Globe and Mail
Jan 10, 2000

Is Big Brother on-line?



DIGITAL SURVIVOR

JIM CARROLL

As the Internet becomes a more important part of working life, have you considered who may be watching you?

There's lots of hype about the Internet's security risks, and people continue to have a number of concerns — mostly about the safety of using credit cards on-line. Yet there are more fundamental issues that you should be thinking about.

Among the most crucial of these is that it can be easy for people and companies to track what you are doing. You may not be doing anything illegal or improper, but even innocent on-line activities could lead to problems.

Let's say you've been checking out a medical Web site about a health condition that you experience. Surprise — everyone in the office knows now, because some snoop had a look at where you've been in your Web browser.

It's easy for anyone to do this while you are away from your desk. They simply have to look at the "history" within your browser. Want to know what they can see? In Netscape, look for a menu item called "history." You may find it underneath a menu item called "tools," or in Internet Explorer, simply click on the history icon. Double-click on any listed item you see, and you'll be taken to the Web page that's been visited.

You can quite easily delete the history file maintained by your browser program. If you do this regularly, you don't need to worry.

But are you sure that your company isn't tracking what you do? Many organizations have that capability. When they put in place a single, high-speed connection to the Internet, they often do it through a software program known as a firewall or proxy server.

One of the most popular features of such software is a tracking mechanism that can be used to build detailed lists of who has been where. Although many firms ignore such information, some may use it.

If you're satisfied that your company isn't following your activities on-line, are you sure you aren't being tracked by the Web site you're visiting?

Many sites maintain "log files" containing some rudimentary information about who visits them. While such details are often restricted merely to the company you represent, if you work for a small company the information could be quite specific — for example, your personal name as the firm's owner.

Then there are cookies, those small chunks of computer code that are deposited on your computer when you visit a site. A company may match up this information to other data you provide when registering (such as your name and address). Then it can prepare an extremely detailed profile of what you are looking at. And guess what — the firm could sell it to anyone who may want it.

Finally, the biggest privacy problem may not be that you've got all of these people and software programs watching what you do. You may be the issue. A huge number of Web sites ask people to provide all kinds of personal information when they are registering for a free service.

Ask yourself whether you really want to provide it. How can you possibly trust that the data you supply will be kept confidential, particularly in the absence of privacy legislation in Canada? Survey after survey shows that increasing numbers of people are providing false information when asked to fill out such a form.

The fact is, everyone should take the time to learn of the privacy risks involved with the Internet. To learn more, visit sites such as the Electronic Privacy Information Centre (**epic.org**), the Electronic Frontier Foundation (**www.eff.org**) and Electronic Frontier Canada (**www.efc.ca**). All of them contain extensive information about privacy issues that you can use to learn about your on-line rights.

◆ ◆ ◆

Jim Carroll is co-author of Light Bulbs to Yottabits: How to Profit by Understanding the Internet of the Future, *and can be reached by E-mail at jcarroll@jimcarroll.com*