Cookies and Privacy Policies for Internet

Bau-Min Tu

Abstract

Cookies, the Web and new technology provide unprecedented opportunity for Web sites to collect detailed information about individuals. In this study, several topics including cookies fundamentals, the privacy of data about a person and privacy policy for Web sites will be discussed. Also, twenty-seven Web sites how they use cookies and their privacy policies will be compared. There are 37 percent used cookies to keep track of consumer behavior in the Internet but not announced. This result may be revealed less privacy for network users.

Keywords: Cookies, Privacy Policy, Internet

I. INTRODUCTION

DoubleClick, the leading Web advertising company plans to build a database of consumer profiles that will include each user's "name, address, retail, catalog and online purchase histories, and demographic data," according to the company's new privacy policy. The database, which the company says will only be seen by DoubleClick, is intended to help members of its budding, U.S.-based Abacus Alliance perfect their target marketing (Macavinta, 2000).

The move comes a little over a month after New York-based DoubleClick completed its $1.7billion acquisition of Abacus Direct and in the wake of the Federal Trade Commission's (FTC) November probe on the growing trend of online profiling. Privacy advocates, who protested the deal from the start, have unsuccessfully tried to get the FTC to review the implications of the merger because they say it means one thing for consumers: less privacy.

Until Jan 2000, DoubleClick's policy did not correlate personal information with its 100 million cookies, which are scattered worldwide. But the new database will rely on the cookies, which the company places on Internet users' computers to record surfing habits and display pertinent advertising. Internet users aren't informed when they are given DoubleClick cookies unless their browser is preset to do so, but they can "opt out" through the company's Web site.

The more than 11,500 sites that belong to DoubleClick's network could feed into the new database, which will correlate with the personal information in Abacus' existing database of more than 2 billion consumer catalog transactions.

There are many reasons a given site would wish to use cookies. These range from the ability to personalize information (like on My Yahoo or Kimo), or to help with on-line sales/services (like on Amazon Books or Microsoft), or simply for the purposes of tracking popular links or demographics (like DoubleClick). Cookies also provide programmers with a quick and convenient means of keeping site content fresh and

relevant to the user's interests. The newest servers use cookies to help with back-end interaction as well, which can improve the utility of a site by being able to securely store any personal data that the user has shared with a site.

II. COOKIE FUNDAMENTALS

Cookies are very useful tool in maintaining state variables on the Web. Since HTTP is a "stateless" (non-persistent) protocol, it is impossible to differentiate between visits to a Web site, unless the server can somehow "mark" a visitor. This is done by storing a piece of information in the visitor's browser. This is accomplished with cookies. Cookies can store database information, custom page settings, or just about anything that would make a site individual and customizable.

Cookies are a message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server.

The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When you enter a Web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into cookies and sent to your Web browser that stores it for later use. The next time you go to the same Web site, your browser will send cookies to the Web server. The server can use this information to present you with custom Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.

The name cookies derive from UNIX objects called magic cookies. These are tokens that are attached to a user or program and change depending on the areas entered by the user or program. Cookies are also sometimes called persistent cookies because they typically stay in the browser for long periods of time.

2.1 How do Cookies Work

Cookies are a standard mechanism that allows a Web site (or server) to deliver simple data to a client (or end user); request that the client store the information; and, in certain circumstances, return the information to the Web site. Cookies are a way of storing persistent client data so that a site can maintain information on a user accoss HTTP connections. (“Persistent” means that the information from the Web site lasts longer than the immediate connection.)

Cookies are small data structures delivered by a Web site to a Web client. The Web site may deliver one or more cookies to the client. The client stores cookies data on its local hard drive. In certain cases (determined by the data in the cookie itself), the client returns cookies to the server that originally delivered it.

Using a specially constructed URL, a Web site can read Intenet Explorer cookies set from any domain. For example, to read a user’s Amazon.com cookie, a site could direct the user’s browser to:

http://www.peacefire.org%2fsecurity%2fiecookies%2fshowcookie.html%3F.amazon.com

If you replace the “%2f” with “/” characters, and the “%3F” with “?”, this URL is actually:

http://www.peacefire.org/security/iecookies/showcookie.html?.amazon.com

But IE gets confused and thinks the page is located in the Amazon.com domain, so it allows the page to read the user’s Amazon.com cookies.

2.2 What Information can a Server Store

When a browser sends a request to a server, it includes its IP address, the type of browser you are using, and the operating system of your computer. This information is usually logged in the server’s log file. Cookies sent along with the request can add only that information, which is contained in the cookie and which, was originally sent to the browser by the same server. Thus, there is no additional personal information explicitly sent to the server by allowing cookies (CIAC, 1998; Whalen, 2000).

But cookies are used by Internet shopping sites (e.g. Amazon) to keep track of you and your shopping cart. When you first visit an Internet shopping site, you are sent cookies containing the name (ID number) of a shopping cart. Each time you select an item to purchase, that item is added to the shopping cart. When you are done with your shopping, the checkout page lists all the items in the shopping cart tied to those cookies. Without cookies, you would have to keep track of all the items you want to buy and type them into the checkout page or buy each item, one at a time.

Another method is for the shopping site to send separate cookies containing the item number to your browser whenever you select an item to purchase. Your browser sends all those cookies along with the request for the checkout page. The checkout page uses the cookies to make a list of the items you want to purchase.

Another use of cookies is to create customized home pages. Cookies are sent to your browser for each of the items you expect to see on your custom home page (e.g. yahoo, kimo). Whenever you request your custom home page your cookies are sent along with the request to tell the server which items to display without cookies, a server would require you to identify yourself each time you visit the custom page so it knows what items to display. The server would also have to store the custom page settings for every visitor.

The advertising firm sends cookies along with the advertisement, and that cookies are sent back to the advertising firm the next time you view any page containing one if its advertisements. If many Web sites support the same advertising firm (e.g. DoubleClick), that firm will be able to track your browsing habits from page to page within all the client sites. They will not be able to see what you do with the pages you view; they will only know which pages you are viewing, how often you view them, and the IP address of your computer. This information can be used to infer the things you are interested in and to target advertising to you based on those inferences.

2.3 Stoping Cookies in Explorer and Netscape

Internet Explorer no-longer stores cookies in a single file, but each cookies as a separate file in the windows\cookies directory, this makes it harder stop cookies, but if you want to stop individual cookies, like the doubleclick cookies, you can corrupt the cookie by deleting the contents then saving the file and setting its attributes read-only, hidden and system, this means when you log onto a site which has set that cookies it cannot read any information off your cookies or give you a new one. You also can set IE to alert you before accepting cookies, to do this go to the Tools\Internet\Options\ Security\Custom Level\Cookies and click on “Disable”.

In the netscape directory there should be a file called cookies.txt or magiccookie on the mac, search for this file if you cannot find it. This file is where all cookies entries are found, and you can delete the contents of this file regardless of the warning at the top of the page. After the contents have been deleted save the file and set its attributes to read-only, hidden and system. This will stop cookies from being set persistently on your hard disk, but it will not stop cookies from being set in memory while netscape is running, but when you exit netscape these cookies will be cleared. This is probably a good alternative to have netscape alert you when a site wants to set cookies, this becomes more of an annoyance than a prevention. You also can set netscape to stop cookies, to do this go to the Edit\Preferences\Advanced\Cookies and click on “Disable”. Another good way to stop cookies is to use some software (CNET, 2000).

III. PRIVACY OF DATA ABOUT A PERSON

Data about individuals is collected by numerous government agencies and private organizations. In the United States, there is no single statute or regulation that governs the collection, communication, and use of all types of information about individuals (Smedinghoff, 1996). To the extent that individuals have a right of privacy with respect to this information, it is usually provided by a limited statute that applies to a specific entity (such as the government) or to specific industries (such as the banking industry, credit-reporting industry, etc.). Thus, the legality of the online collection and communication of personal data must be evaluated in the context of any such limited law that may exist.

In Europe, privacy rights in information about individuals has received much broader protection than it has in the United States. Moreover, this protection applies not only to the collection, maintenance, and use of information about individuals, but also to the electronic communication of such information across national borders.

In October 1995, the Council of the European Union formally adopted a Directive on “the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.” This Directive, which member countries have three years to implement formally through appropriate legislation, seeks to protect individual privacy by prohibiting the improper collection, use, and communication of data relating to individuals. In doing so, the Directive seeks to protect certain fundamental rights of individuals, while at the same time ensuring the free flow of personal data within countries comprising the European Union.

Persons who collect and maintain personal data (data controllers) must abide by four key areas of responsibility: data quality, lawful processing, sensitive data, and notification. With respect to data quality, a data controller must ensure that personal data is processed fairly and lawfully; that it is collected and processed only for specified, explicitly legitimate purposes; that what is collected is not excessive in relation to the

purpose for which it was collected; that the data is accurate and kept up to date; and that it is kept no longer than necessary for the purpose for which it was collected.

The obligation to process data lawfully means the data may be processed only: 1) If the data subject has consented; 2) If it is necessary in relation to entering into performance of a contract; or 3) If it is necessary in the pursuit of the legitimate interest of the person controlling the data.

The processing of sensitive data is generally forbidden. Sensitive data includes that relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health information, or sexual-related information. There are, however, exceptions, including consent, vital interests, healthcare, and so on.

Finally, the data controller is obligated to provide the subject of the data with notice of: 1) The identity of the data controller; 2) The intended purposes of the processing; and 3) Any other information that may be necessary to ensure that the obtaining and processing is fair.

Individuals about whom data is collected have three fundamental rights. First, they have a right of access—that is, the right to know whether or not data about them is being processed, communication in an intelligible form of the data processed, and knowledge of the logic involved in the automatic processing of data relating to them. Second, they have a right to correct or erase incomplete, inaccurate, or unlawfully processed data; and a right to require the data controller to notify any third party to whom the data has been disclosed of any such correction. Finally, where a person has a compelling and legitimate ground, he or she may object to the processing of personal data. A data subject may also object to the processing of personal data for the purposes of direct marketing.

IV. COOKIES AND PRIVACY STATEMENT FOR WEB SITES

Many Web sites consider the responsible use of personal information to be a critical element in enabling the Internet to reach its potential as a serious tool for personal and professional activities.

In this study, twenty-seven Web sites were selected to examine how cookies they use. There are classified for three items including: 1) Portal site and search engine; 2) ISP and online news; 3) Online Store.

For portal site and search engine, eight Web sites were surveyed (see table 1). Five Web sites have privacy policy and announced that cookies have been used. But others have not privacy policy and not use cookies.

For ISP and online news, ten Web sites were surveyed (see table 2). In these Web sites, five have privacy policy and one not announced but used cookies (e.g. hinet.net as see table 2). The others have not privacy policy and four use cookies.

For online store, nine Web sites were surveyed (see table 3). Three Web sites have privacy policy and one use cookies. The others haven't privacy policy and five use cookies. In general, there are 37 percent used cookies but not announced from twenty-seven Web sites which we surveyed.

Table 1: Portal Site and Search Engine

Domain Name	Have Privacy Policy	Announce Cookies	Use Cookies
kimo.com.tw	✓	✓	✓
yahoo.com.tw	✓	✓	✓
yam.com.tw	✓	✓	✓
sina.com.tw	✓	✓	✓
pchome.com.tw	✓	✓	×
gais.cs.ccu.edu.tw	×	×	×
openfind.com.tw	×	×	×
dreamer.com.tw	×	×	×

Table 2: ISP and Online News

Domain Name	Have Privacy Policy	Announce Cookies	Use Cookies
hinet.net	✓	×	✓
seed.net.tw	✓	✓	✓
is.net.tw	×	×	×
gigigaga.com	×	×	✓
etwebs.com	×	×	✓
ettoday.com.tw	×	×	✓
taiwan.cnet.com	✓	✓	✓
udnnews.com	✓	✓	✓
chinatimes.com.tw	✓	✓	✓
digitimes.com.tw	×	×	✓

Table 3: Online Store

Domain Name	Have Privacy Policy	Announce Cookies	Use Cookies
acercm.com.tw	×	×	×
acertwp.com.tw	×	×	✓
compaq.com.tw	✓	✓	✓
hp.com	✓	✓	×
leomart.com	×	×	✓
synnex.com.tw	×	×	✓
taconet.com.tw	×	×	✓
tomorrow.com.tw	×	×	✓
tw.ibm.com	✓	✓	×

V. CONCLUSION

The sad truth is that revealing any kind of personal information opens the door for that information to be spread. The very nature of Web servers allows for the tracking of

your surfing habits alone, and other information about you can be gathered with time. While cookies themselves are not gathering that data, they are, unfortunately, used as a tracking device to help the people who are gathering that information. As information is gathered about you, it is associated with the value they keep in your cookies. The never-ending ethical debate associated with these facts shall be left to other forums. However, it is wise to consider carefully the information you collect and share over the Internet.

The right of privacy is a concept that is used in a variety of ways to mean a variety of different things. Moreover, some aspects of privacy are protected or regulated by law, whereas others are not. Thus, it is important to understand the different things that can be discussed in the name of “privacy,” and how they affect one’s right to use, or control the use of, online information.

REFERENCE

CIAC (1998). I-034: Intenet Cookies. Retrieved July 25, 2000 on the World Wide Web: http://www.ciac.org/ciac/bulletins/I-034.shtml.

CNET (2000).網上馳騁的威力影伴：Webroot software Window Washer 3.0. Retrieved August 10, 2000 on the World Wide Web: http://taiwan.cnet.com/computer/software/power/ss06.html.

Macavinta, C. (2000). Privacy Fears Raise by DoubleClick Database Plans. Retrieved August 14, 2000 on the World Wide Wed: http://news.cnet.com/news/0-1005-200-1531929.html?tag=st.ne.ni.rnbot.rn.ni.

Smedinghoff, T. J. (1996). Right of Privacy. In T. J. Smedinghoff (Eds.), Online Law: The SPAS Legal Guide to Doing Business on the Internet (pp. 267-281). Addison-Wesley.

Whalen, D. (2000). The Unofficial Cookie FAQ, version 2.53. Retrieved July 25, 2000 on the World Wide Wed: http://www.cookiecentral.com/faq.

網際網路之 Cookies 技術與隱私權政策之探討

涂保民

摘要

在網際網路的發展上有一項名為“cookies”的技術可用來收集網路使用者的個人資料。在本研究中將對 cookies 的基本定義、個人隱私資料保護及網站的隱私權政策等議題進行討論，同時也針對 27 個網站使用 cookies 的情形及其隱私權政策進行比較。結果顯示：有 37%的網站在未事先告知網路使用者的情形下，便擅自使用 cookies 技術來進行追蹤網路使用者行為，此結果顯示網路使用者在隱私權的保護上是非常不受到尊重的。

關鍵詞：Cookies，隱私權政策，網際網路