

Cookies and Privacy

Amir M. Hormozi, Ph.D., CFPIM

This article provides an overview of cookies, the small files used by companies to collect information about Internet users. Although cookies were initially designed to assist users in shopping online, they have become a synonym for the invasion of privacy. The article discusses the structure of cookies, the advantages and disadvantages of cookies, legal issues, and United States and European Union (EU) laws regarding the use of cookies.

COOKIES

A cookie is a small text file that is saved on a user's hard drive by a Web server. Cookies perform state management functions, which assist Web sites in maintaining information about the state of their users or what their users are doing. This function allows Web sites to remember information about users as well as their preferences. Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored on name-value pairs. Table 1 describes the cookie's six parameters.

Cookies are often incorrectly defined as a *program* that a Web site places on the user's hard drive, which collects information that the Web site can access.¹ Cookies are not programs and they cannot be accessed at any time by Web sites to determine where the user has been. Incorrect definitions may have led some Internet users to the fearful

state in which they currently reside. When cookies were first developed, there were no intentions of using them as the type of spy mechanism they have the reputation of today. Cookies were developed only for the purpose of informing the Web site's server that a user had returned.² The server recognizes the user by accessing the information previously stored in the cookie file. This process of user tracking was originally intended to be in the interest of the user. Saved information about the user results in saved time and more personalized visits in the future for the user.

Lou Montulli, a software engineer, claims to have developed cookies in 1994 while working on the first version of Netscape. They were originally designed to assist users in online shopping, by saving information about the items selected by the user. Montulli defines a cookie as a "piece of data that is stored, then given by the server to the client, stored by the client, and returned to the server each time the client returns."³ Cookies were intended to be used as a "shopping cart" that would save information for the user, and that is still seen as a primary advantage of using cookies today. However, somewhere along the line, their purpose was misconstrued and users began to lose focus of their usefulness.

Cookie uses have since grown far beyond their original intention and have become a very controversial issue. Users believe that

AMIR M. HORMOZI, Ph.D., CFPIM, is a professor at the College of Business of Texas A&M University-Corpus Christi in Corpus Christi, Texas.

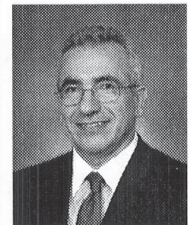


TABLE 1 Cookie Attributes

Attributes	Description
Name	Required The name of the cookie
Value	Required Contains information the server wants to save on the user's hard drive
Expiration date	Optional Date when the cookie expires If no date is specified, the cookie will expire when the session ends
Path	Optional Potentially the most useful of the four optional cookie settings Sets the URL path the cookie is valid within Pages outside that path cannot read or use the cookie
Domain	Optional A partial or complete domain name that indicates the cookie is valid Browser will return the cookie to any host that matches the partial domain name If no domain is specified, the cookie will be returned only to the Web server who created it
Secure	Optional Indicates if the cookie is secure A flag indicating that a cookie should only be used under a secure server condition

Source: See References 6, 19, and 20.

their privacy is being violated, with the progression of cookie functions moving beyond basic user customization and personalization. Cookies are stored in the user's computer without his consent or knowledge. This was not a concern in the past when they were used for remembering which user wants which item; but now they are being used by marketers to collect personal user information and by Web developers to track the visits and paths of users. The largest fear among users is the use of third-party cookies and the possibility of cookies being compiled by various Web sites into large user profile databases.

Advantages

Cookies provide a variety of advantages for users, Web developers, and marketers. It is very difficult to use the Internet today without cookies. Many Web site functions, including online ordering, site personalization, Web site tracking and user IDs, do not work when cookies are not enabled.³ Although they have a "big brother" reputation, they allow users to customize Web site features and save preferences for future visits. Web site content can be personalized

and shopping on E-commerce Web sites is made easier when cookies are enabled.

The original function of cookies — the "shopping cart" feature — has become very useful, both for companies that sell their products on Web sites and for the consumers purchasing those products. Cookies allow users to save numerous items, as well as quantities, colors, and sizes in their shopping cart until they are ready for check-out. Often, thousands of users will shop concurrently on the same Web site. A user's Web browser can keep track of the items the user wants to purchase, as well as other information for billing and shipping purposes, more efficiently than the Web site's Web server.⁴ When users shop on a Web site, they can add items they wish to purchase or view later in their shopping cart, while the cookies keep track of items selected and added to the cart.⁵

Cookies can also be used to store information about user interests. For example, if a user shops online for books, the bookstore can save information about which books are viewed and purchased. This enables the bookstore to provide suggestions for other books that might be of interest to a specific user. Advertisers and marketers also use the

interests determined through cookie usage to select which advertisements will be most effective for a particular user. Cookies can save users' geographic locations, which allows Web sites to personalize information about weather, movie theaters times, television listings, or local events. Cookies also allow for a Web site personalization. The users' names can appear when welcoming them back to the site, or the users may be able to choose what content they would like to see (or not see) on the site. Cookies save users' time by remembering their information. Future visits are less of a hassle when the Web site does not need to repeatedly ask users for any required information.

An alternative way for Web sites to accomplish this is to allow users to create unique IDs and passwords for themselves. This will keep each customer's information separate and private. For example, when purchasing products from an E-commerce Web site, users do not need to fill in their name, address, and billing information every time they buy from that particular site. Cookies allow the user to save the information with their ID and password so it is available when the user returns and is ready to make another purchase. The more information a user provides, the more cookies can assist the user in finding the information or products desired. The information is saved with back-end interactions, which allow the site to securely store important personal data such as passwords or credit card information on a user's hard drive.⁶

Marketers and advertisers use cookies for collecting demographic information about users. When one sees an advertisement for the first time from a particular server, the browser is assigned a unique ID that is saved with one's other cookie files. When visiting a Web site that contains an advertisement from that server, the cookie will be used to display the most effective advertisement based on one's interests that were determined by the information previously provided.⁷ Information can be collected in a variety of fashions, such as by the topics of the Web sites visited, the advertisements

clicked on, the items purchased, or any forms filled out. The user could provide the information directly by filling out forms, or passively by being tracked across several Web sites. Cookies are very beneficial for the advertisers that want to target the interests of consumers.

Similar to the way cookies are used to count and track the visitors to a Web site, they can also be used to determine the effectiveness of advertisements placed on the Web. Users benefit from these counts as well, because they prevent them from seeing advertisements too frequently. After clicking on an advertisement that collects information through cookies, users will be tracked on the Web site to which they are directed. Clicking on a particular advertisement will also help determine the interests of the user, which will lead to more personalized advertisements shown in the future.⁷ DoubleClick, the Internet advertising company, uses this technology by tracking which advertisements are seen by a user on the various Web sites DoubleClick's cookies are on, and then changing those advertisements periodically so they are not seen too frequently. This strategy also prevents consumers from seeing advertisements that are not suited to their interests.

Web developers use cookies for statistical purposes. They can track how many visitors arrive, how often a visitor returns, and how many are new visitors versus repeat visitors. This information can be used to plan future Web site updates, by keeping the data collected in a large database. Each user is assigned an ID when visiting a Web site for the first time. That ID is placed in the user's cookie files, on the user's hard drive. When the user returns to the Web site, the Web site will count that user as a return visitor. This is a continuous process that is used for each Web site visitor.¹ The cookies are also used to track the paths of users throughout the duration of their visit to the Web site. This is not done to spy on the users, but rather to provide information to Web site designers. By knowing where the users visit, designers can focus on those pages to

The more information a user provides, the more cookies can assist the user in finding the information or products desired.

Because there is rarely one user using a single computer, cookies may not be the most effective way to keep track of the number of users.

present the information in the most user-friendly way. Attention can also be given to the pages that have a low visitor count to determine any problems with the page content.⁵ Tracking visitors can also determine where the user left the Web site. A certain page may need investigation if numerous visitors exit the Web site on a particular page. There may be an ineffective link or an error that needs correcting. By tracking where users spend their time, Web site changes can be made to improve the user experience and increase the likelihood that they will return.

Disadvantages

Several problems have arisen when attempting to use cookies to track the number of users who visit a particular Web site. Visitor counts can often be inaccurate due to users who use more than one computer or frequently share computers. Users might access a Web site from their home computer, work computer, or their laptop; and each time that user changes computers, a different ID is assigned. This causes inaccurate counts when determining which visitors are new and which visitors are returning. In addition, the home computer could have various family members accessing different sites. When attempting to track user interest to provide the most effective advertisements, this would also cause inaccurate results.

Cookies can often get erased when temporary Internet files are deleted, which would also cause creation of a new ID.¹ A user can delete his cookie files at anytime so they cannot be relied on for saving important information.⁸ Because there is rarely one user using a single computer, cookies may not be the most effective way to keep track of the number of users. The best solution to this common problem is to have users create an ID and password to log in to the site, which can be used by only that one user from any number of computers. This will provide Web sites with the most accurate counts.¹

According to Drott,⁹ we do not know how beneficial cookies are to Internet users. We only know that tracking visits and customizing sites is most valuable for users that return to the site. Cookies may not be as useful for users who visit a site once or only visit periodically. The user ID process could possibly be ineffective or more time consuming for users who do not plan on returning to the site.

Users often perceive cookies as an invasion of privacy due to the information collection without their consent. Users may not know that a cookie is being placed on their hard drive, what it will be used for, or if any third parties have access to the information. In 2000 and 2001 studies, Drott⁹ examined the home pages of 60 Web sites of the companies listed in the 1999 issue of *Fortune Global 500*. These were the first 30 listed and the last 30 listed. More than one third of the corporate sites in the survey set cookies in connection with their home pages. This is why it is critical for Internet users that have cookies enabled to read privacy policies when visiting a Web site. If users do not read the Web site's privacy policy, they may not know why the cookie is being placed or how the Web site intends to use the collected information. Users generally do not know when a cookie that is stored on their hard drive is being accessed. The Web server does it all automatically. Essentially, cookies make use of user-specific information, transmitted by the Web server onto the user's computer for use of the specific information at a later time by itself or other servers.¹⁰

A third-party cookie either originates on or is sent to a Web site different from the one being viewed currently. Third-party cookies raise the most concern among users today. These cookies can originate on the Web site one is viewing, or can be sent from the Web site one is viewing to a different Web site. This is usually done for advertising purposes. The site one is viewing may not use cookies; but if there is an advertisement on the page from a third party that uses cookies, one could be tracked through the other Web site's cookies. Third-party cookies are

usually employed to observe user browsing habits and determine interests for advertising customization.¹¹

Cookies today are capable of performing more than was formerly intended. When Montulli came up with the cookie concept, he did not know third-party cookies were possible. Although they are seen as a threat by and to many Internet users, they are not a hazard when only one Web site is collecting information. They become potentially dangerous when many Web sites collectively track and gather information about users.³ Advertising network companies collectively compile the information collected by the cookies and share it with thousands of other Web sites.

DoubleClick is the most notable of all these companies. Anyone who has used the Internet with cookies enabled is likely to have a cookie file that was placed by DoubleClick although they probably do not know who DoubleClick is nor have they visited its Web site. There is no need for the user to visit DoubleClick's Web site because there are more than 11,000 Web sites that use DoubleClick cookies, which have provided the company with information on 100 million users.¹² There are various concerns about large databases that could potentially be created with all the user information collected by cookies. This could enable marketers to create detailed profiles about users such as what sites were visited, what was purchased or what advertisements were clicked on. This information could then be sold to third parties that can complete the profile with more personal information. Once a user provides an e-mail address, names, addresses, and other personal information can be found in other databases.

According to the World Wide Web Consortium (W3C), which promotes the evolution and interoperability of the Internet, DoubleClick does not include names or e-mail addresses or phone numbers in its databases, but often the other information cookies collect is enough to identify the user. DoubleClick only maintains that it uses information

about browsers and Web surfing habits to provide the advertisements that are best matched to the user's interests. Many users feel cookies that track their path across Web sites are invasive even if their identity is not known. Users should be especially concerned about this tracking behavior if they fill out forms that contain information that could identify them.

Users may have a right to be concerned about their privacy when cookies are being used. Cookies can easily be seen and information can be accessed by anyone who knows how to get to the cookie files stored on the hard disk of a computer. This is why private information such as credit card information, addresses, or phone numbers should not be stored in a cookie. Cookies should be used only for storing the ID of the user. Any other information provided may not be secure enough to protect the user's privacy.⁸ However, cookies still only contain personal information if the user has provided it. If users are concerned about privacy, personal information should not be provided to Web sites that use cookies. Reading the privacy policies of Web sites can help users determine whether or not they want to provide the Web site with their private information.

The privacy controversy continues to grow with the number of lawsuits against Internet companies that do not disclose their use of cookies. In a June 2002 survey by Jupiter Research, 70 percent of E-commerce users said they were worried about their privacy online. In another survey conducted by Jupiter Research, 93 percent of E-commerce users said it was very important that sites disclose their privacy practices. Goldman¹³ also believes that users attempting to protect their privacy are a small percentage of the Internet community. Many users who are concerned about their privacy do little or nothing to protect their privacy. Many do not even know how to configure a browser to stop cookies from being recorded, or read the privacy policies of the Web sites to learn what information cookies collect and how it is used.

Cookies should be used only for storing the ID of the user. Any other information provided may not be secure enough to protect the user's privacy.

User uproar concerning privacy complaints has increased with users distressed about cookies that have been placed on their hard drives.

LEGAL AND BUSINESS IMPLICATIONS

There have been several attempts to pass laws limiting the use of cookies but there are currently few legislative measures that protect Internet users. Privacy is not a constitutional right in the United States, which makes it difficult to get new privacy legislation enacted when new technological problems arise. Privacy issues only appear in the courtroom when a problem occurs and citizens need additional protection that current laws do not provide. Because of lacking government protection, Internet users must protect themselves when using the Internet with cookies enabled.

The Federal Trade Commission (FTC) approved of self-regulation with a unanimous vote in 2000. This plan requires companies to inform users of their activities involving any customer profiling that gives users an opportunity to choose whether they allow their information to be collected.¹⁵ Although it is up to the users to decide what information they want to provide to Web sites or whether they want to use cookies, the FTC is still taking action against companies that do not abide by their own privacy policies. The majority of Web sites currently provide users with information about what information is collected and its intended use. However, the FTC continuously observes companies to ensure they are not violating their own privacy policies. Section 5 of the FTC Act permits the FTC to enforce any statements made in a company's privacy policy.

Cookies can be used to collect information about adult Internet users without any repercussions, as long as the Web site is obeying its own stated privacy policy. However, the privacy issue becomes much more serious when the Internet user is a child. Cookies cannot be used to collect any identifiable information about children unless a parent has given consent. This is stated in Section 312 of the Children's Online Privacy Protection Act, which applies to children under the age of 13. Therefore, cookies cannot be used to collect names, addresses, phone numbers, or any other identifiable

information, as well as any creation of user IDs that numerous Web sites currently assign for statistical and demographical purposes.

There have been several lawsuits resulting from the use of cookies. User uproar concerning privacy complaints has increased with users distressed about cookies that have been placed on their hard drives. The majority of these lawsuits have focused on companies that failed to disclose to users their use of cookies or used information in ways that were not disclosed in their privacy policies. While companies that use cookies are not required to do more than inform users of their cookie use, they are required to abide by the policies they set for themselves. Many companies believe their privacy responsibility ends when they disclose the use of cookies in their privacy policy. However, unless the company abides by its own privacy policy and protects the information collected about its users, legal action will be imminent.¹⁶ Previous lawsuit attempts were to prohibit companies from using cookies to track the user's paths across Web sites to protect user information from being used to develop detailed profiles.

The FTC and several State Attorneys General have brought lawsuits against several companies for their use of cookies. Esurance,¹⁷ an auto insurance company, was accused of not disclosing the use of third-party cookies by advertisers on its Web sites. The cookies were reportedly used to collect information about users and then compiled into a customer profile database. Esurance now informs users in its privacy policy about the cookies placed by third parties and how they are used.

Avenue A, Inc., a marketing agency, was accused of utilizing cookies to track users' Web habits and compile information about its users.¹⁷ Avenue A, Inc., now part of aQuantive, Inc., uses Atlas DMT, another part of aQuantive, to set its cookies. Atlas DMT has a very detailed privacy policy that informs users of Avenue A's use of cookies and mentions their Network Advertising

Initiative (NAI) membership as well as their compliance with the W3C's Platform for Privacy Preferences Project (P3P) specifications. Users are also given an opportunity to replace the current cookie on their hard drive with an opt-out cookie to avoid any future cookie collection practices. There have also been similar lawsuits against Toys "R" Us and Yahoo! for using cookies without user consent.¹⁷

SOLUTION TO PRIVACY ISSUES

DoubleClick has been sued numerous times for violations of privacy relating to the company's cookie tracking practices. Its information collection practices first caught the attention of the Electronic Privacy Information Center (EPIC), which filed a complaint with the FTC in February 2000. The FTC closed its investigation of the company after determining that DoubleClick had disclosed its practices in its privacy policy and never used or disclosed users' information for any purposes that were not stated in its privacy policy. DoubleClick made an agreement with the FTC under the provisions of the NAI to update its privacy policy, inform users of their "opt-out" option, and explain to users how the company tracks users and intends to use the collected information. The NAI has developed a set of privacy principles with the FTC that requires all Web sites to disclose any information collection practices in their privacy policies. DoubleClick has changed its privacy policy since the lawsuit, and now explains to users how they can choose to opt out. When a user decides to opt out of DoubleClick's cookie collection practices, the user's original cookie will be replaced with this cookie:

id=OPT_OUT

The opt-out cookie replaces the unique ID number that previously identified the user. By placing this cookie on the user's hard drive, DoubleClick's server will know that the user has opted out and will not attempt to assign other cookies in the future.¹⁸ The NAI Web site also gives users the option to opt out of advertising. Its Web sites inform

users how to opt out of all cookies placed by any of the NAI's advertising networks.

Users also have another option to protect their privacy and prevent cookies from collecting personal information. With the public uproar of privacy issues that comes along with the use of cookies, software suppliers have taken advantage of the opportunity. Available software such as Junkbusters, Cookie Cutter, and Cookie Monster give Internet users an opportunity to control the cookies that are placed on their hard drives.⁸

The World Wide Web Consortium's P3P gives users another opportunity to determine whether they want certain cookies to be placed on their hard drives. They have developed a standardized privacy policy that will answer all questions a user might have concerning a company's use of cookies. The company answers several multiple-choice questions about what information will be collected and how it will be used. The privacy policy is then drafted in a manner that will be consistent with all other P3P privacy policies, which will make reading privacy policies easier for Internet users.

Businesses that wish to provide users with the most security and ease of use while visiting their sites can obtain privacy seals from several Web sites. Users who are worried that their privacy may be violated when using cookies on the Internet can look for the following seals. The 3rd Party Privacy Seal assures users that the site's privacy policies are being followed. Users who feel privacy policies have been violated are able to contact several businesses that protect Internet privacy. The Better Business Bureau (BBB) is protecting the interest of user privacy through the BBB Online's privacy seal. This seal posted on a Web site guarantees that a company will follow its privacy policies and has met all privacy standards required by the BBB. A TRUSTEe seal on a Web site similarly informs users that all information collection practices are disclosed in that company's privacy statement. Both BBB Online and TRUSTEe can be contacted if a user feels a Web site is not abiding by its privacy policy.

Available software such as Junkbusters, Cookie Cutter, and Cookie Monster give Internet users an opportunity to control the cookies that are placed on their hard drives.

Cookies perform state management functions and have multiple advantages and disadvantages.

Companies that do not want to risk losing any customers can choose to avoid using cookies on their Web sites. Although cookies were originally intended to assist users in their Internet experience, many users today still see them as a threat. Any company that does not want to lose up to 10 percent of its customers may decide it is better to not use cookies and allow users to feel more secure.⁸

USING COOKIES INTERNATIONALLY

While the United States relies on a few laws, but mostly on self-regulation of privacy, the European Union has taken a different approach. Businesses need to be aware of international privacy laws, especially the European Union Data Protection Directive, when dealing with Internet users in other countries. While the United States does not provide protection of privacy in the Constitution, the European Union does. When collecting information in the United States, users must choose to opt out of practices if they do not want their information shared with third parties. However, the European Union's Directive protects users from similar information collection practices. To collect data about European users, individuals must choose to opt in.¹⁴ With Internet users spread out across the world, U.S. companies must be cautious when using cookies. Information about a European user cannot be collected in the same manner as an American user. Businesses that do not abide by European privacy laws could be prosecuted.

CONCLUSION

Since the creation of cookies, Internet users have become increasingly concerned with privacy issues. Some consider cookies a program to determine where a user has been; but in fact, cookies are small text files that are saved onto a computer hard drive by a Web server. Cookies perform state management functions and have multiple advantages and disadvantages. Cookies perform Web site personalization, facilitate online shopping, and help advertisers determine

which advertisements may be of interest to each particular user. Cookies also perform statistical functions such as counting the number of Web site visitors and also providing information to Web site designers. In turn, designers can focus on presenting a Web site in the user-friendliest way and troubleshoot any problems with the page content.

Cookies also have disadvantages, such as inaccurate visitor counts. Users often use more than one computer, share computers, or access the same Web site from a work computer. Each time a user changes computers or deletes temporary Internet files, a different ID is assigned. In addition, cookies have created issues regarding user privacy. Cookies are used to collect information without a user's consent and this is especially troublesome with third-party cookies. Privacy issues continue to increase, as evidenced by the number of lawsuits against Internet companies that do not disclose their use of cookies.

The United States primarily has self-regulation in regard to companies' use of cookies; however, the FTC does take measures against companies that do not abide by their own privacy policies. In contrast, the European Union has more rigid laws regarding the use of cookies and does not allow the collection of personal information of their users. Another difference between the United States and the European Union regarding privacy policies is that a U.S. user must read the Web site's privacy policy and select to "opt-out" of receiving cookies from certain Web sites. In turn, EU users must "opt-in" to receive a cookie and thus allow a company to collect information about them.

Cookies are now used for many more purposes than they were originally designed for and therefore are often perceived as threats to user privacy. With more lawsuits and controversy about privacy issues, the United States may pass laws to restrain or stop the use of cookies and deny a company's ability to freely collect user information without their consent. ■

Acknowledgments

The author wishes to thank Ms. Teresa Coble and Ms. Kelly Harrison, research assistants, for their valuable contribution in gathering information.

References

1. Brain, M. (2003), "How Internet Cookies Work," How Stuff Works. Retrieved June 30, 2003, from <http://computer.howstuffworks.com/cookie.htm>
2. Microsoft Profile Center (2002), "Cookies: What They Are, Why You Are In Charge," May 19. Retrieved June 30, 2003, from <http://www.microsoft.com/info/cookies.htm>
3. Gyorgy, P. (2002), "The Tale of Cookies (Dr. Jekyll and Mr. Hyde)," *Social Research*, 69(1), Spring, 239.
3. Privacy Foundation (2001), "Cookie Maker," Resources, April 16. Retrieved July 8, 2003, from <http://www.privacyfoundation.org/resources/montulli.asp>
4. Netscape (2001), "Cookies: What They Are and How They Work," June 14. Retrieved June 30, 2003, from <http://help.netscape.com/kb/consumer/19970226-2.html>
5. Cunningham, P.J. (2002), "Are Cookies Hazardous to Your Privacy?," *Information Management Journal*, 36(3), May/June, 52.
6. Whalen, D. (2002), "The Unofficial Cookie FAQ Version 2.6," Cookie Central, June 8. Retrieved June 19, 2003, from <http://www.cookiecentral.com/faq/>
7. Interactive Advertising Bureau Resources & Research (2003), "Privacy-Educational Information." Retrieved July 3, 2003, from http://www.iab.net/resources/privacy_edu_info.asp
8. Williams, A. (2002), "A Cookie by Any Other Name — Is It Safe to Use Cookies Again?," *New Architect*, April 1, 16.
9. Drott, C.M. (2002), "Indexing Aids at Corporate Web Sites: The Use of Robots.txt and META Tags," *Information Processing & Management*, 38(2), March, 209.
10. Mayer-Schönberger, V. (1998), "Internet Privacy: The Internet and Privacy Legislation: Cookies for a Treat?," *Computer Law & Security Report*, 14(3), May 6, 166.
11. Microsoft TechNet (2003), "Understanding Cookies." Retrieved June 24, 2003, from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxpro/proddocs/sec_cook.asp
12. *The Economist* (2003), 336(8308), January 25, 5.
13. Goldman, E. (2002), "The Privacy Hoax," *Forbes*, 170(8), October 14, 42.
14. Jennings, A. (2003), "The European Union Data Directive: What Does It Really Mean for Your Business?" Retrieved July 10, 2003, from <http://www.truste.org/partners/newsletter/fall98.html#2>
15. Azmi, I.M. (2002), "E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill," *International Review of Law, Computers & Technology*, 16(3), 317.
16. Fitzgerald, K. (2001), "Push to Protect Privacy Grows," *Crain's Chicago Business*, 24(35), August 27, SR10.
17. Collier, S.S. (2002), "Privacy Law in Q1 2002: 6. Cookies and Web Bugs," FindLaw Professionals. Retrieved July 3, 2002, from <http://profs.lp.findlaw.com/privacy/index.html>
18. DoubleClick (2002), "Privacy," June 17. Retrieved July 3, 2003, from http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=&
19. Stein, L.D. (1998), "CGI: Cookie-Interface to Netscape Cookie." Retrieved September 15, 2004, from <http://www.seas.gwu.edu/~seascf/www/CGI.pm/CGI::Cookie.3.html>
20. W3 schools (2002), "The Cookie Collection." Retrieved September 15, 2004, from http://www.w3schools.com/asp/coll_cookies.asp

Additional References

- U.S. Department of Commerce (2003), "Introduction to the Safe Harbor." Retrieved July 17, 2003, from <http://www.export.gov/safeharbor/>