Ideas for keeping your data safe from spying (Update)

June 14 2013, by Raphael Satter

Phone call logs, credit card records, emails, Skype chats, Facebook message, and more: The precise nature of the NSA's sweeping surveillance apparatus has yet to be confirmed.

But given the revelations spilling out into the media, there hardly seems a single aspect of daily life that isn't somehow subject to spying by the U.S. agency.

For some, it's a matter of indifference who or what is rifling through their electronic records. Others, mindful of spy agencies' history of abuse, are more concerned.

Here are some basic tips to avoid having your personal life turned into an intelligence report:

___

ENCRYPT YOUR EMAILS

Emails sent across the Web are like postcards. In some cases, they're readable by anyone standing between you and its recipient. That can include your webmail company, your Internet service provider and whoever is tapped into the fiber optic cable passing your message around the globe—not to mention a parallel set of observers on the recipient's side of the world.

To beat the snoops, experts recommend encryption, which scrambles messages in transit, so they're unreadable to anyone trying to intercept them. Techniques vary, but a popular one is called PGP, short for "Pretty Good Privacy." PGP is effective enough that the U.S. government tried to block its export in the mid-1990s, arguing that it was so powerful it should be classed as a weapon.

Disadvantages: Encryption can be clunky. And to work, both parties have to be using it.

___

USE TOR

Like emails, your travels around the Internet can easily be tracked by anyone standing between you and the site you're trying to reach. TOR, short for "The Onion Router," helps make your traffic anonymous by bouncing it through a network of routers before spitting it back out on the other side. Each trip through a router provides another layer of protection, thus the onion reference.

Originally developed by the U.S. military, TOR is believed to work pretty well if you want to hide your traffic from, let's say, eavesdropping by your local Internet service provider. And criminals' use of TOR has so frustrated Japanese police that experts there recently recommended restricting its use. But it's worth noting that TOR may be ineffective against governments equipped with the powers of global surveillance.

Disadvantages: Browsing the web with TOR can be painfully slow. And some services—like file swapping protocols used by many Internet users to share videos and music—aren't compatible.

___

DITCH THE PHONE

Your everyday cell phone has all kinds of privacy problems. In Britain, cell phone safety was so poor that crooked journalists made a cottage industry out of eavesdropping on their victims' voicemails. In general, proprietary software, lousy encryption, hard-to-delete data and other security issues make a cell phone a bad bet for storing information you'd rather not share.

An even bigger issue is that cell phones almost always follow their owners around, carefully logging the location of every call, something which could effectively give the NSA a daily digest of your everyday life. Security researcher Jacob Appelbaum has described cell phones as tracking devices that also happen to make phone calls. If you're not happy with the idea of an intelligence agency following your footsteps across town, leave the phone at home.

Disadvantages: Not having a cell phone handy when you really need it. Other alternatives, like using "burner" phones paid for anonymously and discarded after use, rapidly become expensive.

___

CUT UP YOUR CREDIT CARDS

The Wall Street Journal says the NSA is monitoring American credit card records in addition to phone calls. So stick to cash, or, if you're more adventurous, use electronic currencies to move your money around.

Disadvantages: Credit cards are a mainstay of the world payment system, so washing your hands of plastic money is among the most difficult

moves you can make. In any case, some cybercurrency systems offer only limited protection from government snooping and many carry significant risks. The value of Bitcoin, one of the better-known forms of electronic cash, has oscillated wildly, while users of another popular online currency, Liberty Reserve, were left out of pocket after the company behind it was busted by international law enforcement.

___

DON'T KEEP YOUR DATA IN AMERICA OR WITH AMERICAN COMPANIES

U.S. companies are subject to U.S. law, including the Patriot Act, whose interpretations are classified. Although the exact parameters of the PRISM data mining program revealed by the Guardian and The Washington Post remain up for debate, what we do know is that a variety of law enforcement officials—not just at the NSA—can secretly demand your electronic records without a warrant through an instrument known as a National Security Letter. Such silent requests are made by the thousands every year.

If you don't like the sound of PRISM, National Security Letters, or anything to do with the Patriot Act, your best bet is to park your data in a European country, where privacy protections tend to be stronger.

Disadvantages: Silicon Valley's Internet service providers tend to be better and cheaper than their foreign counterparts. What's more, there's no guarantee that European spy agencies don't have NSA-like surveillance arrangements with their own companies. When hunting for a safe place to stash your data, look for smaller countries with robust human rights records. Iceland, long a hangout for WikiLeaks activists, might be a good bet.

___

STEER CLEAR OF MALICIOUS SOFTWARE

If they can't track it, record it, or intercept it, an increasing number of spies aren't shy about hacking their way in to steal your data outright. Edward Snowden, the NSA leaker, warned the Guardian that his agency had been on a worldwide binge of cyberattacks.

"We hack everyone everywhere," he said.

Former officials don't appear to contradict him. Ex-NSA chief Michael Hayden described it as "commuting to where the information is stored and extracting the information from the adversaries' network." In a recent interview with Bloomberg Businessweek, he boasted that "we are the best at doing it. Period."

Malicious software used by hackers can be extremely hard to spot. But installing an antivirus program, avoiding attachments, frequently changing passwords, dodging suspicious websites, creating a firewall, and always making sure your software is up to date is a good start.

Disadvantages: Keeping abreast of all the latest updates and warily scanning emails for viruses can be exhausting.

___

SO WILL ALL THIS KEEP MY DATA SAFE FROM SPYING?

Safer, maybe.

Using anonymity services and encryption "simply make it harder, but not impossible for a dedicated investigator to link your activities together and identify you," Ashkan Soltani, an independent privacy and security researcher, said in an email.

"Someone can always find you—just depends on how motivated they are (and how much information they have access to)."