security of the site and its information, whether or not it will incur costs to the company, and will provide these security features free of charge to the user.

Provision 25 of the directive, states what information can be collected about a user or subscriber. With regards to cookies, the information can be used for analyzing the effectiveness of website design and advertising, as well as to verify users for transactions (*Directive on Privacy and Electronic Communications* 2002). Also, information can be used to determine the effectiveness of how well a website is designed, how well advertisements are used, or to identify whether the user currently accessing the site is acceptable. Otherwise, cookies can be used for legitimate purposes, given that the user has been informed about the cookie. This includes informing the user that the site is using cookies and also informing the user in a clear and precise manner of what the cookie is used for (*Directive on privacy and Electronic Communications* 2002).

Another related set of provisions that are of interest are 26, 27, and 28. These provisions further specify the type of information that can be collected for processing. They also cover how long the data can be kept, and how the data can be processed.

Provision 26 directly concerns the data related to the subscriber and how it can be used. The information directly related to a person can only be used and stored as long as the data is needed for the service, except for the purposes of billing and interconnection payments, and can only be used for a limited time. Processing the data any further for the use of marketing must be consented to by the user. Although processing the data is allowed, these guidelines must be met once the user has consented: the information to be processed must be accurate, the provider must specify what types of processing will occur, the provider must inform the user of which data will be processed, and the provider must inform the user of the duration of the processing. After processing has occurred, the provider must do one of two things, either erase the data or make the data anonymous.

Provisions 27 and 28 explain how and when the data must be erased or made anonymous. The moment the transmission has completed, the data must be erased except in cases of billing, and for

purposes the data was intended for as noted in provision 26. Although data must be erased and made anonymous, provision 28 allows for some data to be kept, provided that the data is used for caching the domain name system of IP addresses, or is used to control access to networks.

Another directive is the “Guidance to the Privacy and Electronic Communications (EC Directive) Regulations of 2003”. This directive takes the above directives to further explain in detail what services are considered legitimate. The Electronic Communications Guidance (ECG) states the same as the above directives, with the exception of what cookies can be used for. The above directives stated that cookies could be used for billing purposes unless otherwise consented by the user. The ECG takes cookie usage further by stating that, if the cookie is used to provide value added services than the use of cookies is allowed. But, just like in the directives these cookies still must be consented to by the user (ECG 2003). Concerning marketing of the data, the service provider may only do so if the user has consented to allowing cookies, with the exception of information such as usage patterns and traffic information.

Although these provisions have restricted service providers from obtaining users information, it has not completely stopped them from doing so. The statement, “using cookies in any fashion has to add value to the website” has been stretched far from its real meaning (e.g. websites claim to collect personal information about a user because it is critical for the website to function properly). Also, all a website has to do now is to include a privacy policy, data protection notice, or both and, if done in a clever way, may never be seen by the user. The last requirement by the directives is to allow the user to refuse cookies from servers. This is all too easy to bypass though. Having a link on the site telling the user that they can block the cookies via the securities in the browser’s options is all a site needs to do.

The European Union has definitely taken the reigns in protecting the user’s privacy in regards to cookies. Although the EU has made the push to protect users and to force websites to follow certain guidelines, the directives themselves are not complete as was demonstrated by the previous examples. The EU has definitely made the step in the right direction by protecting users against websites, but the directives could be made more detailed to help the user while being lenient enough to not create a large burden on websites.

U.S. Regulations

Here in the US, a different approach has been taken to confront the dynamics of the Internet. The government and the Federal Trade Commission (FTC) have had to deal with different opinions. “...those involved in e-commerce policy say it’s time for the Federal Trade Commission to step up to the plate on behalf of the privacy rights of Internet consumers. Others claim there’s no need; give self-regulation a chance to win the game (Moss 2000, p. 24).” Although the government has not taken any one side they have certainly swayed in the direction of those seeking a free market, mainly towards large corporations trying to avoid further legislative guidelines and cost. Only time will tell if congress will lean in the other direction or compromise between both sides.

In an attempt to solve the dilemma of privacy online, the US Senate requested the FTC to research the matter through studies of corporations that operate their business with computer databases. About a year later, on October 17, 1997, the FTC reported their results in a report titled, "Individual Reference Services: A Report to Congress," which essentially concluded the industry is best off regulating itself (Peek 1998). Neither the FTC nor Congress made real strides with this report. The matter seemingly was addressed with a lack of care and concern for our right to privacy.

Not long after the 1997 report, another report was released by the FTC in June 1998 titled, "Privacy Online: A Report to Congress." This report was based largely on an extensive survey of over 1,400 commercial websites; from this study the FTC concluded self-regulation had yet to be effective, and children's privacy online needed immediate attention (Landesberg 1999). Congress's response to the FTC's findings was the Children's Online Privacy Protection Act of 1998 (COPPA). This act targeted young children to protect those less than thirteen years of age. The act forces websites to follow the following guidelines: (1) provide the child's parents with notices of their information practices; (2) obtain verifiable parental consent for the collection of personal information before doing so; (3) provide parents with the capability of reviewing the information upon request; (4) provide the opportunity to stop collection of information at any given time; (5) limit collection of personal information; (6) maintain procedures to protect the child's confidentiality and integrity (Landesberg 1999). This act was a huge step in the right direction, however, it is not a reason to back off and avoid making the Internet a safe and secure environment. In a similar reaction to the 1997 report, Congress again felt a free market should be achieved and given more time. They have suggested, but have not enforced self-regulation online should be based on four practice principles, notice/awareness, choice/consent, access/participation, and security/integrity. Children should definitely be more protected from online predators, but everyone else is also at risk of having their rights violated and so it begs the question, why is Congress avoiding a solution to the issue?

One reason why action should be taken is that many companies have unethically invaded the privacy of their clients. Take, for example, DoubleClick Inc., an advertising agency that announced in January 2000 they would merge databases containing names, addresses, and off-line buying habits of millions of consumers gathered by its cookies. The company suffered, through an e-mail campaign against them and a stock price drop (Harrison 2000). Though DoubleClick Inc. postponed the profiling program and suffered a drop in stock price, other companies are doing similar things and getting away with it. Another reason why legislation should intervene is that the majority of companies either do not have a privacy policy, do not have to follow their policy, or have an inadequate policy. Dr. Larry Ponemon, head of PricewaterhouseCooper's privacy practice, has announced his belief that approximately 80% of companies do not comply with their own policies (Petersen 2001). With the US taking a sluggish approach to the issue compared to the EU, this will only mean that the US will be a step behind in the future when more problems occur.

Comparison of US and EU Regulations

Although the United States has not made the same move as the European Union, the United States has begun to make some progress. So far they have moved toward self-regulation. Although the United States has made steps to enforce government regulations, the majority of regulations are self-governing.

The United States primarily has focused on self-regulation rather than forcing government policies on companies. The only government policy set in place thus far has been the Safe Harbor Act, which will be discussed later.

There has been a select amount of companies that have created their own privacy policies. For example, companies such as TRUSTe and BBBOnline provide seals of approvals to companies, which meet their privacy policy requirements. Although websites with this seal do have some levels of privacy, critics still believe that they are not enough. "The seal programs -- TRUSTe, BBBOnline -- are inherently ineffective self-regulatory measures (Moss 2000, p. 24)." According to Moss, the seal programs may make a user feel a bit safer, but the seals themselves do not guarantee companies will follow the privacy policies they have set forth. Another example is in the financial community, where banks and investment firms have themselves set forth privacy policies about the information collected. The downside to this is that financial institutions do not have to abide by these rules if they are not a part of the organization creating these policies.

As the European Union continues to create directives to govern how companies will treat cookies and data collected, the United States continues to push for self-regulation. But the question stands, what happens when a user from the European Union accesses a website in the United States? The answer is, the Safe Harbor framework developed jointly by the European Union and the United States.

In May of 2000, the European Union approved the Safe Harbor act (Shimanek 2001). The Safe Harbor framework allowed companies that voluntarily joined the organization safe haven from doing transatlantic transmissions. As the European Union felt that the United States' idea of self-regulation was unsatisfactory, the United States had to develop some type of regulations to meet the privacy needs of the European Union. The Safe Harbor framework brought the privacy policies from the European Union to websites in the United States (Shimanek 2001).

Members of the Safe Harbor group have strict regulations that they must follow if they want to continue transatlantic transmissions. For companies to receive the benefits of the Safe Harbor Act, they must adhere to privacy policies, which meet the requirements (Shimanek 2001). Companies may also join private privacy organizations such as TRUSTe, or create their own privacy policies, which adhere to the safe harbor requirements. Companies must also annually apply to be apart of the safe harbor (Shimanek 2001).

All in all, the European Union and the United States have differing views on the regulations of cookies. The European Union has set forth regulations that companies must follow, and the United States trust companies to govern themselves. Regardless of whether or not one method is better than the other, some form of regulation needs to be

present, enforced and standardized. The privacy issues behind cookies are unlimited and as technology advances further, regulations will have to keep up as well as catch up.

A solution to serve the interest of both sides would be to compromise, while keeping the market efficient. Corporations must be able to follow the policies with partial ease without hindering their operations, while consumers deserve a substantial amount of safeguard. Such implementation can be accomplished by congressional intervention; however it is important that a solution is created with as much market research as necessary.

Solution to Current and Future Privacy and Ethical Problems

Policy needs to educate the public over cookie technology and how companies use information about them collected through this avenue. A survey conducted by CNN showed that the majority of the public, about 56%, did not know that websites and advertisers have the capability to track their activities by placing cookies on their hard drives (CNN.com 2004). This lack of understanding of cookie technology only makes it easier for the public to be exploited by unscrupulous sites. Their lack of awareness does not entitle others to take advantage them over the Internet. Also, from the survey, 94% of Internet users feel that firms and their executives should be punished if they violate a user's privacy while they are online (CNN.com 2004). The numbers show that the vast majority of the public is worried their privacy will be violated and if so, someone should be held accountable. But there is no current directive to force firms to follow an adequate privacy policy and there is not any real consequence for firms to face. At this point it does not seem the public will be able to feel any safer so long as there is not a lasting reaction.

When Al Gore was the Vice President, he took it upon himself to be concerned about the lack of privacy on the Internet. During his term, he proposed the idea of an "Electronic Bill of Rights." However, when his term ended and he lost in the 2000 Presidential election to President Bush, his initiative was ignored. Gore was able to recognize a problem destined to grow along with the growth of the online market. His program idea would have been able to help the US in facing future dilemmas. It is our intention to advance Gore's initial idea of an electronic bill of rights through our suggestion for a possible future privacy policy. More importantly, we would like to borrow the name and give credit to Al Gore for the purpose of answering the ethical problem of privacy invasion of cookies. Our proposal is only a suggestion and not anything that should be considered definite by any means. The following is our "Electronic Bill of Rights":

Electronic Bill of Rights

- 1) Prior to the usage of cookies, users must consent to and agree with the privacy policy
- 2) Users must be informed that the website is using cookies
- 3) Users must be informed in a clear and concise way of how the cookies will be used
- 4) Users must have the options to Opt-In *and* Opt-Out
- 5) Cookies may only be used in the event that the information obtained through a cookie is directly related to the value added services of the company
- 6) Users must be informed of how the data will be used
- 7) Users must be informed of when the data obtained through cookies is transferred to another company other than the originating website
- 8) Users must be informed of the duration of the cookie and its data
- 9) Information gathered by cookies is to be erased or made anonymous when the purpose of the information no longer exists, except in the event that information stored is for billing or historical transaction records
- 10) The service provider must secure the information being transferred, as well as secure the information obtained

The consensus of the current system of handling online privacy follows an end-based thinking philosophy. End-based thinking is based on doing whatever is the best for greatest good for the greatest number. The objective of self-regulation aims to best serve the online market as a whole and not the individual consumer. The theory is that if the companies are able to efficiently operate they will pass on the savings to consumers. This also would benefit the economy as a whole. Our belief is the care-based thinking philosophy best fits this situation. Care-based thinking suggests that people should do what they would like others to do to them. This way of thinking would allow for a compromise between sides so an effective solution can be made. If firms used care-based thinking they would be more sensitive to the rights of their customers. Thus, a solution of compromise will be made possible to keep our worries about privacy to a minimal. Although the concerns for privacy are looming large, there is hope for us if we take precautions now, not when it is too late.

Works Cited

- Bayan, Ruby. "Privacy Means Knowing Your Cookies." *Link-up* Jan/Feb 2001: 22-23.
- Cattapan, Tom. "Destroying E-Commerce's 'Cookie Monster' Image." *Direct Marketing*. April 2000: 6.
- "Cookie Law." AboutCookies.org: Cookie Law :: AccessKey 3. Out-Law Compliance. 21 Oct 2004 <<http://www.aboutcookies.org/cookieLaw.asp>>.
- Dictionary.com. 20 Oct 2004 <<http://www.dictionary.com>>.

Electronic Communications Guidance. "Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003." *Information Commissioner*. November 2003.

European Union. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)." *Official Journal of the European Communities* 201.37 (2002): 7.

European Union. "Privacy and Electronic Communications (EC Directive) Regulations 2003." *EC Directive* (2003).

Harrison, Ann. "Keeping Web Data Private." *Computerworld*. May 8 2000: 57.

Landesberg, Martha K., and Laura Mazzarella. "Self-Regulation and Privacy Online: A Report to Congress." *Federal Trade Commission* Jul 1999. 24 Oct 2004 <<http://www.ftc.gov/os/1999/07/privacy99.pdf>>.

Mason, Richard O. "Four Ethical Issues of the Information Age." *Management Information Systems Quarterly*. 10.1 (1986): 5 - 12.

Moss, Mark R. "Ruling e-commerce: The FTC, self-regulation, or both?." *Office Solutions*. August 2000: 24.

Peek, Robin. "Privacy, publishing, and self regulation." *Information Today*. Feb 1998: 38-40.

Peng, Weihong, and Jennifer Cisna. "HTTP cookies - a promising technology." *Online Information Review*. 2000: 150.

Petersen, Andrea. "E-Commerce (A Special Report): Industry by Industry --- Privacy --- Private Matters: It seems that trust equals revenue, even online." *Wall Street Journal*. 12 February 2001, R.24.

"Privacy Compliance Resources." IDcide Inc. - Privacy Compliance Resources, Privacy Glossary. IDcide. 25 Oct 2004 <http://www.idcide.com/pages/res_term.htm>.

Shimanek, Anna E. "Do You Want Milk With Those Cookies?: Complying With the Safe Harbor Privacy Principles." *Journal of Corporation Law*. 26.2 (2001): pg. 455.

Stenger, Richard. "Hotmail, Yahoo scramble after email security flaws exposed." CNN.com - Technology - Hotmail, Yahoo scramble after email flaws exposed - May 10, 2000. CNN. 18 Oct 2004 <<http://archives.cnn.com/2000/TECH/computing/05/10/email.security/>>.

"Survey: Most in U.S. want companies to guarantee online privacy." CNN 21 August 2000. 2 Nov 2004 <<http://archives.cnn.com/2000/TECH/computing/08/18/privacy.report/>>

Vijayan, Jaikumar. "Users of online job services risk lack of privacy protection." *Computerworld*. Nov 17 2003: 10.