WSJ .com THE WALL STREET JOURNAL. ONLINE

They know who you are

Why you should take steps to protect your identity on the Internet

December 16, 2005

The Internet is great. Most of us can go anywhere, do anything, read anything, see anything, say anything, download (more or less) anything; and all of this can be done apparently anonymously. As a famous 1993 New Yorker magazine cartoon had it, with one mutt at the computer keyboard explaining to another at his feet: "On the Internet, nobody knows you're a dog." Actually, much to the disappointment of canine surfers everywhere, this isn't exactly true. The Internet will quickly figure out that a) you order weekly supplies of Lick Your Chops (Adult Dog Maintenance Formula) from PetFoodDirect.com, and b) you regularly visit canine dating service AfterBark.com. Your dog status has been rumbled.

The truth is, you aren't as anonymous on the Internet as you thought you were. It is possible for companies, organizations, governments and individuals to collect extensive details of your identity, interests and activities merely by watching you surf. Just by linking your computer address (where your computer hooks up to the Internet) with the data you send and receive, and the footprints (or pawprints) you leave on the Web sites you visit, they can build up an extensive profile of you.

As Lance Cottrell, Internet anonymity advocate and creator of a program called Anonymizer, puts it: "There is generally a perception that activity on the Internet is anonymous with the possible exceptions of credit cards and identity theft." In fact, it isn't like that: "In reality," says Mr. Cottrell, "time spent on the Internet is probably the least private time one spends in any activity. Almost all sites are involved in detailed user and usage tracking. While most of this isn't for any nefarious purpose, the amount and detail of information gathered and stored is mind boggling."

This is because, over time, a detailed dossier is being gathered, explains Mr. Cottrell. "The issue isn't the single click and information related to that, but the accumulation of data over tens of thousands of hits and pages spread over years and hundreds of Web sites." This information is being gathered not just by the sites being visited but by other related businesses such as advertisers.

While many users install firewalls and run antivirus software to ensure we don't get fooled into giving away our personal details, Mr. Cottrell is talking about something different. Security isn't always the same thing as anonymity. Keeping your personal data secure is one thing -- it's akin to keeping your wallet, credit cards and ID card safely away from pickpockets. Anonymity is different. In the real world we can walk around without letting people know who we are -- we can browse in a shop without registering our name at the door. On the Internet we don't have quite the same choice: By default, we aren't only leaving our calling card in most places we visit, we're also telling each of them where we last came from, where we're going, our hometown, what we bought, and lots of other juicy tidbits. All of this, coupled with personal information we may have submitted to job-hunting sites, say, or medical newsgroups, gets stored away for years, exchanged, leaked, stolen, or sold.

You might not think you're leaving much of a trail that could be abused by Web watchers, but security experts disagree. "Who is to say the profile they build is really accurate?" says security consultant Matthew Tanase. "What if this information falls into the wrong hands? How secure is the information and what is the potential for abuse?"

So what can we do about it? Well, it depends on how much effort you want to put into it. For a start, your computer address. A lot can be told from this, especially if you use the same computer and the same Internet connection over a long period. Masking this address is the first step to Internet anonymity. This can be done by simply visiting a Web site that cloaks your address so the places you visit only see the Web site you're visiting from. It's a bit like going into a shop with a grocery store bag over your head. The shop can tell only that you've got some link to the grocery store. Apart from that, nothing. For examples of these Web sites, check out Anonymouse.org or Proxify.com.

But this doesn't help with the data itself. Disguising your address doesn't necessarily disguise what you do -- and the data that passes between you and the sites you visit. This is where Mr. Cottrell's Anonymizer comes into its own. Anonymizer (www.anonymizer.com) removes anything from the data your computer sends that may identify you -- or your computer -- to the Web site you visit. It also prevents that Web site from trying to reach your computer to get more information, or dump files on your computer that may help it remember who you are the next time you visit. Anonymizer encrypts the data you do transmit so that other people can't see it; it also warns you when you are visiting Web sites that may contain nasties trying to get into your computer. (A new version of Anonymizer's Anonymous Surfing package costs $30 for a one-year subscription.)

Another option is the USB key drive StealthSurfer II, which is great if you use other people's computers a lot. Plug in the StealthSurfer ($90 to $270 from www.stealthsurfer.biz) and use its onboard software -- including a browser, email program, password management program and a version of Anonymizer's software. All the data will be encrypted and none of it will be left on the computer you're using -- only your key drive.

Using the StealthSurfer might be too fiddly for some people. But if I've scared you enough about all this, it does offer you an all-in-one package that should give you some peace -- and keep your "dog-ness" a secret.

? Send comments to wire@jeremywagstaff.com.