How to Muddy Your Tracks on the Internet

By KATE MURPHY Published: May 2, 2012

Legal and technology researchers estimate that it would take about a month for Internet users to read the privacy policies of all the Web sites they visit in a year. So in the interest of time, here is the deal: There are no secrets online. That emotional e-mail you sent to your ex, the illness you searched for in a fit of hypochondria, those hours spent watching videos can all be gathered to create a defining profile of you.

Your information can then be stored, analyzed, indexed and sold as a commodity to data brokers who in turn might sell it to advertisers, employers, health insurers or credit rating agencies.

While it's probably impossible to cloak your online activities fully, you can take steps to help protect yourself. Some of these measures are quite easy and many are free. Of course, the more effort and money you expend, the more concealed you are. The trick is to find the right balance between cost, convenience and privacy.

Before you can thwart the snoopers, you have to know who they are. There are hackers hanging around Wi-Fi hot spots but security experts and privacy advocates said more worrisome were Internet service providers, search engine operators, e-mail suppliers and Web site administrators — particularly if a single entity acts in more than one capacity, like Google, Yahoo, Facebook and AOL. This means they can easily collect and cross-reference your data, that is, match your e-mails with your browsing history, as well as figure out your location and identify all the devices you use to connect to the Internet.

"The worst part is they sell this extremely creepy intrusion as a great boon to your life because they can tailor services to your needs," said Paul Ohm, an associate professor at the University of Colorado Law School in Boulder who specializes in information privacy and computer crime. "But do most people want to give that much away? No."

He advised logging off sites like Google and Facebook as soon as practicably possible and not using the same provider for multiple functions if you can help it. "If you search on Google, maybe you don't want to use Gmail for your e-mail," he said.

If you do not want the content of your e-mail messages examined or analyzed at all, you may want to consider lesser-known free services like HushMail, RiseUp and Zoho, which promote no-snooping policies. Or register your own domain with an associated e-mail address through services like Hover or BlueHost, which cost $55 to $85 a year. You get not

only the company's assurance of privacy but also an address unlike anyone else's, like me@myowndomain.com. Or you can forgo trusting others with your e-mail correspondence altogether and set up your own mail server. It is an option that is not just for the paranoid, according to Sam Harrelson, a self-described technology aficionado in Asheville, N.C., who switched to using his own mail server this year using a $49.99 OS X Server and $30 SpamSieve software to eliminate junk mail.

"The topic of privacy policies and what lies ahead for our digital footprints is especially fascinating and pertinent for me, since I work with 13- and 14-year-olds who are just beginning to dabble with services such as Gmail and all of Google's apps, as well as Facebook, Instagram, social gaming," he said. "I have nothing to hide, but I'm uncomfortable with what we give away."

But even with your own mail server, Google will still have the e-mails you exchange with friends or colleagues with Gmail accounts, said Peter Eckersley of the Electronic Frontier Foundation, a digital rights advocacy group in San Francisco. "You're less exposed," he said. "But you can't totally escape."

Another shrouding tactic is to use the search engine DuckDuckGo, which distinguishes itself with a "We do not track or bubble you!" policy. Bubbling is the filtering of search results based on your search history. (Bubbling also means you are less likely to see opposing points of view or be exposed to something fresh and new.)

Regardless of which search engine you use, security experts recommend that you turn on your browser's "private mode," usually found under Preferences, Tools or Settings. When this mode is activated, tracking cookies are deleted once you close your browser, which "essentially wipes clean your history," said Jeremiah Grossman, chief technology officer with WhiteHat Security, an online security consulting firm in Santa Clara, Calif.

He warned, however, that private mode does nothing to conceal your I.P. address, a unique number that identifies your entry or access point to the Internet. So Web sites may not know your browsing history, but they will probably know who you are and where you are as well as when and how long you viewed their pages.

Shielding your I.P. address is possible by connecting to what is called a virtual private network, or V.P.N., such as those offered by WiTopia, PrivateVPN and StrongVPN. These services, whose prices price from $40 to $90 a year, route your data stream to what is called a proxy server, where it is stripped of your I.P. address before it is sent on to its destination.

This obscures your identity not only from Web sites but also from your Internet service provider. These services encrypt data traveling to and from their servers so it looks like gibberish to anyone who might be monitoring wireless networks in places like coffee shops, airports and hotels.

While V.P.N. providers generally have strict privacy policies, Moxie Marlinspike, an independent security researcher and software developer in San Francisco, said, "It's better to trust the design of the system rather than an organization." In that case, there is Tor, a free service with 36 million users that was originally developed to conceal military communications. Tor encrypts your data stream and bounces it through a series of proxy servers so no single entity knows the source of the data or whence it came. The only drawback is that with all that bouncing around, it is very S-L-O-W.

Free browser add-ons that increase privacy and yet will not interrupt your work flow include Ghostery and Do Not Track Plus, which prevent Web sites from relaying information about you and your visit to tracking companies. These add-ons also name the companies that were blocked from receiving your data (one social network, five advertising companies and six data brokers on a recent visit to CNN.com), which is instructive in itself.

"Companies like Google are creating these enormous databases using your personal information," said Paul Hill, senior consultant with SystemExperts, a network security company in Sudbury, Mass. "They may have the best of intentions now, but who knows what they will look like 20 years from now, and by then it will be too late to take it all back."

This article has been revised to reflect the following correction:

Correction: May 4, 2012

An earlier version of this article misspelled Asheville, N.C., as Ashville.

http://www.nytimes.com/2012/05/03/technology/personaltech/how-to-muddy-your-tracks-on-the-internet.html?_r=1&src=me&ref=general