COMPUTER GURU — *by Don Benjamin*
The Donald and Nancy Light Technology and Literacy Lab Programs
sponsored by: Penn Medicine Princeton Health

Internet Tracking

This is the first of three articles about internet tracking. Today, we'll explain how websites track the information you're requesting and how some share that information with other sites. Next month's edition will discuss ways to keep your web activities private. We'll end with an explanation of virtual private network services that make you an anonymous internet user.

If you've ever used Google to search for, say, "socks," you've likely been bombarded with sock ads for days afterward. That's because the Google folks track your searches (yikes!), which enables them to offer up ads for the things you're looking for. Of course, advertisers pay Google for this service, which is how the Google company can afford to redecorate its offices.

On the other hand, tracking lets Google personalize its search results, which should make your searches more productive. It's the price we pay for the "free" internet.

So, how does tracking work, and what are websites tracking?

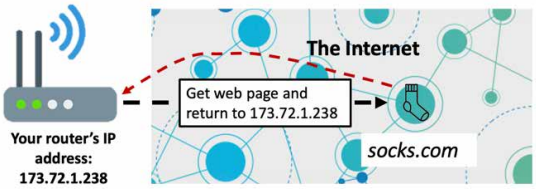
IP Address Tracking

Internet service providers (Xfinity, Verizon, etc.) assign each customer's router[1] a unique Internet Protocol (IP) address. You can reveal your IP address by searching for "my IP" on Google. It might be something like 173.72.1.238. No one else has that address. (There are no "party lines" on the internet.)

Returning to our search for socks, let's assume Google coughed up several websites that sell socks, including the rather banal *socks.com* that strikes your fancy. When you click the *socks.com* link, your browser sends along your IP address so *socks.com* knows where to send its reply. To be sure, *socks.com* doesn't know anything about you—it simply knows that someone at 173.72.1.238 has requested information about socks.

But Google, as well as your ISP, also knows someone at 173.72.1.238 is looking for socks and uses that information to place ads for socks on other websites you visit. Then, when you read articles on, say, *The New York Times* website, up pop ads for socks of all kinds. (When I visit the NYT website, I get ads for anti-gas tablets because, well, I have other issues.)

Some think these bespoke ads are annoying. They could even be embarrassing if you had been searching for some personal product that we won't mention here because this is a family-oriented newsletter.



Your browser attaches your IP address to your request to visit the website.

Cookies

In addition to tracking your IP address, *socks.com* might place a bit of information in your browser called a "cookie" containing information about the kind of socks you were looking for. If you added some nice, though banal, argyle socks to your *socks.com* shopping cart, the cookie includes that information, so when you revisit *socks.com*, you can pick up where you left off.

We call these "first-party" cookies because they're placed in your browser by the vendor you're dealing with. First-party cookies make internet searching and shopping easier and are usually harmless. However, not everyone wants these cookies. But read on…

Some websites are sneakier and provide your IP address and search interests to other websites, which, in turn, also place cookies in your browser. These are "third-party" cookies, which can be troublesome because they're more like interlopers. I've read that Amazon and Google are discontinuing third-party cookies, and that's probably a good thing.

Now What?

The next Guru article will explain how to adjust your browser settings to stop websites from tracking you. We'll also look at search engines and web browsers that emphasize privacy.

If you have questions for the technology lab, visit the PSRC website at **https://www.princetonsenior.org/technology-lab/**, fill out a request form, and we'll be in touch.

1 It's the little black box with a couple of lights that make it look cool.