KATHERINE ALBRECHT

LIZ MCINTYRE

# How and Why to Keep the NSA Out of Your Private Stuff – Even If You've "Got Nothing to Hide"

Have you noticed that after shopping for shoes online, you see advertisements for similar shoes on seemingly every site you visit? It's not a coincidence. You are being watched by Internet marketers. Here are some of the sneaky ways they have cooked up to learn about you and follow your online activities.

1) **They tap into your data.** Whenever you make a purchase, create an online account or give your name and email address to a website, you're accepting a mountain of fine print – and probably volunteering to be tracked, too. What you do when logged into that account also gets logged and tied to your identity.
2) **They "review" your email and instant messages.** Check the terms of many free services and you'll find they scan your messages for keywords. This gives them a goldmine of private data, in addition to your signup information. Check out the fine print in Yahoo's privacy policy as an example [1].
3) **They know you wear your location on your sleeve.** Your computer transmits an Internet Protocol (IP) address that tells websites where to deliver content. Since IP addresses are assigned by geography, marketers use them to get a general sense of your location. That's why you may see ads for "Hot babes in [your town name] waiting to meet YOU!"
4) **They milk your cookies.** Cookies are bits of code that let websites keep track of you over time. Some cookies are necessary, for example, to remember what's in your online shopping cart. But many websites place tracking cookies in your browser just to monitor your movements across the Internet.
5) **They "dust" for fingerprints.** Computer browsers are as unique as the people using them. Different time settings, add-ons and privacy preferences create fingerprints that are useful in profiling and tracking you [2].
6) **They insert other stealthy trackers.** Web beacons, pixel trackers and flash cookies are just a few of the other creative tricks marketers have dreamed up to stealthily track consumers.

Fortunately, you can give Internet trackers the slip to reduce your online tracking footprint. Here's how:

1) **Seek out privacy-friendly alternatives.** A small but growing number of websites promise not to log your visits or track you [3].
2) **Manage cookies.** Set your browser privacy options to reject third-party cookies, block marketing cookies, and delete cookies each time you close your browser. Look online for directions explaining how to do this in most browsers

*Digital Object Identifier 10.1109/MTS.2014.2369571*
*Date of publication: 1 December 2014*

such as Firefox [4], Google Chrome [5], Internet Explorer [6], and Safari [7].

3) **Use your browser's privacy options.** If you must visit sites known to track visitors, keep them at bay with the "Do Not Track" setting. Unfortunately, some sites don't honor the setting.
4) **Visit websites using a proxy.** A proxy fetches information for you so you remain anonymous.
5) **Use Ghostery to block trackers such as web beacons.** New-fangled trackers are stealthy, but Ghostery (www.ghostery.com) helps level the playing field by showing who's trying to track you.

## Is the Government Really Watching Us?

Are you wondering if you should bother protecting yourself from online tracking? The answer is a resounding yes. Online privacy is about more than just preventing marketing companies from snooping – the government wants this data too! Could you be a surveillance target? Take this short quiz to find out.

Have you ever:

- Grumbled about high income taxes in an online forum?
- Performed an Internet search about the Bill of Rights?
- Said you'd oppose the government injecting RFID microchips into people?
- Supported a 3rd-party U.S. presidential candidate like Ron Paul or Bob Barr?
- Forwarded an email with pro-life content?
- Visited any websites about these or other controversial topics?

While these examples are U.S.-based, you can find parallels regardless of where you live. If you answered yes to any of them, you need to think harder about protecting your privacy. Whether you're a school teacher, cab driver, doctor, fast food worker, or stay-at-home parent – and the most law-abiding person in the world – doesn't matter. You could still be considered a "person of interest" based on perfectly legal online activities and comments. In fact, you could wind up on a government watch list for simply exercising your right to free speech and association.

## Don't Believe This?

Take a look at the Missouri Information Analysis Center Report, a document that originated from a "fusion center" that combines intelligence information from the Department of Homeland Security and other federal, state and local agencies [8].

Long before Edward Snowden's revelations of government spying made the headlines, this 2009 law enforcement document revealed some shocking things about the government's interest in our lives. It urges law enforcement agencies to scrutinize regular folks based on the causes they support, their religious beliefs, their political affiliations, and what they read and watch. Any interest in the topics listed above could peg you as belonging to "The Modern Militia Movement" and mark you as a potential domestic terrorist, according to the MIAC report.

When government suspicion tips into paranoia, thoughtful people start thinking hard about privacy. Over time, your posts, texts, and searches and what you write through "free" email services paint an intimate picture of your life — and one you should probably keep to yourself.

Recently, Edward Snowden revealed that the U.S. National Security Agency (NSA) is collecting much more than just metadata. We can argue whether this is right or wrong, necessary or a power grab. But arguing won't keep hackers, snoops, and advertisers out of your data. Face it: You've got private stuff to protect, and you need a way to keep it from prying eyes. The Internet offers one clear solution — encryption.

## Encryption Basics

Encryption is a method of mathematically scrambling information so only you and your recipient can make sense of it. If someone intercepts an encrypted email, conversation, or photo, it appears as gobbledygook. Unless the intercepting person has the key, it can take years or even decades to decode a single, powerfully-encrypted message.

That level of encryption is useful for thwarting Wi-Fi hackers and nosy email providers, but could it actually stop the NSA? The answer is a resounding "yes," as confirmed by Ed Snowden himself in a *Guardian* interview [9]. To everyone's relief, our favorite whistleblower confirmed: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

The encryption of the past required a technical background, but today's tools make it easy for everyone to get on board. You can use one of these methods to get more encryption in your life, even if you're a security novice.

## Encrypt Your Email Messages

The best email encryption is called Pretty Good Privacy, which fortunately is a misnomer, since PGP is actually very powerful. PGP scrambles your message, making if impossible to read unless you have the key. While PGP is notorious for being difficult to set up and use, Katherine has been part of a team working to make it easier. Their project, StartMail, gives users the power of PGP encryption with a single click and is scheduled to launch in late 2014.

## Switch to Encrypted Versions of the Services You Use Most

Now that people are wising up to surveillance, a bumper crop of new programs can help keep your chats, texts, and even phone calls private. *Fight for the Future* has put together a helpful Privacy Pack of encryption tools you can use to "reset the net." You can download encrypted alternatives to your favorite tools at their Reset the Net website [10].

## Encourage Websites to use Encryption, and Support Pro-Encryption Activists

When you see "HTTPS" in a website's URL address when you connect to it, that's your sign the website is foiling eavesdroppers by encrypting what you type and what the site displays to you. Sites that handle sensitive data like email and credit card numbers should always display the "https" (and often a lock) in the address bar. Not all sites are using this protocol yet, but activists groups like *Access* are working hard to get the whole Internet on board. You can support their efforts at Encrypt All the Things [11].

## Encrypt Your Hard Drive and Portable Devices

It's easier than you think to encrypt your laptop and other devices that can be lost or stolen — or confiscated. While recent rumors warn that some hard-drive encryption programs may have been compromised, they can still provide a first level barrier against snooping. Look online for tools to encrypt your platform. For Windows use BitLocker; for Mac, FileVault; for Linux search for "Encrypted LVM" and your Linux distribution name.

## Equip Yourself for the Information Arms Race

Modern encryption goes beyond protecting personal files, it's about equipping yourself for an information arms race that is fundamental to privacy and civil liberties. Even if you're the NSA's biggest fan, consider that sharing unencrypted information online is like showering in front of a picture window with the curtains wide open. Have some self-respect, folks. Draw the shades!

## Author Information

Katherine Albrecht is the VP Marketing for StartPage, Inc. Email: kma@startmail.com.

Liz McIntyre is the co-author of *Spychips*. Email: liz@startmail.com.

## Acknowledgment

This article has been adapted from three previous online posts first published by the authors on eHow.com between June 30, 2014 and July 14, 2014 [12]–[14].

## References

[1] "Yahoo Mail FAQ," Yahoo.com, 2014; https://info.yahoo.com/privacy/us/yahoo/mail/ymailfaq/.

[2] M. Brinkmann, "At least 1% of the Top 10000 websites use fingerprinting to track users," ghacks.net, Oct. 11, 2013; http://www.ghacks.net/2013/10/11/least-1-top-10000-websites-use-fingerprinting-track-users/.

[3] Startpage, "the world's most private search engine," startpage.com, 2014; www.startpage.com.

[4] Firefox, "Privacy and security settings – Cookies," Mozilla support, 2014; https://support.mozilla.org/en-US/products/firefox/privacy-and-security/Cookies.

[5] Google, "Manage your cookies and site data," Help, 2014; https://support.google.com/chrome/answer/95647?hl=en&ref_topic=3421433.

[6] "Delete and Manage Cookies," Windows, 2014; http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-11-win-7.

[7] "Safari 7 (Mavericks): Manage cookies and other website data," apple.com, May 29, 2014; http://support.apple.com/kb/PH17191

[8] Missouri Information Analysis Center, "MIAC Strategic Report: The Modern Militia Movement," constitution.org, Feb. 20, 2009; http://www.constitution.org/abus/le/miac-strategic-report.pdf.

[9] G. Greenwald, "Edward Snowden: NSA whistleblower answers reader questions," theguardian.com, June 17, 2013; http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

[10] "Privacy pack," Reset the Net; https://pack.resetthenet.org/, accessed Nov. 1, 2014.

[11] "Encrypt all the things," 2014; https://encryptallthethings.net/.

[12] K. Albrecht and L. McIntyre, "Six ways websites ID and track you – and how you can fight back!," Ehow.com, Jun. 30, 2014; http://www.ehow.com/ehow-tech/blog/ways-websites-track-you-and-how-you-can-fight-back/.

[13] K. Albrecht and L. McIntyre, "Why care about online privacy (if you've got nothing to hide)," Ehow.com, Jul. 7, 2014; http://www.ehow.com/ehow-tech/blog/who-cares-about-online-privacy-got-nothing-to-hide/.

[14] K. Albrecht and L. McIntyre, "Encryption 101: Keep the NSA out of your private stuff," Ehow.com, Jul. 14, 2014; http://www.ehow.com/ehow-tech/blog/encryption-101-keep-nsa-out-of-your-private-stuff/.