Ethics and the Internet: An Analysis of On-line Privacy

An Honors Thesis (HONRS 499)

by

Stuart T. Janney

Thesis Advisor
David B. Annis, Ph.D.

Ball State University
Muncie, Indiana

May, 1997

May 10, 1997
Abstract

The explosion of the Information Age has brought with it unforeseen challenges to society. One such challenge is the establishment of what should and should not remain private and how to enforce these rights. This paper examines privacy issues in relation to the Internet in three specific areas: anonymous remailers, "cookies," and encryption software. Standards in place today are examined, and steps towards protection of privacy are suggested for the future.
Stylistic Note:

Unfortunately, there is no one official standard for MLA-style citation of all electronic information. For the purposes of this paper, I have selected to use *MLA-Style Citations of Electronic Sources* as formulated by Janice R. Walker of the University of South Florida. Since Walker’s guide does not mention a proper method for in-text citation of material, I have been forced devise my own method. When citing information obtained from the World Wide Web, the author’s name will be given without a page number. This is necessary because web pages are not broken down into pages when viewed in browsers. Further, not all browsers have a standard method for printing; in other words, what may be page three when printed from Netscape Navigator may be page four when printed from Microsoft Internet Explorer.

If the reader wishes to verify the accuracy of a quotation, he or she is invited to visit the web site listed in the “Works Cited” portion of this paper. Since some of these web sites can be quite large, I would suggest that the reader use the “Find” feature in their browser to locate the phrase in question.
Ethics and the Internet: An Analysis of On-line Privacy

I. Introduction and General Outline

The Internet is fundamentally changing the way the world operates. It has forced societies around the globe to re-evaluate traditions and features of society which have gone unquestioned for decades. The Internet has modernized the way human beings communicate and has completely altered perceptions of distance; communications that once took days to deliver now take only fractions of a second to reach their destinations. It is also true that the Internet has led to an explosion of information. This is almost a unanimously celebrated consequence of this newest global communications network; however, it is not without its downside as well. Some fear that the new medium will almost certainly spell an end to privacy as it is now known or enjoyed. It is the position of this thesis that in order to protect privacy in this new medium, there must be moderation; neither absolute privacy nor absolute disclosure will provide a reasonable answer to the problem at hand.

This discussion will explore issues surrounding privacy on the Internet. It will seek to answer questions such as, “Is there really any such thing as privacy on the Internet? How much privacy should there be, if any even exists? Who should set the standards for on-line privacy?” To begin, definitions of key terminology will be established. A philosophical notion of privacy, in addition to a legal definition of the right of privacy, will be given. Following this will be a brief discussion of what the Internet is. Specific aspects of the Internet will be elucidated as they become relevant to the discussion at hand.

Following this, privacy will be examined with respect to the following three areas of the Internet: the right to anonymity on the Internet, “cookies,” and encryption. After examining these issues, the discussion will turn to the question of what should be done regarding on-line
privacy, and will then look at one event involving the Social Security Administration which spawned a great amount of concern about what personal information can be obtained via the Internet by almost anyone. The discussion shall turn to what measures are in place now to protect the privacy of individuals in cyberspace. Finally, an answer will be posed to the question of whose responsibility it is to safeguard privacy in a digital world and why a moderate approach to privacy issues is the most preferable solution to the problems at hand.

II. Definitions of Key Terminology

Before any serious discussion of privacy and the Internet can take place, key terms must be defined in order to establish a common understanding of the topics at hand. In *The Oxford Dictionary of Philosophy* Blackburn defines privacy as "that which it is no business of the public, and particularly the public institution of law" (303). Also, Blackburn notes that "private information about a person would be that to which there can be no right of public access" (303). He further states that any attempt to assign an objective opinion on an abstract notion is often heavily criticized by certain groups. As an example of this, Blackburn recalls that feminists often question *any* distinction between the terms "public" and "private," claiming that notions of privacy only serve to hide "unrestricted male domination of children and women" (303).

However, for the purposes of this discussion, Blackburn’s definitions of private conduct and information will be accepted as a legitimate explanation. For the purposes of this paper, one must examine a legal definition of the privacy and one’s right to it, as well. *Black's Law Dictionary* defines the right of privacy as a "generic term encompassing various rights recognized to be inherent to a concept of ordered liberty, and such right prevents governmental interference in intimate personal relationships or activities, freedoms of individual to make
fundamental choices involving himself, his family, and his relationship with others” (Black 1195). This definition is highly similar to the philosophical definition given earlier, and is equally vague. However, Black's Law Dictionary expounds on this definition somewhat by noting the four varieties of tort actions included under the more general “invasion of privacy.” The first is appropriation, which refers to assuming the identity of another individual for any advantage or gain of he or she who assumes the persona (Black 1195). The second is intrusion, which “consist[s] of intrusion upon the plaintiff’s solitude or seclusion, as by invading his home, eavesdropping, as well as persistent and unwanted telephone calls” (Black 1195). The third variety is public disclosure of private facts, the meaning of which is understood almost prima facie. The most important item to note about this type of invasion of privacy is that all disclosed facts are true; this is not to be confused with an instance of an individual creating and subsequently circulation falsehoods about another person. That type of invasion of privacy is the fourth classification, known as false light in the public eye, “[consists] of publicity which places the plaintiff in a false light in the public eye” (Black 1195). Of primary concern to this discussion will be intrusion and public disclosure of private facts.

In order to establish a common framework for discussion of the issues at hand, it is necessary to formulate a definition for the Internet. Bill Gates gives this definition of the Internet in his book, The Road Ahead: “[the Internet] is a group of computers joined [which are] exchanging information using current technology” (3-4). This group of computers is joined or connected primarily by wires. These range from ordinary telephone cable, which carries information at a rate of 28,800 bits (or more commonly “baud”) per second (bps) to 33,600 bps to special cable known as ISDN, which can support up to 128,000 bps. Although there are
connections which provide even greater speed, most of these are reserved for use by large corporations and Internet Service Providers because of the prohibitive cost associated with them. Only a small percentage of the information which traverses the Internet does so by means of satellite technology; for the most part, data transmission is done by wire. The Internet is truly a global phenomena. According to PBS Online, “the World Wide Web sports a growth rate of 341,634% in service traffic in its third year, 1993.” This means it spans a great number of countries, which creates problems when dealing with issues of regulating the Internet, as will be discussed later in this paper.

III. Privacy and the Internet

Before discussing electronic privacy, Cavazos and Morin discuss the views most Americans hold regarding privacy in general. They remark that privacy is “considered [to be] a core value by most citizens . . . [although] it is not explicitly delineated as a protected right by the U.S. Constitution” (13). The hypothesis is then formulated that “the reason privacy is not explicitly mentioned in the Constitution is that at the time of its drafting there were only a small number of ways that one’s privacy could be invaded” (Cavazos and Morin 13). However, in the last two centuries in particular there has been a veritable explosion of ways which one can invade the privacy of another. Cavazos and Morin comment that “the framers of the Constitution could not address . . . the myriad of privacy concerns that developed as new technologies were introduced into society” (13). This has necessitated the formulation of laws which are designed to prevent such invasions.
One proposal to curb the number of invasions of privacy performed via electronic means\(^1\) is the end of anonymity on the Internet. Consider the case of “anonymous remailers.” Because e-mail can easily be traced back to its origin, anonymous remailers were introduced to the on-line world. These anonymous remailers are “programs that receive mail, strip it of any traceable identifying information, and forward it to the addressee” (Cavazos and Morin, 16). Further, there are also “anonymous servers,” which are systems that allow the individuals or groups of individuals to communicate with complete anonymity (Cavazos and Morin, 16).

Anonymous e-mail can be used for many purposes which would benefit society. Individuals could safely register legitimate complaints without having to worry that their identity will be made known. People could safely report criminal activity without having to worry about their safety — for example, a person could report that his neighbor was selling drugs in the apartment complex with much more security than having to place a traceable telephone call. Individuals could even share stories in public forums that they might not otherwise share; in other words, there could be a very large advice column, where instead of one person giving suggestions, thousands upon thousands could voice their recommendations.

Unfortunately, anonymity and e-mail can be used for less than noble (and legal) purposes as well. Consider the case of certain newsgroups. A newsgroup is similar to a large bulletin board, and any messages posted upon it are relevant to one particular topic. For example, suppose that there are a large number of students at State University who are interested in John

\(^{1}\text{By “electronic invasions of privacy,” Cavazos and Morin are referring to “electronic eavesdropping devices, video and sound recording instruments, and large databases of personal information” (13). Although they do not implicitly state that interception of e-mail is a form of electronic eavesdropping, most would concur that it is.}
Grisham novels. They wish to organize a meeting so that they may discuss their favorite author. However, since the group is so large, there is no way that the students can all meet at one time. One student proposes that they reserve a bulletin board in the Student Union for their exclusive use. Here students may post messages about *The Partner*, Grisham's latest, to share their thoughts on the matter. Each message has a subject line at the top so that someone may walk up to the board and read just one line to see whether or not they care to invest the time to read the entire message. If they do read it and wish to reply, they may do so. Now, another group of students, having seen the success of this idea, reserves their own bulletin board for messages regarding the TV series *Star Trek: Deep Space Nine.*

Newsgroups operate in a similar fashion. There tens of thousands of newsgroups, each one organized by topic as in the preceding example. Internet users may choose to view newsgroups about topics which interest them, and they can then choose to participate in discussion through electronic messages which are "posted" to these electronic bulletin boards. Once a message has been posted, it is possible for anyone with access to that newsgroup to read it. As pointed out earlier, anonymous messaging can serve many useful purposes. Think for a moment of rape victims. These individuals understandably may not want to share the stories of their victimization with other people in a face-to-face situation. In this case, the Internet provides a forum, with the help of anonymous servers, where victims may discuss their situations.

---

2In fact, there is a newsgroup dedicated to this particular author's works: alt.books.john-grisham. There are also many newsgroups for discussion of Star Trek in its many incarnations; the most popular is probably rec.arts.startrek.current.
without the same level of awkwardness that might be present when physically surrounded by others. This forum may help many come to terms with devastating experiences.

Unfortunately, as noted earlier, it can also be used for other purposes which do not share the same high goals. The following screen capture shows the results received when a search was performed for all newsgroups with the word “rape” in their title. The newsgroup “talk.rape” is perhaps a newsgroup dedicated to helping victims of that particular crime overcome their negative feelings. However, what positive thing can be said about the newsgroup entitled, “alt.binaries.pictures.erotica.rape”? Most likely, individuals who post pictures of rapes to this group will use anonymous servers in order to prevent apprehension by authorities.

Figure 1 - Screen capture of a list of newsgroups containing the term “rape” in their titles.

3 At no time were any of the newsgroups seen on this screen accessed by the author.
Coursey argues that this service should not be allowed. “Sure, on the Internet nobody knows you’re a dog, but they also don’t know you’re a stalker, a child pornographer or a member of the Cali drug cartel,” he writes. “I’d like that to change.” Therefore, he proposes that “every account or username would have to be linked to a master account and a human being. Online services would be required to keep user E-mail logs and transcripts for at least thirty days, allowing for the resolution of disputes and criminal investigations”. Coursey’s idea is extreme; he readily admits this himself. Is this, however, a good idea?

As it stands, just because a person uses anonymous e-mail does not mean that he or she will not be apprehended or reprimanded by the authorities. The government has already “used fire to fight fire.” Government authorities will frequently use anonymous e-mail to allow them to go undercover on the Internet. Imagine a situation where someone is using anonymous servers to organize buyers for illegal substances. When the goods are shipped or delivered in person, the guilty party may be apprehended. In effect, it is no different from undercover officers soliciting prostitutes or drug dealers in order to apprehend them. Further, as noted earlier, anonymous servers can be used for perfectly legal and positive uses, as well. Therefore, some may feel that Coursey’s suggestion ultimately goes too far and may ultimately do more harm than good. “If it isn’t broken,” the adage says, “then do not fix it.” In this particular instance, the adage may apply.

Following Coursey’s idea would lead to a loss of privacy which can be very beneficial in many circumstances. Forcing individuals’ identities to be linked to a central database by which their comments may be linked back to them could create a stifling atmosphere wherein people
may be too afraid to speak their minds. Imagine if Ann Landers either printed real names instead of pseudonyms or provided a means by which the identities of the persons writing letters to her could be obtained. Certainly this would decrease the volume of letters her column receives. Who would want to write about their new spouse’s annoying family or co-workers bad personal hygiene? Similarly, this could be the case on the Internet. Granted, the cases in the previous example may seem trivial, but they could just as easily concern victims of fraud or personal tragedies whose comments could positively affect the lives of countless others.

Yet another method to limit abuses by anonymous servers would be to make sure that those who operate them are subject to strict federal regulation. This might limit the number of servers available to users. If they are not very common, it is possible that their use might be limited (or the use of those few might increase dramatically, conversely). Finally, if users were forced to pay for an account, this too might limit the use of the services to those who only need to use the service for legitimate purposes. Of course, it might also compromise the privacy of the person using it — although complete privacy is never assured when using these services in the first place. Cavazos and Morin note that “their traffic might be monitored, or the individuals operating the service might keep system logs that compromise the confidential nature of the service” (16). Perhaps it might be possible to set up a system of anonymous payment in which the identity of an individual would be compromised only if he or she did not pay. Regardless, there are enough possibilities of monitoring these systems to prove that eradicating them would be a premature and unnecessary step.

Yet another area of concern regarding privacy and the Internet are web browsers and “cookies.” A web browser is a program such as Microsoft Internet Explorer or Netscape
Navigator which allows a user to view World Wide Web documents. If viewing information on
the Internet is truly like surfing, as the very popular analogy suggests, then the web browser is
the board upon which you surf. Most people assume that browsing is a relatively secure
operation; they mistakenly believe that the sites they visit cannot be tracked. This, however, is
not the case — small pieces of data known as “cookies” ensure that someone somewhere will
have the ability to determine whether or not an individual has visited their web site.

Mayer-Schönberger explains the concept of the cookie by an example similar to the one
which follows. Picture Joe Smith in front of his PC. He connects to his ISP\(^4\) and uses his web
browser to access the MSNBC homepage. MSNBC is a news service which is a joint venture
between the Microsoft Network (an ISP such as America Online) and NBC. MSNBC presents
current news and editorials on both a web page and a cable or satellite television station.
However, unlike the MSNBC television station, their web page allows users to customize how
the page will appear. For example, Joe Smith is a conservative political science professor. He
can therefore customize the page such that it shows more news relating to state and federal
government and fewer sports related stories. Further, he can even choose to read editorials from
writers who are more conservative than liberal. However, there must be a way for the computer
to remember this information so that even after Smith has logged out and back in, all of his
personalized features will not be lost. This is where the cookie enters the picture. As Smith is

\(^4\)ISP stand for Internet Service Provider. These are businesses which allow other
businesses, schools, and individuals to access the Internet with a PC and a modem. Probably the
most well-known example of an ISP is America On-Line. Other national ISPs include Microsoft
Network and Prodigy. Smaller, local ISPs available to residents of Delaware county include Net
Direct, Iquest, and IndyNet.
customizing his page for the very first time, the MSNBC computer creates a small packet of data which contains a list of features which he has personalized. The computer then sends this to Smith's computer, where it remains. However, the next time Smith logs back into MSNBC, the cookie is transmitted from Smith's computer to the MSNBC server. This entire process occurs without the knowledge or consent of the user. "This happens without any notification or user consent," writes Mayer-Schönberger. This in itself seems rather harmless; in this context, perhaps it is.

However, Mayer-Schönberger continues: "... a Web server (the computer to which the user connects to when viewing a web page — in the case of our previous example, the MSNBC web server) may set a cookie so that an unlimited number of other servers have access to the cookie information as well." Consider the impact of this; if a cookie is designed so that any web server can access it, what information is being given to companies or individuals around the globe? Suppose that you have accessed twenty-five pages in the last month which make use of cookies. Of those twenty-five, ten are written such that they are sent to every web server which utilize cookies. What personal information about the individual is being transmitted without consent, and who is receiving it? Further, for what purpose are those on the receiving end using the information?

"While the U.S. and Europe are in general agreement on the principal importance and validity of privacy and the protection of one's personal information, the scope of privacy rights differs substantially between the U.S. and Europe," Mayer-Schönberger writes. He goes on to write that the United States tends to protect only certain forms of electronic privacy, "such as in
the area of credit reporting or video cassette rental. European nations have openly embraced omnibus data protection acts covering each and every electronic processing of personal data."

Clearly, this use of the cookie is an invasion of privacy by both a public disclosure of private fact, and a case can be made that privacy is invaded by intrusion as well. In the case of public disclosure of private facts, if you customize a page with information which potentially discloses your racial background, religious affiliation, or even sexual orientation in the form of a cookie which will be distributed to any number of individuals without your knowledge or consent, the loss of privacy is obvious. How, though, is it a case of intrusion? Recall that any intrusions into "[an individual's] solitude or seclusion, as by invading his home, eavesdropping, as well as persistent and unwanted telephone calls" (Black 1195). The point of interest here is eavesdropping — and in essence, is not the collection of facts one's private interests, pastimes, and background with neither the consent nor knowledge of the one studied eavesdropping?

Undoubtedly, the answer is yes. However, an opponent of this position would be quick to point out that the individual whose preferences, etc., were being made known was in error in believing that their on-line activities were somehow private to begin with. Ignorance does not constitute an excuse, they might claim.

Steps are already being taken to counter the problematic nature of cookies. Newer versions of browsers can be customized such that they display a warning message before a cookie is accepted. However, as Mayer-Schönberger points out, "such warnings do not contain the information required . . . for the user to give her 'informed' consent." Consider, as an example, an actual warning this author received from his browser as he accessed a commercial web site.
As the reader can plainly see, the warning is cryptic and impossible for the lay person (and even those who are not lay people, in many cases) to understand. Further, this warning says nothing of the information which will be divulged. Instead, it asserts that the contents of the cookie are "BHLBDFZRAIWWIEZ." Further, take note of the expiration date field! There is nothing there, which means that perhaps this cookie will terminate as soon as the session ends, or perhaps it does not ever expire. Finally, note that if the user clicks the "No" button, the page may not display properly. This might convince the average computer user that perhaps they would be better off accepting the security risk which they do not understand so that the page will display as it should. It seems that perhaps this security feature is not so much for the user's peace of mind, but rather for the purpose of the browser manufacturer being able to tout their highly secure browser.

Cookies are also used for advertising purposes, in which case unsuspecting users become demographic data for companies with a web presence. Often, Mayer-Schönberger points out, many commercial web sites are supported by advertising, which works in the following fashion.
Suppose a user visits the ACME company homepage. To help subsidize the cost of their page, ACME allows other companies to advertise on small segments of the ACME page. Now, further suppose that Yoyodine Industries wants to advertise on the ACME homepage. ACME sets up their web page so that each time the page is accessed, their web server contacts the Yoyodine web server and downloads the advertisement.

Mayer-Schönberger writes, "... as this transpires, something quite clandestine happens: the advertisement server sets a special cookie in the user's computer." Now suppose that Yoyodine advertises on over 1,000 different corporate web pages around the globe. If Joe Smith (from the earlier example) leaves the MSNBC homepage to view a list of ACME's products, and Yoyodine is advertising on the ACME page, then a cookie will be deposited into Smith's computer from the advertisement. If Smith visits a different web site upon which Yoyodine advertises, "the cookie data residing in the user's computer will be transmitted automatically to the advertisement server," Mayer-Schönberger notes. This data is then collected and used to create profiles of who the company's most likely customers would be. "The user has become the unpaid agent of the direct marketing agency, supplying it with all the personal information and preferences needed, but without ever knowing it," Mayer-Schönberger concludes.

Netscape Communications, however, has this to say in response to the question, "Can cookies be used to gather sensitive information, such as a user's email address?"

Cookies cannot be used to gather sensitive information such as the fields in a Netscape preference file. They can be used to store any information that the user volunteers, for example by filling out an HTML form. In this case, however, the same information can just as easily (and with potentially more objectionable privacy concerns) be stored on the
server by using a simple server-side application that stores user information in a database.

Cookies are passive data structures that are delivered to the client, stored on the client's hard drive, and returned in certain situations to the same server that provided the information in the first place (Cookies and Privacy FAQ).

The above is true of cookies which conform to the Netscape standard (Netscape Navigator has supported cookies since version 1.1). However, Mayer-Schönberger points out that the Netscape standards easily enables servers to overwrite those standards. "Though it is not illegal per se, the browser companies provide a structure that not only creates loopholes but makes compliance with specific requirements of data protection norms, like notification and consent, difficult to conceive and realize," Mayer-Schönberger says.

This leads one to the conclusion that cookies do not allow for protection of private facts. Again, this could ultimately lead to claims that the browser manufacturers have allowed for public disclosure of private facts, and that more steps should have been taken to protect the privacy of the end-user. Obviously, one way to maneuver around the cookie problem would be to make it very easy for the user to manipulate them. Imagine if cookies were as easy to control and understand as the web browser itself was. Consider Figure 2. Would it be quite as objectionable if it told the user exactly what data was being transmitted in language simple enough for everyone to understand? For example, instead of saying "BHLBDFTZRAIWWIEZ," what if the warning screen said, "Information regarding the number of times you have visited this site as well as data regarding your preference for conservative editorials, the stock quotes you have chosen to see, and NBA scores you want reported is about to be sent to the MSNBC server. Do you want to send this information?" Further, the page should display the same regardless of
whether or not a cookie is sent. Cookies should not be allowed to be sent to any server other
than that which created it. Ease of use, coupled with full disclosure of the cookie’s contents, as
well as information regarding the cookie’s ultimate (and only) destination would prevent these
files from potentially invading the privacy of the end user.

Yet another area of concern for those wishing to protect the right to privacy in the on-line
world is encryption software and the attitude of the federal government towards it. According to
Bill Gates, mogul of the Microsoft empire, the traditional encrypting of data is a fairly simple
process; deciphering that same data, on the other hand, can represent quite a challenge if the
encryption has been done properly (109). Encryption uses prime numbers, which are numbers
unable to be divided evenly by anything other than 1 and itself. For example, 7 and 13 are prime
numbers, while the numbers 9 and 27 are not; the latter two numbers are both evenly divisible by
three. Therefore, they cannot be prime. It is exceedingly simple to multiply the prime numbers 7
and 13 and discover that the resulting number is 91. It is, however, more difficult to try to find
out which two prime numbers were used to produce 91. Now, consider multiplying two prime
numbers when each number contains over two hundred and fifty digits. Gates reports that “... mathemicians today believe that a 250-digit-long product of two primes would take millions of
years to factor [the process by which the two prime numbers were multiplied to end up with any
resulting number x] with any foreseeable amount of computing power” (110).

How does this figure into encryption? Once again, imagine Smith at his PC. He wishes
to send encrypted data to Jones, a recipient in a different country. Presumably, the process of
encrypting data or e-mail for the end user will be simplified to the point of clicking on a toolbar
icon which resembles a padlock or a key. However, what goes on inside the computer when the
button is clicked is not so simplistic. “Each user’s computer,” Gates writes, “... will use prime numbers to generate an enciphering key, which will be listed publicly, and a corresponding deciphering key, which only the user will know” (108). When Smith clicks on the toolbar icon which encrypts the contents of his message, the computer will look up the intended recipient’s public enciphering key. This public enciphering key is then used to encrypt the message. Upon receipt of the encrypted message, Jones’s computer utilizes its private deciphering key to decode the message so that it may be read. If Jones sends Smith a reply which he wishes to be encrypted, the process is reversed. Now Jones’s computer will look up Smith’s public enciphering key and use that key to encrypt his message. Smith’s computer will then use its private key to decipher the message. Since both of these keys are created by utilizing remarkably large prime numbers, this system is remarkably secure — some even say perfectly secure. The WWW Security FAQ says this of encryption: “The message can only be decrypted by the owner of the secret private key, making it safe from interception. This system can also be used to create unforgeable digital signatures.”

Naturally, this system of encryption has both practical utility as well as less-than-noble uses. For example, encryption could allow doctors to securely discuss their patients in an effort to help diagnose or cure an illness with greater privacy (and speed) than ever before. Lawyers could use the system to consult with not only their clients, but also other attorneys on their particular case and similar cases, secure in the knowledge that the attorney-client privilege was in no danger of being violated. Government officials could discuss matters of national security without having to worry about covert surveillance. The possibility for encryption to do enormous amounts of good for society are endless.
The detractors of encryption are quick to point out that it can also do enormous amounts of damage, as well. Child pornographers could exchange materials without concern of being apprehended by the authorities. Drug cartels and organized crime could engage in illegal doings without having to worry about getting caught. Naturally, this is not a desirable situation as far as most are concerned.

Of course, this means that the federal government no longer has the ability to monitor communications as it once did. Naturally, this has received attention origination from the highest levels. “President Clinton and I are committed to promoting the growth of electronic commerce and robust, secure communications worldwide while protecting the public safety and national security,” Vice President Gore said in a statement regarding encryption on October 1, 1996. However, Alex Lash, in a recent C|Net article, writes that “the Clinton White House wants access to encrypted messages everywhere . . . according to a March 12 draft of the ‘Electronic Data Security Act of 1997’ obtained by . . . [the] Center for Democracy and Technology . . . the administration wants to find a sponsor for a bill that would give law enforcement agencies the ability to intercept and [sic] encrypted communication and stored data.”

What does this mean for on-line privacy? As Esther Dyson was quoted as saying in the transcript of “Third Panel Discussion Questions and Answers” from the White House Forum on the Role of Science and Technology in Promoting National Security and Global Stability, “. . .if the government can watch everything that goes on and the government is good, that is a very good situation. If the government can watch everything that goes on and the government is bad, that is a very bad situation.” Consider, as an example, an investigation into a high-ranking government official at the behest of the general public. If the investigators trade any information
electronically, there would be a risk that the security of that information might be compromised, resulting in a perversion of due process and justice. It would also mean that those individuals working for government agencies could potentially have access to medical and financial records of any person who transmits any electronic reports regarding those matters. Again, it could result in an invasion of privacy through public disclosure of private facts. Ethically, though, does not the American government have the responsibility of safeguarding its citizens from criminal activity? Undoubtedly, the answer is yes, the government is responsible for the well-being of the public. However, this could be done even more effectively if the government did not require warrants to search homes. Should it be given the right to search the contents of email without any similar document? In his article, Lash reports that "[according to] Jonah Seiger, a policy analyst at the [Center for Democracy and Technology] . . . ‘Email communications are a much richer view of what you do and who you are, more analogous to your living room than to your phone. We don’t allow secret searches of people’s living rooms.’"

In WashingtonPost.com article by Pacheco and Whitney regarding encryption, FBI director Louis Freech is quoted as saying, “. . . we are simply looking to continue . . . electronic surveillance under very stringent conditions. If we foreclosed from those areas . . . the safety of this country will be impaired.” Undoubtedly, he is correct. Also in that same article is a quote from Senator Conrad Burns which reads, “. . . denying millions of law-abiding people the use of . . . a security product for ‘law enforcement’ reasons is like banning deadbolt locks because they make it a little harder to kick down the doors of a few drug dealers.” Undoubtedly, Senator Burns is also correct. Therefore, an acceptable solution to all concerned parties must lie between these two positions. Currently, “the Clinton administration has espoused a policy that gives law
enforcement, with a court order, easy access to all encryption keys. The Commerce Department is also authorized to limit the strength of encryption that can be exported from the United States. 

. . [and] the Department of Justice has the right to review any export license application” (Pacheco and Whitney). This means that ultimately, the government will have access to all public keys should it want them, a position which is highly unacceptable to privacy advocates. Instead, perhaps the government should look towards a policy similar to the one which they now have, only without giving the government the ability to directly intercept any encrypted communication. What might be more acceptable to all concerned parties would be a program by which any manufacturer or exporter of encryption software would have to receive a license before dealing with the product. Standards for receiving a license would be agreed upon not only by the government but also by representatives from the industry to ensure that the criteria were not so stringent as to make it impossible to obtain the necessary certification. Finally, any end-users who desire to use the product should be made to obtain a license or a permit and be registered as a user of encryption software. Some restrictions on end-users which would prevent them from being able to obtain encryption software would be prior criminal convictions, for example. In this way, encryption software would be marginally controlled, but still accessible to those with legitimate needs.

IV. What Should Be Done?

Determining what is to be done about these privacy issues and the ethics surrounding them has become a hotly debated topic in Washington, D.C. One notable event recently caught the attention of U.S. lawmakers: “. . . the Social Security Administration’s Web site [had a] feature that allowed surfers to look up their salary information, records of taxes paid into Social
Security or Medicare, and eligibility for benefits” (Macavinta). This spawned a rush of legislation designed to prevent any further breaches of privacy. Macavinta notes that soon after, the Personal Information Privacy Act, the Federal Internet Privacy Protection Act, the Social Security Information Safeguards Act, and the Social Security Online Privacy Protection Act were all introduced or reintroduced for consideration to Congress. The Social Security Information Safeguards Act and the Social Security Online Privacy Protection Act are both designed in order to prevent the disclosure by ISPs of clients’ Social Security Numbers to third parties. The Personal Information Privacy Act also seeks to keep Social Security Numbers from being disclosed on the World Wide Web, but in addition attempts to prevent the use of “unlisted telephone numbers and other personal information” (Macavinta). The Federal Internet Privacy Protection Act is different in that it is “would prohibit federal agencies from making available online individual’s records on education, financial transactions, medical history, or employment history that contain the name, an identifying number, or symbol assigned to individuals” (Macavinta). In the article, Senator Dianne Feinstein of California was quoted as saying, “our private lives are becoming commodities with tremendous values in the marketplace.” This is especially true when considered in the light of the cookie debate. Further, this leads to a highly probable invasion of privacy by appropriation (taking the name or likeness of another for the benefit of the appropriating party).

Consider the following example. In a virtual world, invasion of privacy by appropriation could be performed by simply accessing that feature of the Social Security web site which allowed users to obtain such information about other individuals (it is important to note that this feature of the web site was quickly disabled). With the Social Security Number of another
individual, it would be possible to obtain very important personal information, such as bank
records. With these bank records, it is conceivable that credit card numbers would be a phone
call away. This would clearly be a case of violation of privacy.

Ethically, though, whose responsibility is it to serve as watchdog for on-line privacy?
Some seem to believe that it should be the federal government in domestic matters. Coursey
states:

“online services need to rewrite their terms of service to make it clear that users have no
expectation of privacy if a law-enforcement authority shows up with a warrant. Privacy
should also be waived if it’s necessary to investigate serious infractions of other parts of
the service agreement — such as unsolicited pornography, password hackers, stalkers and
threats. But the services should be prohibited from reading users’ E-mail without proper
cause.”

This, of course, is one possible answer to the question of on-line privacy. However, he
leaves unanswered the even more important question — what is proper cause to read users’
e-mail? Naturally, if standards which are applicable for interception and reading of postal mail
were applied to e-mail, this would provide a set standard which would likely be acceptable to the
vast majority of users. However, he says that privacy should be waived if there is an
investigation of a severe infraction of the agreement the user entered into with his or her ISP
upon signing on for the service. This seems to indicate that the ISP would be responsible for the
investigation. If this is true, then it would stand to reason that they would set the standards for
what constitutes “a serious infraction.” This may lead to the possibility that e-mail could be
intercepted and read in the name of “investigating a serious infraction.” Moreover, the end user
would likely never know that the e-mail was read by someone other than the sender and him or herself. It would likely be acceptable to a majority of people to let only the local or federal authorities investigate such matters, and as shall be discussed next, the Electronic Communications Privacy Act seems to stand in disagreement with Coursey. If small businesses are able to have access to personal communication, this could lead to a public disclosure of private facts if employees who routinely read users' e-mail divulge their contents. Having the authority to intercept and read electronic communications in the hand of people who are trained and trusted to perform such investigations would seem more likely to protect the average person's privacy.

V. Safeguards In Place Today

Another perhaps more sensible step taken to protect on-line privacy was first formulated in 1968 by Congress. According to Cavazos and Morin, the lawmakers were concerned that "newly developed means of electronic eavesdropping posed a serious threat to privacy rights" (16). The result was the Electronic Communications Privacy Act (ECPA), and it was revised in 1986 to account for newer forms of communication (16). Under the ECPA, it is illegal to attempt to or successfully intercept electronic communication in any form, as well as to "intentionally use or disclose the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of the ECPA" (Cavazos and Morin 17).

Obviously, the key term to understand is "intercept." According to the ECPA, interception is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" (qtd. in Cavazos
and Morin 18). However, the authors note that this definition is under constant revision and should not be said to be absolutely finalized. The Act also goes on to describe the roles of those in charge of the ISPs, the system operators (or simply, “sysops”). It carefully outlines the only conditions in which they may divulge the contents of any communication sent to them or those they employ. The first is if the sysop is authorized to take such action under the ECPA. The second situation in which the sysop would be legally able to reveal the contents the message is if the sysop has the permission of the sender or any recipient of the communication. The third provision arises if it is necessary for the sysop to open or divulge the contents of the message in order to properly send the message (presumably to prevent the message being lost because of a technical problem). Finally, the sysop may divulge the contents of a message if it was accidentally sent to him or her and the contents deal with impending criminal activity (Cavazos and Morin 18).

In the case of e-mail or other electronic messages not sent directly to the sysop or those working for them, the following are exceptions where either interception or disclosure (or both) are not considered to be violations of the ECPA. Cavazos and Morin summarize the most important of these exceptions as being situations where:

- the interception or disclosure were done while performing tasks necessary to the rendition of service to customers;
- when providing assistance to those legally able to intercept electronic communications;
- one is legally authorized to intercept an electronic communication and has the consent of any party involved in the communication or is a party involved with the communication;
one is not legally authorized to intercept an electronic communication and is or has the consent of any party involved in the communication unless the interception is performed with the intent committing a crime in doing so;

- the electronic communication is considered to be in a public forum;

- the communication was intercepted to verify that such a communication was sent (18, 19).

Now, consider the following summary of an actual story reported by USA Today on March 13, 1997. Sharon Lopatka of Maryland, age 35, was a married woman who created and maintained World Wide Web pages out of her home. She met Robert Glass over the Internet. Glass proceeded to send Lopatka e-mail detailing “in detail how he was going to sexually torture . . . and eventually kill her,” according to police documents quoted in the USA Today article. Lopatka agreed to meet Glass. Eventually, Lopatka’s husband reported to the authorities that his wife was missing; however, his wife left him a note, a portion of which read, “. . . if my body is never retrieved, don’t worry, know that I’m at peace.” Further, the article says that the note specifically requested that Lopatka’s husband not pursue her assailant in any way. It is unknown as to why she agreed to meet with Glass.

Suppose now that either Glass’s or Lopatka’s sysop had for some reason intercepted the message detailing the planned murder. Suppose further that the sysop in question was not acting in any manner by which he would be excused by the ECPA. In this instance, the sysop would be found to be guilty of the crime of intercepting an electronic communication? If he chose to notify the authorities, however, would he be charged for divulging the contents of that communication? This is one area which the ECPA does not seem to address. Is the sysop
ethically bound to notify the proper authorities and risk being punished for the illegal interception, or should he or she say nothing since legally, they should not even know of the contents of the message? Naturally, this quandary is not one which will occur with great frequency; what is important is how this issue would be addressed.

VI. Conclusion

As in many issues, moderation is called for when dealing with the regulation of privacy rights on the Internet. As Feinberg sarcastically wrote, “only those who have done or wish to do something shameful demand privacy” (343). This is, of course, not the case. As has been demonstrated in this thesis, absolute privacy could be as damaging as absolute disclosure. Therefore, the answer which causes the least damage must lie somewhere between these two points of view. Anonymous e-mail can be a dangerous thing; simply ask any one of the persons who has an image of themselves being raped in the newsgroup “alt.binaries.pictures.erotica.rape,” and you will discover just how damaging anonymity can be. However, ask any number of people who use it for legitimate purposes how useful it can be, as well. As long as those investigating crimes committed by people using anonymous e-mail have access to anonymous services as well, no one is guaranteed to be able to perform an on-line crime without worry of being caught.

This simply goes to show that there can be no one blanket policy to cover all privacy issues on the Internet. There must be at least as many safeguards as there are ways of violating privacy in order to protect the users around the world. Frequently, issues which pit competing interests against one another often lead to policies which are solutions for specific situations. Gunther notes that there can actually be two senses of the term “privacy.” The first is “a ‘right to
selective disclosure,' or interest in the control of information . . . and [secondly] a private
‘autonomy’ of choice about performing acts or undergoing experiences” (504). Interestingly,
this discussion of privacy in the on-line world has touched on both senses of the term as noted by
Gunther. Cookies, of course, refer to the first term, while the right to use cryptography might be
a case of one choosing to perform an act and wishing to do so without government interference.
Discussing the decision regarding Roe v. Wade, Gunther notes that the government may only
interfere in with the woman’s decision to have an abortion when the state’s interests are
“sufficiently ‘compell[ed]’” (514). This case may be applied to the Internet; perhaps it should
only be the case that privacy may be invaded when the state has a compelling reason to do so —
for example, if encryption software is being utilized to transmit to individuals who seek to
violate national security. There could never be only one situation or one blanket statement of
what events would compel the state to invade the privacy of an individual. Again, there must be
solutions to which are specific to the individual problems which arise.

It should be duly noted that anyone looking for a perfect solution in an imperfect world is
simply engaging in a waste of their time; instead, efforts should be made to find the happy
 mediums proposed by this thesis. However, who is responsible for seeking out this medium? Is
the manufacturers of Internet access software? Is it the ISP? Or perhaps the governments?
While all of these must have a hand in finding that medium, more than ever the responsibility
rests in the hands of the individual for the time being. However, the problem with governments
regulating what is legal and what is not is made more difficult by the nature of the Internet itself.
Since it spans the entire globe, it also spans almost every nation’s borders, as well. What is legal
in one country may not be legal in another. For example, in country X the standards for
obscenity are such that if a man or woman exposes their knees in public, they are committing a crime. How can this county’s laws be satisfied when the Internet provides access for uncountable instances of just this infraction of their legal code? Obviously, human nature would seem to dictate that for anything on the Internet, there is the possibility that someone in the world will be offended by it. It is not unlike the case of the adult bookstore in a neighborhood; the locals may object to its presence, but they do not have to visit it. Is this a satisfactory answer to their problem? Most likely, the answer is no — this bookstore may attract a number of insidious individuals who are unwanted in the neighborhood. Is the same true of the Internet? Will the availability of offensive materials cause an increase in criminal activity? Possibly — but in the case of the Internet, the availability of information and the ability to communicate inexpensively with people around the globe is more likely to cause more good overall than it will cause harm. Eventually, perhaps, the Internet could be regulated by a council of representatives around the world who speak for their individual governments so that standards can be set which are agreeable to the majority of individuals. Until such time as this is a feasible solution, which hopefully is not a time far off, one should take the time to educate him or herself about the possible invasions of their privacy which can occur and take steps to avoid them. For now, common sense and careful reasoning are the best answers to problems concerning on-line privacy.
Works Cited


Mayer-Schönberger, Viktor
http://www.wvjolt.wvu.edu/issue1/articles/mayer/mayer.htm (5 April 1997).
(5 April 1997).

(5 April 1997).

“E-mail indicates woman may have agreed to be slain.” *USA Today.* March 19, 1997.
http://167.8.29.8/plweb-cgi/idoc.pl?2128+unix+_free_user+_cgi.usatoday.com..80+USATODAY_ONLINE+USATODAY_ONLINE+NEWS+NEWS++e-mail%26indicates%26woman%26may%26have%26agreed%26to%26be%26slain
(5 April 1997).

http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html#java
(5 April 1997).

“Third Panel Discussion Questions and Answers.” *Welcome to the White House.* Tuesday, April 9, 1996.
(5 April 1997).

http://www.pbs.org/ners/timeline/network.html
(5 April 1997).