When we're all connected, online privacy is tough to achieve

July 3 2013, by Pete Carey

Services that offer secure Web browsing and search have been enjoying a surge in popularity since the revelations about National Security Agency monitoring of domestic phone calls, email and Internet activity.

"We always knew people didn't want to be tracked, but they didn't know what to do about it," said Gabriel Weinberg, founder of the Pennsylvania-based DuckDuckGo, which allows users to search the Internet anonymously. "Now there are private alternatives you can switch to and never look back."

But how secure can we really be in an age of social networking, e-commerce and the cloud?

We now store our documents and photos in the cloud, where a determined hacker might find them. Federal authorities armed with a search warrant can read our texts in real time, as Galleon hedge fund founder Raj Rajaratnam learned when he was charged with insider trading. And we spill out our lives on Facebook and our opinions on Twitter.

Experts say that while sites offering online anonymity can conceal part of your Internet activity from prying eyes, they can't hide all of it. Even when you use a secure Web searcher, by clicking on one of the links it displays, you leave privacy behind, and your information is visible to whatever Web page you land on.

"There are limits to what they can do," said Seth Schoen, the Electronic Frontier Foundation's senior staff technologist.

Jeff Chester, executive director for the Center for Digital Democracy, says most Americans "have already sacrificed their privacy" by shopping, signing up for discounts and engaging in other online activities that people take for granted.

That makes it easier for the government to spy on us, Chester said, if that's what it wants to do.

Still, there are many ways to increase your online privacy. You can tinker with the privacy settings on your browser; add encryption and ad-blocking extensions to it, and search anonymously with several search engines. You can encrypt emails and mobile phone calls and the data you store in the cloud.

For browsing, for example, Chrome's "incognito mode" doesn't save a history of where you have been, and deletes cookies after you're done with a Web page. Firefox and Internet Explorer have similar settings.

A browser extension called HTTPS Everywhere defaults to the encrypted version of a Web page if it's available.

The Tor Project is considered by some to be the ultimate in protecting your identity on the Internet. The project provides a free bundle of software, including a special browser, that it says prevents the tracking of the source and destination of your Internet activity, which could be used to track your behavior and interests. Tor routes your activity through three randomly selected computers around the globe out of a total of more than 3,200 staffed by volunteers. HTTPS Everywhere is built into the browser.

For searching, DuckDuckGo provides anonymous Web searches and Blekko has its own proprietary "spam-free" search engine so it doesn't send your queries to other search engines, as many "anonymizing" platforms do.

The Netherlands-based Surfboard Holding's Ixquick and Startpage let you continue to Web pages via a proxy server, which substitutes its address for yours, masking your identity.

But Jeremiah Grossman of WhiteHat Security says "proxies and Tor are the way to go" but warns "the value provided by proxies is completed voided when using sites like Gmail and Facebook when you voluntarily hand over your data - something that pretty much everyone does."

If you're worried about government snooping, the Dutch company that makes Ixquick and Startpage is beyond reach of a U.S. court subpoena and doesn't save your data anyway.

"It's a lot harder to force a Netherlands-based company to cooperate with programs like PRISM than it would be with a U.S.-based company," said Ixquick CEO Robert Beens.

For phone calls and emails, PGP by Symantec and the free GPG offer public key encryption for email and data, while RedPhone and TextSecure by Whisper Systems encrypt your mobile Android phone and text messages. Both people have to be using the software.

For the advertising averse, Adblock Plus lets users filter ads on websites. It claims 40 million users. Yahoo allows visitors to its Web pages to opt out of ads through its Ad Interest Manager.

Some search sites filter content, blocking out most advertising. Blekko searches are pretty much free of unwanted clutter.

And Yippy is a search engine that blocks malicious and objectionable content and is considering moving to a subscription-based model with no ads. "Advertising is Big Brother," said CEO Rich Granville.

On the other hand, Google likes to remind people that advertising pays for the many services it offers.

—-

ONLINE SECURITY TIPS:

Here are a few ideas for specific situations where you want more privacy than is afforded by your native software and system, courtesy of Seth Schoen, senior staff technologist at the Electronic Frontier Foundation.

1. You want to keep your browsing private at work: Use a browser made by the Tor Project or a paid VPN (for virtual private network) link, or a personal hotspot. Don't use an employer-provided or administered computer if company policy allows surreptitious monitoring.

2. You want to avoid government surveillance: Install HTTPS Everywhere on your browser and consider the Tor Browser Bundle.

3. You want your mobile calls to be shielded from eavesdroppers: Install an encrypted VoIP application such as RedPhone or Silent Circle.

4. You want your information in the cloud secure from snooping: Encrypt your data before uploading it. Some services actually require data to be encrypted before it is uploaded: SpiderOak, Wuala and Tarsnap.

—-

SOFTWARE AND SITES FOR THE PRIVACY-CONSCIOUS:

-Tor Browser Bundle (Tor Project): Preconfigured to protect your privacy and anonymity on the Web as long as you're browsing with the Tor browser itself.

-HTTPS Everywhere (Tor Project and Electronic Frontier Foundation): Firefox and Chrome extensions that encrypt communications with many major websites.

-DuckDuckGo: Internet search engine that protects your identity when you search, does not keep your data.

-Ixquick/Startpage (Surfboard Holding): Dutch search engine that does not collect data on users.

-Blekko: A search engine that does not save user data.

-PGP (Symantec): Encryption for emails and data.

-CPG (GNU Project): Encryption for emails and data.

-RedPhone and TextSecure: Encryption for phone calls and texting on Android mobile phones

©2013 San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services

Citation: When we're all connected, online privacy is tough to achieve (2013, July 3) retrieved 17 April 2024 from https://phys.org/news/2013-07-online-privacy-tough.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.