If you wanted to know...

What to do about Cookies

... Read on ...

The growth of the World Wide Web has been explosive. So have the opportunities for individuals to access information, and for websites to amass information about users. Personal information that is used or disclosed without the knowledge and consent of the user poses critical challenges to preserving one's privacy. Often, these digital tracks are laid invisibly and involuntarily by the consumer via an information-gathering software tool called a "cookie."

Many websites deposit cookies. These are small text files that are planted and stored on your computer's hard drive by a website when you first visit. Once planted, the cookie lies dormant until you visit that particular website again. When the follow-up visit occurs, the contents of the cookie are passed from your computer back to the web page's server — in this way, the website is able to identity and keep track of your computer as a repeat visitor.

Cookies are one example of tracks that are laid, but almost all movements across the web leave tidbits of an electronic trail as a result of a number of factors: maintaining an account with an Internet Service Provider or an on-line service; mouse clicks (especially on banner ads); posting messages to e-mail lists, Usenet newsgroups or other discussion lists.

Privacy is eroded when information about a user is collected, used or disclosed without the knowledge or consent of the user. Although cookie information may be largely benign, threats to privacy can escalate when cookie information is combined with other tidbits of information such as on-site registration details, filling out an on-line survey, or with data from the website's server log files (name of user's Internet Service Provider; the type of computer and software being used; the linking website; which files were accessed; and the amount of time spent on each page).

As a first step, we believe that on-line privacy begins with knowledge: users who are informed and aware of the potential of on-line privacy threats such as cookies are far better-equipped to assess various risks and to make their own choices about how much effort or control they want to exert towards guarding their privacy. At the end of this article, we provide a list of web resources that offer detailed information on cookies and other related issues.

Understanding how to control your cookie intake will reduce the electronic tracks you leave on the web. But like most issues related to privacy, users need to decide how far they are willing to go to protect themselves in exchange for services and information that they may need or want from content providers on the web. Ultimately though, the safest assumption that a user can make is that nothing on the web should be considered as being totally private.

INFORMATION AND PRIVACY COMMISSIONER/ONTARIO

November 1998

ANN CAVOUKIAN, Ph.D.
COMMISSIONER

Why are Cookies Used?

Cookies were developed as a way for simplifying and personalizing a website visit. But they have now evolved, amid much controversy, to also being used as a tracking tool for marketing purposes. Advertisers see cookies as a way to enhance personally targeted or "one-to-one marketing." Cookies make it possible for companies that are selling products over the web to track patterns of repeat customers and offer them special promotions.

Cookies are used in a variety of ways so that you (through your computer) carry with you some specific information that will be useful to the websites you re-visit. On the web, cookies are used for: website tracking (when, where, and how long you travel within a website), passwords, user identification, storing preferences of personal start pages within your browser, and online shopping/ordering.

Target marketing is one of the main uses of cookies. Cookies can be used to build up a profile of where you go and which banner advertisements you click on. This information is then used to target advertisements specifically at you. Actually, advertisers are not that interested in you, *per se*, only in what you may buy. What they do need is a unique way, such as a unique number or token — or cookie — to identify you so that your clicks and movements and preferences can be tracked in order to target messages and advertisements more precisely.

What is in a Cookie?

The basic ingredients in this recipe are: 1) the name of the cookie (chosen by the programmer at the website you are visiting); 2) the value of the cookie (the specific data that are being stored for future recognition and action by the web server); 3) the expiration date of the cookie; 4) the path the cookie is valid for (information about the path of the web page a user was on when the cookie was sent); 5) the domain the cookie is valid for (the domain name from the server that created and planted the cookie); 6) the need for a secure connection to exist to use the cookie (if the cookie is marked "secure," it will only be transmitted if the user is on a secure server).

What Can You Do?

As always, there is no one solution to guarantee on-line privacy, but generally, concerned users should always restrict the amount of information they volunteer on-line, even if it curbs the usability of a site.

With cookies, there are two basic ways in which you can reduce your electronic tracks. In practice these ways may vary somewhat, depending on your computer system and the browser you are using.

1. Activate Your Cookie Alert

Different versions of Netscape Navigator and Microsoft Internet Explorer provide different choices for controlling cookies. Netscape 3.x and Microsoft Internet Explorer 3.x both allow users to be warned that a cookie is on its way. If the "alert before accepting cookies" is enabled, the user can hit "OK" to accept or "CANCEL" to reject. This is done through the *Options/Network Preferences/Protocols* menu in Netscape or *Internet Options/Advanced* menu in Microsoft Internet Explorer.

Versions 4.x in both browsers give more options. For example, in Netscape Navigator, the cookie alert is activated by pulling down the *Edit* menu and then clicking on *Preferences*, then *Advanced Settings* at the bottom of the dialogue box. The choices shown are: accept all cookies; accept only cookies that get sent back to the originating server; disable cookies; warn me before accepting a cookie.

In Microsoft Internet Explorer 4.x, go to *View/Internet Options/Advanced* menu and the choices are: accept all, warn before accepting, or reject all.

2. Regularly Check Your Cookie File

In Netscape, from the start menu in Windows 95, Windows 98, and Windows NT, select *Find*, then *Files Or Folders*. Type cookies.txt in the *Named* box and then click on *Find Now*. Once the cookies.txt file is opened, look at each line. Here you will see the name of the website that placed the cookie, followed by what looks like gibberish. To get rid of the cookie, delete the entire line. To delete all information, delete all entries in the cookies.txt file. Next, select *Save* from the *File* menu and *Exit* to quit.

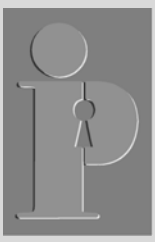
In Microsoft Explorer, cookies are kept in different locations, depending on the version you are using. For example, in Explorer 3.x, cookies are found in the folder *c:\windows\cookies*.

For Macintosh users, deleting cookie files is a little more involved and may be best approached by using a shareware utility. Various software solutions are available — many of which are discussed on the *Cookie Central* website.

Getting Information

As everyday social interactions dissolve from the physical to the digital, keeping informed and staying aware are perhaps the best ways to adapt. Here are some starting points for obtaining more information about guarding your privacy on-line:

- *Privacy statements:* Some websites display a "privacy statement" or "privacy policy" somewhere on the site, and cookies are often mentioned in these statements. Here are some examples: Microsoft's privacy policy is posted at http://home.microsoft.com/privacy.htm. Netscape's policy is at http://home.netscape.com/legal_notices/privacy.html.
- *Cookie Central* provides a vast array of information about cookies — including cookie blocking software, frequently asked questions, uses of cookies, and stopping cookies. It also includes a cookie demonstration: www.cookiecentral.com
- *Junkbusters* covers many topics related to privacy on the web — including cookies, banner ads, telemarketing, and unsolicited e-mail (spam): www.junkbusters.com/ht/en/index.html
- *Links2Go* has an extensive list of linked resources offering a variety of perspectives on cookies: www.links2go.com/topic/cookies
- *The Anonymizer* offers a service that shows users how to surf anonymously: www.anonymizer.com/.
- *The Centre for Democracy and Technology site* has a privacy demonstration page that alerts users to the kind of information that a website can collect about its visitors: www.13X.com/cgi-bin/cdt/snoop.pl



If you wanted to know…

is published by the **Office of the Information and Privacy Commissioner**.

If you have any comments regarding this publication, wish to advise of a change of address, or be added to the mailing list, please contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street West, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

30% recycled paper,