

Cookies and Internet Issues

Why talk about cookies?

For many individuals getting on-line brings with it a lot of insecurity and often that anxiety is compounded by all the new terms that accompany the virtual environment. The first time my browser alerted me that someone wanted to put a cookie on my computer, I froze. I had never heard of cookies before, and I had no idea what they would do. In a fit of paranoia, I refused the cookie and took my surfing elsewhere on the web. Eventually, cookies became so widespread, that I finally started accepting them and even turned off the notification in my browser preferences. Despite their diffusion across the web, I still had no clue as to what they were or did. Compounding this apprehension, are recent news reports about questionable usage of cookies and even the filing of a lawsuit. This paper answers those questions and also explores some of the concerns about cookies.

What is a cookie and would can it do?

The definition is not hard to locate on the Internet if you know how to search for it. I used the Northern Light search engine to locate it. Initially, I used their power search. Limiting my search to educational sites, learning materials, Q&A, and newspapers, wires & transcripts returned 3,333 hits in the subjects of computing & Internet, products & services, reference and technology. To further limit the results, I selected the digital signature folder and security sub-folder, and that yielded 14 hits. From those 14, I found four useful sites which in turn led to other useful sites. All of the sites I visited provided a similar definition of a cookie. It is a small amount of

information stored in your browser when you first visit a Web site. Your browser then returns that information to the site each time you revisit it and from that point on, whenever you visit that site it can, in essence, recognize you.

The Netscape Corporation first introduced cookies in an attempt to deal with the “stateless nature” of the web (The World Wide Web Security FAQ, Question 64). Without cookies, each time you move to a new URL, even just another page within a site, the server would treat the request for that page as a completely new interaction no matter how many other pages you have visited on their site. Cookies are how a web site “remembers” where you are and where you have been. For example, if we were to go e-shopping at a site and added several things to our “shopping cart,” it is the cookie that site has placed on your browser that identifies which of the shopping carts in their database belongs to you.

The cookie itself contains no personal information and is merely a tag that your browser sends back to the Web site when you revisit. Whatever information you have previously given that site is now accessible to them again. As an example, let’s say you gave them your birth date. The birth date itself is not stored in the cookie, but rather in a database on the server. The cookie on your browser tells the server where to find that information in the database. You might consider a cookie as your ID number to that Web site. So, the cookie really only points to whatever information you have provided to the site in the past. If you do not provide any personal information to the site, then a cookie can not reveal anything personal about you.

Many networks compile demographic information through the use of cookies to target banners of interest to the browsers that visit them. I say “browsers” because cookies do not transmit personal information. However, if you give personal information to a Web site, they can later access that with the aid of the information returned to them by a cookie. Most sites use cookies only for the convenience of their on-line visitors, however, the potential for abuse is certainly present.

Why worry about cookies?

What is the biggest concern about cookies then? On Nov. 8th, 1999, at a Public Workshop on On-line Profiling sponsored by the US Department of Commerce and Federal Trade Commission, Peter Swire, US Chief Counselor for Privacy, Office of Management and Budget quoted a Wall Street Journal-NBC poll. Earlier in the fall, it asked “What do you fear most in the coming century?” Response included overpopulation, terrorism, global warming. Out a litany of a dozen terrifying thing, the number one item, ranked either first or second by 29% of respondents, was the loss of personal privacy. None of the other responses came in higher than 23%.

The panel discussion included representatives from the advertising networks Engage and MatchLogic, consumer advocate groups, including Electronic Frontier Foundation and Junkbusters, and specialists on Internet Security. The industry representatives explained that cookies assist in counting unique visits to sites, profiling visitors for targeted banner advertising, and easing navigation. Both explained the steps their companies take to insure the anonymity of the data they collect. For instance, they do not collect personal data, and the cyberdata center is structured to avoid collecting combinations of data that could triangulate personal identities, for example zip code and date of birth.

In late January of 2000, a California woman, filed a lawsuit against the DoubleClick Network who she alleges is unlawfully collecting personal information without the consent of the user (Junnarkar). DoubleClick’s acquisition of Abacus Direct, a company heavily involved in advertising via direct mailing, has raised a lot

of concerns among privacy advocates. “On November 23, 1999, DoubleClick Inc. completed its merger with Abacus Direct Corporation. Abacus, now a division of DoubleClick, will continue to operate Abacus Direct, the direct mail element of the Abacus Alliance. In addition, Abacus has begun building Abacus On-line, the Internet element of the Abacus Alliance.” (DoubleClick Inc.). In this same policy statement, DoubleClick admits they will be compiling personal information, including names, addresses, purchase histories as well as demographic information. Although their policy statement explicitly says this information will not be sold to anyone else, it is not hard to imagine them using that information to exploit it through the direct mailing division of Abacus.

On February 21, 2000, the FTC announced an investigation into alleged privacy abuses by DoubleClick, Inc. Perhaps in response to this investigation, DoubleClick CEO Kevin O'Connor announced a moratorium on tracking by name on March 2, 2000. “We commit today, that until there is agreement between government and industry on privacy standards, we will not link personally identifiable information to anonymous user activity across Web sites.”

What should I do about them?

As with most topics dealing with the Internet, the lack of a governing body and the reliance upon self regulation come up frequently in the discussion of cookies and on-line privacy. There are remedies to cookie intrusion, but nearly all of them require the computer user know what is going on. Many users aren't even aware that they are collecting cookies. Most browsers allow for a refusal of cookies, and recent ones allow the placement of cookies only from sites you actually visit. The

latter feature is protection against “network” cookies like those used by DoubleClick. There is also free software available from Junkbusters to block cookies and banners.

The surest way to rid yourself of cookies is just to delete them from your computer. The World Wide Web Security FAQ page, question 64, explains how to find cookies on Windows, Macintosh and Unix systems and gives (<http://seclab.anseo.dankook.ac.kr/papers/www-security-faq.html#contents>). Once you have located the cookie file (sometimes called MagicCookie also) the easiest way to get rid of them is to delete that file.

References

Cookie Central:

<http://www.cookiecentral.com/>

DoubleClick Inc.:

http://www.doubleclick.net/privacy_policy/

DoubleClick Inc. Press Release:

http://www.doubleclick.net/company_info/press_kit/pr.00.03.02.htm

Federal Trade Commission, Transcript of Public Workshop on “On-line Profiling”
(PDF file):

<http://www.ftc.gov/bcp/profiling/>

Junkbusters, News and Opinion on Marketing and Privacy:

<http://www.junkbusters.com/ht/en/new.html>

Junnarkar, S. (2000). DoubleClick accused of unlawful consumer data use.

CNETNews.com, January 28, 2000.

<http://news.cnet.com/news/0-1005-200-1534533.html>

GTE Internetworking Internet Glossary: <http://www.bbn.com/support/glossary/>

Netscape DevEdge, Open Profiling Standard:

<http://developer.netscape.com/ops/opsfaq.html>

The Electronic Frontier Foundation, Top 12 ways to protect your privacy:

http://www.eff.org/pub/Privacy/eff_privacy_top_12.html

The World Wide Web Security FAQ, Question 64:

<http://seclab.anseo.dankook.ac.kr/papers/www-security-faq.html#contents>

US Department of Energy, Computer Incident Advisory Capability:

<http://www.ciac.org/ciac/bulletins/i-034.shtml>

Rodger, W. (2000a). DoubleClick backs off Web-tracking plan. USA Today.com,
Tech Report.

<http://www.usatoday.com/life/cyber/tech/cth486.htm>

Rodger, W. (2000b). DoubleClick target of FTC investigation. USA Today.com,
Tech Report. February 21, 2000

<http://www.usatoday.com/life/cyber/tech/cth374.htm>

*This paper is written by Scott Gibby for the course EDC385G Multimedia

Authoring at the University of Texas at Austin.