

# Privacy In The Age Of Technology

Ken Griffin, (Email: [keng@mail.uca.edu](mailto:keng@mail.uca.edu)), University of Central Arkansas  
Roy Whitehead, (Email: [Royw@mail.uca.edu](mailto:Royw@mail.uca.edu)), University of Central Arkansas  
Phil Balsmeier, (Email: [Mnmk-pwb@nicholls.edu](mailto:Mnmk-pwb@nicholls.edu)), Nicholls State University  
Jim Packer, (Email: [Jimp@mail.uca.edu](mailto:Jimp@mail.uca.edu)), University of Central Arkansas

## Abstract

*The rapid developments in technology have brought increased convenience, but at the price of loss of privacy. Consumers should be aware of the potential threat to their personal information and should learn the facts and take steps to protect themselves.*

## Introduction

In his political satire *Nineteen Eighty-Four*, George Orwell wrote about the government he imagined would exist by then, “There was, or course, no way of knowing whether you were being watched at any given moment” (Orwell 1949). Written half a century ago, this passage rings ominously true today, when, in the words of columnist Joseph Perkins, “Privacy, as we used to know it, no longer exists” (Perkins 1999). Advances in technology have made it very easy for companies to build up extensive lists of all sorts of information about private citizens and to share this information with other agencies without our being aware of what is going on.

## The Extent of the Problem

This information gathering goes on in all facets of our society; government agencies, health-care providers, financial institutions, schools, and commercial businesses all want to know our secrets. The information gatherers say that the monitoring is good for society and for the individual because, for example, it helps the police to track down criminals, helps banks prevent fraud, and conveniently puts valuable information about products and services in the hands of consumers who need that particular information, thus giving business an important boost. It creates a society that is closely linked and better informed (“About Privacy” 1999). It allows employers to keep track of workers’ activities during company hours, avoiding the loss of time spent playing online games or surfing the Web and possibly even a costly lawsuit filed by an employee offended by a co-worker’s affinity for Internet pornography (Kaprowski 1999).

An amazing array of surveillance possibilities exists today. For years, consumers have been warned that cookie technology allows web operators to identify the surfers’ interests and tailor future advertisements to their tastes. A cookie is a file that is transferred to a computer’s hard drive by some web sites. This file allows the site to record certain information about the customer, such as passwords, how long the user stayed on that site, and what items were viewed. If a purchase is made, it may be recorded as an indication of interests. All this information creates a profile that is valued by marketers as a guide for targeting sales messages to the web user. Most new browsers could be set to reject these cookies, and it is also possible to delete the cookie files from a hard drive (Gelman 1998).

Now, however, Intel has developed the Pentium III chip, which consumers worry will create the “completely transparent surfer.” Each chip carries a unique serial number that can be read by external software (Persson 1999). While the company claimed that its intention was to help eliminate fraud by allowing online retailers to make sure of a customer’s identity, opponents argued that this tracking feature had serious problems in the area of privacy. Finally, several of the major PC manufacturers using Intel’s chip agreed to ship computers with the tracking feature turned off (Gynn 1999). This solution has not satisfied Intel’s critics, who argue that as long as the chip is there, it carries the possibility of abuse (Rotenberg 1999).

---

*Readers with comments or questions are encouraged to contact the authors via email.*

A bug in Microsoft's *Internet Explorer* allows cyber snoopers to examine files on a customer's hard drive using JavaScript commands that are hidden in HTML documents. This bug was uncovered in October 1999 by Georgi Guninski of Bulgaria. It exists in *Windows 95* and *Windows NT 4.0*, and possibly *Windows 98* as well. Credit card numbers and other personal information are available to online pirates (McCullagh 1999).

A new generation of Internet monitoring software now allows employers to track the use of corporate intranets, even generating reports that could be used in court if necessary (Garfinkel 1999). Phone conversations, e-mail messages, and computer files can be monitored. In a 1995 survey of its 3,000 members conducted by the Society for Human Resource Managers, 75% of the 500 participants who responded said that an employer should have the right to read anything contained in a company-owned electronic communication system (Peterson, 1998). Sophisticated new monitoring software makes it possible for companies to keep a close watch over the computers in their offices. Data Corp., a Massachusetts-based research company, reports that 80% of large companies will be using this sort of software by the year 2001 (Shiver 1999). Past employment and salary records are available on computer databases that can be shared with outside companies that in turn give the information out to landlords, credit bureaus, and so on (Guynn 1999).

The National Security Council wants to create a computer surveillance system to watch over activities, not just in the military, but in banking, telecommunications, and transportation industries as well. The stated purpose of the system is to prevent tampering with computer systems by hackers or terrorists, but it would give the FBI access to private data of millions of innocent private citizens (Perkins 1999).

"Who could argue with trying to find out what the truth is," asks General Motors manager Terry Rhadigian, "except for the people who may be doing something wrong?" (Perkins) Still, as the amount of available information grows, so do the possibilities for misuse.

### **What Information is Available?**

An amazing amount of information is kept stored in government and private databases. For example, Sara Baase lists the following information that can be found by examining government files:

- Tax records
- Bankruptcy records
- Arrest records
- Marriage license applications
- Records of property ownership
- Motor vehicles records
- Lists of people with permits to carry firearms
- Voter registration lists
- School records, even results of psychological tests
- Medical records of citizens covered by Medicare or members of the armed services
- Welfare records
- Books checked out of public libraries

She continues with this list of information that is available from databases kept by private corporations:

- Credit histories
- Medical records
- Subscription and membership lists
- Customer lists
- Video rentals
- Bank records
- Telephone records

- Employment files
- Airline travel records
- Personal profiles of Internet use by subscribers (Baase 1997)

Online services like CompuServe and America Online build consumer profiles based on the services their customers use. They can record bulletin board information and keep track of newsgroup postings and web sites visited, thus amassing information about each customer's interests. This information can be, and often is, shared with businesses that want to track consumer interests and target advertising to those whose buying habits match a particular profile. The problem is that this information is often gathered without the consumer's being aware that he is being profiled. Sometimes the facts gathered can be misleading or embarrassing, or even dangerous to the customer, as in the purchase of material about incontinence or neo-Nazism (Baase).

Many Internet sites target children for specific marketing purposes. By offering prizes to winners who fill out an online questionnaire, companies encourage children to give out information about themselves and their parents. This information can be used for marketing or even be sold to other companies, and often the parents are completely unaware of what is going on ("Kids for Sale" 1999).

Sara Baase estimates that the average consumer is on approximately 100 mailing lists and at least 50 databases. The information is compiled from a number of sources. Warranty questionnaires, contest entry forms, and surveys provide information to direct marketers. So do donations to charity, postal change-of-address notices, and the information on checks used to purchase materials or services. The analysis of such information is done with increasingly sophisticated hardware and software and is often called data mining. Such files supply merchants like American Express, Blockbuster Entertainment Corporation, Fingerhut Company, airlines, and cruise lines with information so that they can target potential customers. As a result, discount coupons, special promotions, and other incentives can be targeted to the most likely prospects for their products and services (Baase).

### **Risks Involve in the Availability of Information**

Since these files are computerized, the information they contain is often available over networks that can be accessed by more than one organization. The existence of all this digital information about our private affairs carries risks. First, the people who maintain the files may misuse them. They can pry into our personal lives, steal credit histories, or sell the information for personal gain. Another possible risk involves leaking the information through carelessness or incompetence or its theft by hackers. Sometimes the information is given out intentionally, as in the now-notorious sale of South Carolina's drivers' license photos to Image Data LLC of New Hampshire in 1998. This incident has led to South Carolina's being ranked dead last in privacy protection, receiving the only negative score given in *Privacy Journal's* study of the 50 states' privacy protection for citizens (Davis 1999). Finally, accidental errors in a file can cause enormous trouble to the citizen whose credit history, for example, is incorrectly listed.

The problems of security are increased by the use of Social Security numbers as a method of identification in many databases. There are serious flaws with this practice. First, the numbers are not really unique, as most people believe. There are cases of the same number's being given to different people, sometimes even different people with the same name. Second, the numbers are not secure at all, and are not treated with adequate care; they are easily available to would-be identity thieves. The Internal Revenue Service prints our Social Security numbers on mailing labels for its tax forms, and most credit bureaus and hospitals, for example, routinely ask for the SSN, even though they usually do not really need it (Baase). Some restaurants even ask for a customer's SSN before accepting a check.

The easy availability of SSNs opens up the possibility of identity theft. The Federal Trade Commission maintains a central website to provide information on this growing threat. There, identity theft is defined as the appropriation of personal information for the purpose of committing fraud or theft. Identity thieves take over someone's name, Social Security number, or credit card number and then use this information to their own advantage. Consumers may discover that someone else has been using their credit card accounts to buy huge amounts of merchandise; their credit histories become delinquent when the bills are not paid. Bad checks are written by someone

who has opened a bank account in another person's name ("Theft" 1999).

### **Recommendations for the Consumer**

What's a consumer to do? Is there any hope of salvaging some personal privacy in the age of technology? Many authorities answer with a qualified "yes." In an article in *The State* newspaper, Teena Massingill argues that much of the responsibility for maintaining privacy rests with the individual. "The best way for citizens to ensure the integrity of private information is still the oldest way: Do it yourself." (Massingill 1999) She suggests that consumers refuse to disclose their Social Security and drivers' license numbers, even if this means they must change banks or service providers. Consumers should also guard telephone numbers, names, and addresses. All this information is prized by telemarketers, direct mailers, and businesses that sell data to other companies. In addition, consumers can have their names added to Direct Marketing Association's telemarketing and mailing opt-out lists, which are honored by almost 3,000 Internet companies, banks, and other direct marketers (Massingill).

Consumers should be careful when choosing an Internet Service Provider. A clear privacy policy should be available from any responsible service provider, and any service that fails to offer one should be avoided. In addition, one should check the chart comparing ISPs available at:

[http://www.cdt.org/privacy/online\\_services/chart.html](http://www.cdt.org/privacy/online_services/chart.html). Most major providers are listed. Web sites also should offer privacy policies, and this practice is increasing. Josette Shiner reports that 94% of the top one hundred web sites now have such a policy, as do 65.7% of the 7,500 sites that currently receive the most hits, or visits by Web surfers (Shiner 1999). *Anonymous.com* is a new, free application launched in early October by Advisor. It rates the privacy policies of web sites using a scale of one to four stars ("How Anonymous Advisor Beta Works" 1999).

Another important facet of privacy is the password used to access one's ISP account. It should be made up of a combination of upper and lower-case letters and numbers, never a name, birthdate, or any other term related to personal information. It should be changed often and never written down or divulged to anyone else (Gelman).

Many consumers are rightfully cautious about using a credit card to buy something online. They are concerned about sniffers, software used by hackers to "sniff out" passwords, e-mail addresses, or credit information on the Internet (Peterson). Often a customer service number will be listed on the site so that a potential customer can submit an order by telephone. As an alternative, the customer can e-mail a request for a representative to call and take the order by telephone. (Massingill).

Bills, credit card records, and credit reports should be checked for incorrect information or unsubstantiated charges. Such errors may signal that one's credit card number or identity has been stolen (Massingill). Keep your credit history confidential and stop those unsolicited offers for credit cards by calling 888-567-8688. This is the automated credit opt-out number used by Trans Union, Equifax, and Experian, the three major credit bureaus (Massingill).

Product warranty cards are not really necessary to validate the guarantee on a product. Instead, they are sources of information for data warehousing. Don't return them, either online or by mail, if you want to safeguard your privacy (Massingill).

Because e-mail is never private, consumers should be wary of transmitting personal or confidential information in that manner. Traces of each message remain on the computer of the recipient and any machines it traveled through on its way there as well as on any backup system associated with the sender's computer (Peterson). Newsgroups, or bulletin boards are public places on the Internet where people can deposit or read messages about topics that interest them. Examples include USENET and Deja News. These postings are usually archived and searchable, sometimes for years. By doing a search on one's identity, companies can build personal profiles of users; these profiles can be made available to commercial enterprises or even prospective employers (Gelman). Thus, consumers should be extremely careful when posting messages on Internet bulletin boards or newsgroup sites. Also, they

should remember that the e-mail address of anyone who posts to a bulletin board or a LISTSERV, or electronic mailing list based on interest areas, is available to anyone (Peterson).

October 21, 1999, was termed "Jam Echelon Day" by angry Internet users upset by news that the United States National Security Agency is practicing "routine and indiscriminate" eavesdropping of e-mail messages in search of terrorist plots. The organizers urged others to spam the NSA in an attempt to crash its computer system. While few experts expected the spamming to have any real effect on the NSA's sophisticated system, supporters said they would at least be able to raise public awareness of online snooping (Bridis, "NSA Spammed," 1999).

Similar to bulletin boards, and even more popular with many Internet customers, are the chat rooms furnished by a Web site or an Internet Service Provider. These chat rooms operate in real time. A group of people communicate by typing messages to one another; everyone in the chat room can see everyone else's messages, and the communications can be captured, stored and sent to others not associated with the service. Advertisers often monitor chats so they can insert promotional messages prompted by comments made by the people in the "room." Subtlety of these advertising messages varies, with some not appearing to be ads at all. A San Francisco-based company called Black Sun Interactive Inc. is currently developing "ad robots" that will listen for key phrases in chat rooms and respond to the phrase with an advertisement for a related product. Chat room participants should be aware that their comments are not private at all and phrase them accordingly (Peterson).

Cookie files can be useful in personalizing information for a site, as in "My Yahoo," for example, or for making online sales and services more convenient. However, they can also give out personal information and be used to trace surfing habits without the surfer's knowledge. The web site *Cookie Central* warns of a cookie called "double-click.net," which can be placed on a client machine to collect data for sale to marketing firms. These and other cookie files can be found in "cookies.txt" or, on a Macintosh, "magic cookies," and deleted to ensure greater online privacy ("The Dark Side" 1999). As an alternative to deleting the files, cookies can be disabled. Instructions for disabling cookies are different with each browser, but information about doing so can be found in the help files or the user guide (Massingill). There is also specialized software that will warn users of cookies before they are placed on the hard drive. Examples include *Cookie Pal 1.0*, *InternetJunkbuster*, and *PGP cookie.cutter* (Peterson). Users should also be aware of Java and ActiveX applets, or miniature applications that run on the user's machine when he accesses a web site that uses them. These applications also pose security risks that have not been solved by their developers (Gelman).

Many web sites employ click-stream, or transaction-generated data collection techniques. This very detailed information collects information on web sites visited, time spent at a site, and topics of interest. It is statistical and of great interest to advertisers even though the data is not directly associated with individuals. Other sites ask visitors to register, revealing personal information in the process. When this occurs, the click-stream data does become associated with the visitor in particular and is extremely revealing of his habits and interests. Be careful when asked to register online. Look for a privacy statement before revealing personal information. Such a statement may be hard to find, although they are increasing because of popular demand. In the Electronic Privacy Information Center's 1997 survey of 100 Web sites, only 17 had privacy policies, and many of these were difficult to locate on the page. A good policy should tell the visitor what information is collected, why, and how it will be used. There should be an explanation of what can be done if improper disclosure of facts should occur (Peterson).

Because technology continues to advance, it is important for consumers to stay informed. This can be a time-consuming activity, but there are places to turn for updated information. There is a web site at <http://www.junkbusters.com> that is dedicated to fighting junk e-mail, telemarketing calls, and other practices that invade citizens' privacy. Known as *Junkbusters*, the site contains plenty of ideas for protecting privacy. Another website is *EcoFuture*, located at <http://www.ecofuture>, where one can find a list of ideas to stop junk mail. Professor David F. Linowes has a home page at [www.staff.uluc.edu/dinowes/home.htm](http://www.staff.uluc.edu/dinowes/home.htm) where he gives suggestions for maintaining privacy on the Internet and at work as well as protecting our medical records (Massingill).

## **New Technology**

New technology has made several privacy-protection tools available to the public. For example, encryption scrambles information so that it is unreadable to anyone who lacks the key to unscramble it. One common form, “public key cryptography,” uses prime numbers to generate two different decoding keys, one public (to encipher the message) and one private (for deciphering). Because the numbers used are very large, the code cannot be easily broken, even with the help of a computer. While a 129-digit number code was cracked, it took 600 people from 24 countries working together for eight months to accomplish the feat as an experiment known as RSA Inc.’s *Crypto-challenge* (Peterson). The security of the code has made it a concern for the government, which objects to the use of any code it cannot decipher. The FBI and other Federal agencies want the key to all encryption systems on the market, and they want a back door to any future systems that are developed. If Congress agrees to these terms, it will be a serious limitation on the privacy of all American citizens (Peterson).

Anonymous remailers are another aid to security, especially when the information to be communicated is potentially dangerous to the sender’s safety. For example, political dissidents, whistleblowers, or people with AIDS may need to protect their identities. They could send messages via an anonymous remailer to accomplish this end. These programs forward e-mail with all identifying information removed. A list of anonymous e-mailers is available at <http://www.cs.berkeley.edu/~raph/remailer-list.htm> (Gelman).

A new e-mail plug-in by Disappearing Inc. will soon make it possible for people to direct their messages to self-destruct by a certain date, disappearing from the hard drive of both sender and recipient. The plug-in will work with all the Internet mail systems that exist today (Weise 1999).

## **The Need for Protective Legislation**

Teena Massingill points out that “playing the role of privacy cop can be a time-consuming proposition” (Massingill). Mary Gardiner Jones, head of the Consumer Interest Research Institute and a longtime campaigner for greater protection of consumer privacy, agrees. She argues that people simply do not have the time or the expertise to be responsible for protecting their own privacy rights. Quoted by Sarah Baase in *A Gift of Fire*, she says, “You can’t expect an ordinary consumer who is very busy trying to earn a living to sit down and understand what [consent] means. They don’t understand the implications of what use of their data can mean to them” (Baase).

## **Legislation Privacy**

Concern for the privacy of personal information and business transactions is not a new issue. As early as 1973, The “Code of Fair Information Practices” was recommended by a government advisory committee on automated data systems. It contained the following provisions:

- The existence of no system should be kept secret.
- It should be possible for someone to learn what information is kept on a system and how this information will be used.
- It should be possible for a person to correct mistakes in his files.
- The organization that collects, keeps, uses or distributes data must be responsible for the reliability and the security of the facts in its files.

While the provisions of this code have been incorporated into the policies of several companies and into Federal and state laws, it needs to be updated today. In reference to the first point, for example, experts explain that there are so many databases today that, even though they are technically not secret, people simply don’t think to investigate all of them. We need a new guideline that requires firms keeping such databases to notify each person whose files are included, telling consumers what information about them is contained in those files (Baase).

## **Recent Legislation**

In 1998, Congress passed the "Children's Online Privacy Act." This bill requires Web sites to obtain the permission of parents before they collect any personal data from children younger than 13 years old. On October 20, 1999, a compromise ruling on how this law will be enforced by the Federal Trade Commission was approved 4-0 by commissioners. The ruling states that for the next two years, Internet companies may e-mail parents to ask their permission to gather facts about their children, but they may not share the information obtained with any other businesses without written or faxed permission from parents. The new ruling will go into effect in April of 2000. After then, the FTC will reexamine the policy in light of new developments in technology. While it is now a simple matter to pretend to be someone else (a parent, for example) in an e-mail message, emerging technology should improve the chances of checking on the senders' identities. If this happens, the FTC will consider a wider use of e-mail for seeking parental permission when sharing childrens' information (Bridis, "Ask My Parents," 1999).

This year, a new bill has been proposed that makes it a crime for any company to sell information about children under 16 without the *written* consent of their parents. The bill, known as HR 369, the "Children's Privacy Protection and Parental Empowerment Act," should dramatically reduce the spam (junk and advertising e-mail) targeted to minors over the Internet (Furger 1999).

The "Social Security On-line Privacy Protection Act" (H.R. 367) was introduced in January by Representative Franks of New Jersey to prohibit the disclosure of Social Security numbers and information without consent of the individual ("Social Security On-line Privacy Protection Act" 1999).

The "Inbox Privacy Act" of 1999, introduced in March by Senator Frank Murkowski of Arkansas, would force junk e-mailers to include and obey opt-out provisions in their messages and to identify themselves in all mailings. In addition, they would be forbidden to send unsolicited messages to any domain with an anti-spam policy, although customers of the domain would have the option to receive such mail if they chose. The Federal Trade Commission would have the authority to regulate such activity and investigate suspected violations ("Inbox Privacy Act").

The "Personal Data Privacy Act of 1999," H.R. 2624, introduced July 19 by Hinckey, Kleczka, and Miller, would limit the transfer, sale, or disclosure of information about people by government agencies without the consent of the people involved. Agencies would further be required to give an individual access to his personal data within five business days of his request and to furnish a yearly report to anyone whose date has been collected or maintained during that year ("Personal Data Privacy Act")

The "Internet Consumer Information Protection Act" (H.R.2882) was introduced into the House of Representatives by Representative Vento on September 15, 1999. In the bill, Congress finds that the increasing use of Internet technology in business has made the privacy and proper use of personal information a "public concern." Therefore, it has become necessary to regulate the use of information that is available on the Internet without creating obstacles to business. The act would require ISPs to keep personal information secure. No data could be disclosed to a third party without (a) informing the client (b) giving the client the opportunity to stop such disclosure and (c) clearly explaining the method to be used to stop such disclosure. Each client must have the right to view and correct his personal information free of charge ("Internet Consumer Information Protection Act" 1999).

Representative Bruce Vento of Minnesota has introduced the "Consumer Internet Privacy Protection Act" (HR 313), to regulate how Internet Service Providers can distribute personal information about their customers. If the bill becomes law, ISPs will have to get written permission before supplying a client's data to an outside source and will also have to reveal whatever information is shared and to whom (Furger). The client will have the right to check the accuracy of the information and to correct any errors. No fee may be charged ("Customer Internet Privacy Protection Act" 1999).

After President Clinton signed legislation on November 11, 1999, giving banks permission to share data with affiliated financial companies, a number of states began planning to enact stronger privacy safeguards. Al-

though the new legislation gives consumers the right to stop financial companies from sharing their personal information with outside firms such as telemarketers, the states are concerned because of exceptions that allow such sharing when the outside firm has certain agreements with the bank, thus becoming a sort of “insider” (“New Legislation Spurs States to Action on Privacy” 1999).

There is fierce debate about all this legislation. While people like Bonnie Erbe insist that government regulation is necessary to correct current abuses, others prefer to let the industry regulate itself (Erbe 1999). They believe Orwell’s Big Brother will appear, not as the cyber-snooper, but as the government bureaucrat who tells business what it can and can’t do. Rosette Shiner describes government efforts so far as “ambiguous, unfair, and – most importantly – unnecessary” (Shiner 1999). She argues that consumers need only take advantage of tools that are offered to protect themselves.

### **Privacy Window Narrows**

The data collection never stops. It begins when you log on to the World Wide Web to check the weather or buy a book. From morning to night the mundane details of life are being tracked, recorded, and analyzed. Web Bugs allow our every move to be noticed on the WWW.

Data giants like Doubleclick have created dossiers containing names, addresses, incomes, purchases and many other details. More than 200 million American adults are being tracked by these companies and then sell the data on demand. Profile specialists make models of what consumers are likely to buy or do.

Information allows marketers to try and bring the personal touch back to marketing. While there is a lot of good that comes from all of this data collection, there is opportunity for fraud as well. More than 500,000 people are victims of identity theft each year. A recent victim was Tiger Woods, one of the most recognizable names in America. Using Woods’ Social Security number, Anthony Taylor of Sacramento, California, received a driver’s license and credit cards in Woods’ name and was convicted of making \$17,000 in fraudulent purchases.

While Americans sleep, data warehouse, marketers, financial services companies, and insurers are constantly buying, sharing and parsing data about family income, spending habits, purchases, house value, children, etc.. Surveys have shown repeatedly that nine of ten people worry about privacy, with about seventy five percent very concerned. We shouldn’t say it won’t happen, we can safely assume there will be major abuses (O’Harrow).

### **Privacy at Work**

Employers are increasingly monitoring their workers, especially telecommuters. Bosses are watching where telecommuters go online, what they say in e-mail, even how often they type on their keyboards. Employee surveillance is reaching further as new technology makes monitoring workers easier. Employers can block Internet sites devoted to non-business activities, monitor where employees go online, read their e-mail, and count keystrokes to ensure that work is being done.


Remote monitoring is part of an over-all trend toward more surveillance of workers. Nearly eighty percent of large companies record and review employee communication, according to a survey this year by the American Management Association. This figure is twice the amount in 1997 (Armour).

### **Conclusion**

Problems with Internet security do exist. There are many ideas for solving them, ranging from individual watchfulness to government regulation, but no final conclusion seems imminent. The problem is more complicated because rapid advances in technology keep changing the conditions. Until things are clearer, consumers will be wise to practice caution when going online. Each Internet user should be aware of what personal information exists on the Internet and should take the necessary steps to make sure this information is correct. Everyone should also know how to stop the unauthorized sharing of personal information whenever that is possible. As we have seen, cer-



tain tools are available to the informed customer. Some of these tools can be categorized as technology, while others are simply good practices and reasonable caution.

However, the customer must also be aware that some issues are beyond an individual's ability to control. The extent of self regulation on the part of Internet businesses is still unclear, as is the nature of the government's role in setting policies. In these areas, it is the customer's responsibility to speak out to those with authority to make such decisions. Thus, private citizens can help develop the Internet that will be such a major force in our lives in the twenty-first century. 

## References

1. Armour, Stephanie, *USA Today*, July 20, 2001.
2. Baase, Sara, *A Gift of Fire*, New Jersey: Prentice-Hall, 1997.
3. Bridis, Ted, "Ask My Parents; FTC Says Online Companies Can Ask Parents for Info," Online. October 22, 1999. Available <http://www.abcnews.go.com/sections/tech/DailyNews/netprivacy991020.html>.
4. Bridis, Ted, "NSA Spammed," On-line. October 22, 1999. Available <http://www.abcnews.go.com/sections/tech/DailyNews/netspy991022.html>
5. "Customer Internet Privacy Protection Act of 1999," On-line. *Thomas*, October 18, 1999. Available <http://thomas.loc.gov/cgi-bin/query/D?C106:1./temp/~c106PvloHT>:
6. "The Dark Side," On-line. *Cookie Central*, October 10, 1999. Available <http://www.cookiecentral.com/dsm.htm>.
7. Davis, Michelle R. "S.C. Worst for Citizen's Privacy," *The State*, October 5, 1999, A1.
8. Erbe, Bonnie, "Government Needs to Give Business Incentive to Regulate," *Morning News*, August 15, 1999, B9.
9. Furger, Roberta, "Washington Tackles Internet Law," *PC World*, pp. 33-34, September 1999.
10. Garfinkel, Simson, "Snooping on Workers Goes PC," On-line. September 17, 1999. Available <http://www.wired.com/news/topframe/2250.html>.
11. Gelman, Robert B. with McCandlish, *Protecting Yourself Online; an Electronic Frontier Guide*, San Francisco: HarperEdge, c1998.
12. Guynn, Jessica, "Your Boss Can Monitor Your Every Move, Whether You Like It or Not," *The State*, September 26, 1999, G3.
13. "How Enoonymous Advisor Beta Works," On-line. October 23, 1999. Available <http://www.enonymous.com/howitworks.asp>.
14. "Inbox Privacy Act of 1999," On-line. *Thomas*, October 18, 1999. Available <http://thomas.loc.gov/cgi-bin/query/D?c106:8./temp/~c106PvloHT::> "Internet Consumer Information protection Act," On-line. *Thomas*, October 18, 1999. Available <http://thomas.loc.gov/cgi-bin/query/D?c106:3./temp/~c106PvloHT::>
15. "Kids for Sale," On-line. September 26, 1999. Available <http://www.media-awareness.ca/eng/issues/priv/topics/kid4sale.htm>.
16. Massingill, Teena, "Taking Responsibility for Your Privacy Is First Line of Defense," *The State*, September 26, 1999, G3.
17. McCullagh, Declan, "Bug Finder Exposes MS Again," On-line. *Wired News*, October 11, 1999. Available <http://www.wired.com/news/news/technology/story/22183.html>.
18. "New Legislation Spurs States to Action on Privacy," *Morning News*, November 7, 1999, D4.
19. O'Harrow, Robert, *The Washington Post*, May 21, 2001, 1D.
20. Perkins, Joseph, "Feel Like You're Being Watched?" *Morning News*, September 15, 1999, 7C.
21. "Personal Data Privacy Act of 1999," On-line. *Thomas*, October 18, 1999. Available <http://thomas.loc.gov/cgi-bin/query/D?c106:9./temp/~c106PvloHT::>
22. Persson, Christian, "Pentium III Serial Number Is Soft Switchable After All," On-line. September 20, 1999. Available <http://www.heise.de/ct/english/99/05/news1/>.
23. Peterson, Chris, *I Love the Internet, but I Want My Privacy, Too!* Rocklin, California: Prima Publishing, 1998.
24. Rotenberg, Marc, "Privacy Groups Consolodate Intel Case at FTC," On-line. September 20, 1999. Available <http://www.junkbusters.com/ht/en/nr16.html>.

25. Shiner, Rosette, "Regulations Are Ambiguous and Might Stunt Web's Growth," *Morning News*, August 15, 1999, B9.
26. Shiver, Jube, "Employers Increase Computer Monitoring," *The State*, October 12, 1999, A5.
27. "Social Security On-line Privacy Protection Act of 1999," On-line. *Thomas*, October 18, 1999. Available <http://thomas.loc.gov/cgi-bin/query/D?c106:5:./temp/~c106PvloHT>.
28. "Theft," On-line. September 17, 1999. Available <http://www.ftc.gov/bcp/online/edcams/identity/index.html>
29. Weise, Elizabeth, "Self-Destruct E-mail Offers Virtual Privacy," On-line. *USA Today*, October 23, 1999. Available <http://www.usatoday.com/life/cyber/tech/review/crg441.htm>.