CSO
SECURITY AND RISK

From: www.csoonline.com

The paranoid's survival guide, part 1: How to protect your personal data

Who says privacy is dead? While it's true that marketers, the government, data aggregators and others are gathering and analyzing more data than ever about every individual, you can still exert some control over what's out there, who's tracking you and what they do with that information.

Robert L. Mitchell, Computerworld

March 03, 2014

Who says privacy is dead? While it's true that marketers, the government, data aggregators and others are gathering and analyzing more data than ever about every individual, you can still exert some control over what's out there, who's tracking you and what they do with that information.

From the NSA's admission that it is capturing and analyzing metadata on every American to Facebook's appropriation of users' posts, likes and images for use in product advertising endorsements, privacy concerns are now top of mind. According to a December Harris Interactive survey commissioned by privacy consultancy Truste, 74% of Internet users are more worried about privacy now than they were a year ago. Some 74% also say they are less likely to enable location tracking on the Web, 83% are less likely to click on online ads and 80% say they are less likely to use apps they don't trust.

Consumers' privacy concerns

What people are most afraid of. All percentages are up compared to last year. The study was conducted by Harris Interactive, on behalf of Truste, with more than 2,000 U.S. internet users polled in December 2013.

Online shopping - 93%

Online banking - 90%

Using social media - 90%

Using mobile apps - 85%

Truste 2014 Consumer Confidence Privacy Report

Computerworld asked nine people who live and breathe privacy what steps they recommend to get a handle on your personal data footprint -- both offline and online. Some steps are easy, while others require both time and expertise to set up.

The key, these experts say, is to know what your goals are and go for the low-hanging fruit first. "If your goal is perfection, you'll end up doing nothing. Look for good enough," says Jules Polonetsky, executive director of the Future of Privacy Forum.

There are three primary reasons why people want to reduce their footprint, Polonetsky says. One is to hide from marketers. Another is personal security. Some people have good reason to be cautious about their identity, including those worried about domestic violence or stalkers. That takes a bit more work.

But the most extreme measures are generally reserved for people who have reason to worry that they might be targeted by the NSA, or by law enforcement, or be the subject of civil proceedings. For the latter group, Polonetsky says, the required measures are more difficult to set up and use -- and the techniques may degrade

the user's experience online.

Fortunately, most people don't need to go to these extremes. "Complete privacy is very difficult and expensive to achieve. But reasonable privacy -- minimizing your footprint -- is easier to achieve than you might think," says Rob Shavell, co-founder and CEO at privacy software vendor Abine.

The information out there about you out falls into three basic categories, Shavell says:

Data that's implicitly collected, such as the many services that track your browsing activity online

Data that's explicitly collected, such as when you knowingly give out your email address and other data when signing up for a service online

Publicly available information about you that can be harvested by data collectors online, such as your phone number and address, Twitter feed, Facebook profile and public posts, court and property deed records and so on

The first step toward minimizing your online footprint is to know who's tracking you. Tools like Disconnect and Mozilla's Lightbeam, which visually show who's tracking you as you visit different websites, can help, says Sid Stamm, senior engineering manager for security and privacy at Mozilla.

Mozilla's Lightbeam

Tools like Mozilla's Lightbeam visually show who's tracking you as you visit different websites.

"The second thing is to figure out what the risks are that you're trying to protect yourself from," he says. Do you care who reads your Facebook updates? Or if someone you don't know can read your email? The more data you want to protect, the more work you'll need to do.

"The third layer is control, and that's the hard part," Stamm says. For example, if you want to hide all of your Internet traffic and your identity, you'll need to use Tor or a VPN all the time. Most people, however, just want a reasonable amount of privacy.

Ready to minimize your data footprint? Here's where to start.

The basics: Six standard operating procedures for online behavior

Draw the line: Decide what's personal

The traditional definition of personally identifying information (PII) -- health records, credit card numbers, social security number, etc. -- is so 20th century. The big data age of the Internet is upon us, and even data not previously considered to be PII can feel very personal when viewed in a broader context. "Bits of data, when combined, tell a lot about you," says Alex Fowler, chief privacy officer at Mozilla. Those aggregated bits, which constitute the new PII, may include such information as your email address, browsing history and search history.

"The definition of PII -- information that a person has a legitimate interest in understanding and protecting -- is going to be broadened as we move further into the information society," says Fowler. "It's a different footprint than what your parents ever thought about."

"Think about what you consider personal information," Fowler adds. "You need a working definition."

Don't share your personal information -- even when asked

Are you responding to surveys by phone or online? Filling out warranty cards? (You need only your receipt to make a warranty claim.) Providing optional preference and demographic information when signing up for an online service? "Most of us give out information trivially," says Abine's Shavell, not understanding that all of that information ends up in profiles that may be used by the collector and later shared with data aggregators and others.

When you absolutely must remain anonymous

Tor is an essential tool to use when the sender needs to disseminate information and anonymity is essential. "It is the perfect tool for political dissidents who don't want their names attached to information," says Robert Hansen, a security researcher and director of product management at the vendor WhiteHat Security. (Tor also appeals to organized crime and other people who don't want the law to catch up with their activities.)

But, there's a cost to using it. "It's a hassle," and it can degrade a person's Web experience, says Casey Oppenheim, CEO at anti-tracking software vendor Disconnect.

Tor consists of an open source browser you can download and a network that acts on your behalf to conceal your identity by preventing others from tracing network traffic back to you.

"Tor tunnels your traffic through a volunteer network of 5,000 relays spread around the world. Tor protects your content in transit by wrapping layers of encryption around your data without modifying or touching your data in transit," explains Andrew Lewman, executive director of the Tor Project.

Your data keeps hopping from one node to another until a limit is reached. At that point it exits the Tor network and continues on to its destination. (The last node to handle the data is called the exit node). "Tor is essentially a very large, distributed VPN that's free," and it works well when used properly, Hansen says.

But it can also be dangerous if you don't understand how to use it properly, as the Tor Project's warnings make clear. "Tor can help you remain anonymous -- if the account you logged into on the other end isn't tied back to your real identity," Hansen says.

"That last machine, the exit node, knows who you are if you submit your information in plain text, and that can break your privacy." Users should understand that all of the nodes in the Tor network are operated by volunteers, Hansen says. If you're logged into a service such as an online loan application, the owner of the exit node may be privy to all of that information.

It's also not a good idea to use Tor to download an executable unless you can verify it hasn't been tampered with, Hansen says, because the owners of the exit node could, if they wanted to, modify the content and change it to a malicious binary. But, Lewman points out, "Tor exit nodes are no more risky than your ISP's caching proxy servers and other points along the path."

Hansen's recommendation: "Use Tor only over HTTPS, and only when you don't want your name associated with whatever is going to happen over HTTPS."

Even then, he says, it is important to remember that some entities out there, such as certain government agencies, may still be able to decrypt the message and identify you.

-- Robert L. Mitchell

Lie. About. Everything.

Many online services demand that you divulge some information about yourself if you want to do business with them. If you don't want to share, you can either choose not to use that service -- or you can provide false information. Don't use your real birthday, email, address and phone number on social network sites, and don't use real answers when creating answers to challenge questions, says Robert Hansen, a security researcher and director of product management at the website security consultancy WhiteHat Security.

"Never give out any real information about yourself unless absolutely necessary. Lie about everything. That's basic operational security," he says.

You may, of course, need a working email address to validate an account. You can create a webmail account specifically for this purpose, or you can use a service such as DoNotTrackMe, which creates "disposable" proxy email addresses and phone numbers for this purpose. Yahoo Mail also offers disposable email addresses.

Create personal and professional personas

Stamm creates and maintains separate personal and professional online profiles for browsing the Web. Specifically, he uses separate instances of Firefox for each persona. "The experience is less noisy," he says, because his personal and professional web histories aren't mashed together.

Casey Oppenheim, CEO at anti-tracking software vendor Disconnect, recommends using one browser for Web surfing and another to log into your online accounts like Facebook, Google or Twitter -- to reduce cross-site tracking.

Understand how much you're paying before signing up for "free" apps and online services

By now most people realize that the price you pay for using "free" online websites, apps and services is

measured in data collected about you. The question you need to ask is: How high is the price?

Understand exactly what data you are giving up and weigh that against the value of the app or service you're receiving in return. For example, you might need to share an email address for your Facebook account, but you don't need to share your telephone number and location data, or allow search engines to index and link to posts on your timeline. You can lower the price somewhat by taking advantage of available privacy controls that let you limit the types of data collected or how it's used and shared.

But privacy policies can change at any time, and no one knows what will happen to that data in the future. If the developer of an app goes out of business, for example, your data may be sold. Which is why you should always...

Delete your unused online accounts

Do you leave a trail of orphaned accounts behind you as you try different online services? Close them down, or that trail of digital relationships might come back to haunt you. "There are dozens of social networks that came and went over the years, and I think I signed up with every one of them along the way," says Mozilla's Fowler.

Many of the services you sign up for eventually disappear. "When they do, that information about you will be sold to someone at some time as an asset," he says, and the value of those assets is based on how many users they had and what they know about them.

The deeper they got with their customers, the more valuable the assets. "You have no idea how it's getting used or where it might resurface at another point in your life, so it's important to take this seriously," he says.

Tips for surfing the Web silently

Block "third-party" cookies

The publisher of the site you visit isn't the only organization that knows about your online browsing activity. Many pages have third-party widgets on them that track your computer's online activity as you move from one site to another on the Web. They do this to sort people (or more specifically, the cookie IDs associated with each person's computer) into groups that can be targeted with "behavioral advertising" based on interests gleaned from your Web-surfing habits.

One way to minimize your exposure to this kind of marketing and data collection activity is to turn on third-party cookie blocking in your browser. Safari enables this feature by default, while Internet Explorer, Chrome, Firefox and other popular browsers offer it as an option. If you prefer not to have your browsing activity tracked for behavioral advertising purposes, you should also turn on the "Do Not Track" option found on all popular browsers. This feature sends a "DNT" signal from your browser to Web publishers when you visit their sites.

Go private with your browsing

If you want to minimize your data footprint at home or in the office, or wherever others have physical access to your computer, consider using a secure browser such as WhiteHat Aviator, Dell's Kace Secure Browser and Comodo Dragon. Alternately, you can use the secure browsing mode in Chrome, Firefox, Safari or IE. This will block third-party cookies, delete first-party cookies at the end of a browsing session and leave no trace of your browsing history and search history on your computer.

"Blocking cookies and clearing them regularly stops most cross-site tracking," says Brookman.

Be aware, however, that some sites, such as Google, Yahoo and Microsoft, offer single sign-on for all services. So when you sign onto your Gmail account, for example, all of your information -- user name, password, webmail, images uploaded, etc. -- persists on the provider's servers.

In addition, your search activity can be tied back to your account and the search history maintained, along with your activity on all other services -- unless the provider's privacy policy precludes it or the vendor offers privacy controls you can use to prevent that information from being stored.

Bottom line: Once you log into a service, all of your activity across all related services from that provider -- from webmail to searches -- can be tracked back to your account. So log in only when you need to, and be sure to log out when you're done.

Use anti-tracking software

Unfortunately, blocking third-party cookies doesn't block the activities of all tracking scripts, and many advertisers ignore the DNT signal, so Hansen recommends installing anti-tracking browser add-ons.

"Something like Disconnect blocks ads plus third-party tracking pixels" and has the added benefit of speeding up Web page load times by removing all of that extraneous tracking activity, Hansen says. Disconnect, Abine's DoNotTrackMe, Ghostery and other consumer-friendly anti-tracking tools don't block everything -- doing so can break things you want to use -- but try to strike a balance for the best user experience. For example, Disconnect doesn't block Google's third-party advertising network DoubleClick when you're using Google services. "Google is already tracking you when you log into google.com, so blocking the doubleclick.net request wouldn't stop any tracking, and is likely to break the page," says Casey Oppenheim, Disconnect's co-CEO.

If that's not good enough for you, Hansen says, "The extreme level is to use NoScript or RequestPolicy. "Flash, Java, whatever it is, [these tools] block it if it's cross-domain. It's uber-draconian, and it breaks just about everything, but it's very effective," he says.

These tools also offer greater security because they block malware that attempts to compromise your computer by way of JavaScript include or iframe injection attacks. However, it's up to users to whitelist content that they want to get through. "You have to know what you're doing, and it requires a big expenditure of time," he says.

Secure your searches

Use a search engine such as DuckDuckGo or Startpage -- in other words, one that doesn't retain your search history. (The WhiteHat Aviator browser uses DuckDuckGo as its default search engine.)

Or use a proxy search service such as Disconnect Search, which sits between your browser and the popular search engines so that your search history can't be tracked. (Ixquick, located in the Netherlands, works in the same way and also has the advantage of being out of reach of the U.S. Patriot Act and the FISA court.)

If you prefer to use a commercial search engine, you may be able to turn off search and browsing history. For example, in Google you can turn off search history from the Google Dashboard, while the Chrome browser offers Incognito mode.

Use HTTPS whenever possible

All data that passes between your browser and the Internet is unencrypted and open to snooping, unless you've entered an encrypted session with the service you're communicating with on the other end. Some sites, such as your bank, will encrypt your communications using the HTTPS protocol by default, while others, such as your webmail, may not. For example, Gmail enabled HTTPS by default three years ago, but Yahoo Mail only began supporting HTTPS one year ago, and it's not turned on by default. If you're not sure, check first before you use the service.

You can use the Electronic Frontier Foundation's HTTPS Everywhere browser extension to make sure you're using HTTPS when it's available, but some sites don't offer HTTPS, says Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology. In that case, he says, you may want to consider using a virtual private network (VPN) service.

Sign up for a VPN service

Your IP address gives Web publishers and e-commerce sites an identifier that provides clues to your location. It allows Web publishers to deliver geo-targeted content, such as your local weather, but they can also target you in less pleasant ways. For example, some online retailers have moved to geotargeted pricing, which determines the price you see for an item based on your location and how many brick-and-mortar competitors are nearby. Depending on your location, this could be a good thing or a bad thing.

And if you're browsing the Web using a public Wi-Fi hotspot, it's not just your IP address you need to worry about. If your browsing session is unencrypted, all of that data -- including user account names and passwords -- could be snatched literally from the airwaves.

The solution in both cases is to use a virtual private network (VPN) service such as Astrill, Anonymizer, IPVanish or AnchorFree. These tools not only protect your IP address, but encrypt your communications, which are routed through the VPN service's servers before going on to the intended destination. "People can't eavesdrop on what you're doing, or steal your login credentials and impersonate you," Hall says.