US surveillance flap shines light on Web 'anonymizers'

June 16 2013, by Rob Lever

A woman looks at a webpage on March 15, 2013 in Paris. News of a massive surveillance effort led by the secretive National Security Agency has sent Web users scrambling to find new ways to avoid tracking.

News of a massive surveillance effort led by the secretive National Security Agency has sent Web users scrambling to find new ways to avoid tracking.

It might have seemed paranoid not long ago when netizens used tools to

hide their tracks, "shred" data or send self-destructing messages.

Web anonymizers, encryption programs and similar tools have been available for years, but have been often associated with hackers, criminals and other "dark" elements on the Internet.

"I think the notion of what is an unreasonable level of paranoia has shifted in the past couple of weeks," said Alex Stamos, an NCC Group security consultant and self-described "white hat" hacker.

Ironically, some tools for eluding detection come from US government-funded programs aimed at helping people living under authoritarian regimes.

"The technologies usable in Tehran or Phnom Penh are just as usable in New York or Washington," said Sascha Meinrath, who heads a New America Foundation program helping users maintain secure and private communications in totalitarian countries.

"The real problem is that many people don't know these tools exist and a lot of them are not usable to non-geeks."

One of the well-known programs used to hide online traces is Tor, a tool originally developed by the US military and now managed by the nonprofit Tor Project.

Tor, which has some 500,000 users worldwide, about 15 percent of whom are in the United States, can be used online to hide one's IP address, effectively blocking tracking by governments or commercial entities seeking to deliver targeted advertising.

Tor's development director Karen Reilly said the US government promotes the program in other countries, but noted that it also protects

against snooping from US law enforcement.

"We get inquiries from law enforcement saying criminals are using Tor, and they want to know where the back door is," she said.

"There is no back door. We are protecting you not only from your (Internet provider) but from us. We never keep records that can identify our users."

Reilly brushed aside concerns about nefarious elements on the Internet hiding behind Tor and similar programs.

"Criminals are the ultimate early adopters of new technologies," she said.

If anonymous programs were not available, Reilly said "they would find another option."

People in the hacker and security communities say they are not surprised about the National Security Agency's PRISM program, but that its scope and its ability to scoop up huge amounts of data—if reports are correct—are frightening.

"The problem is we are keeping 'gold' in databases and it's impossible to secure this," said Nico Sell, a founder of Wickr, a startup that makes an app to allow people to secure and "shred" data sent on mobile devices.

Sell said she has seen "a tremendous uptick in downloads over the last week" of the Wickr app.

"People are now realizing that they get more security and are switching over from Skype," she said.

"All of our messages self-destruct... everyone has wanted self-

destructing messages since 'Mission Impossible.'"

Casey Oppenheim, co-founded of an online identity-masking program called disconnect.me, said he has surprisingly not seen a surge in downloads since the revelations, adding that it is not clear if Web users understand the implications of PRISM.

Oppenheim said the databases of major firms contain history of Web browsing searching which he called "highly personal."

"It's a direct connection to your personal thoughts... all of that information is online, it's very easy to get a hold of. Most people don't understand the extent to which this happens."

Oppenheim said the software operates like Tor, but has "an extra layer of protection" that allows users to log into their personal accounts and still remain anonymous online.

Stamos said that on the corporate side, communications cannot be encrypted because they must be available in case of court actions or subpoenas.

He said individuals can encrypt their emails but that this was too complicated for most people, requiring an exchange of encryption "keys."

In the browsing area, the search engine DuckDuckGo, which does not store IP addresses, said it has seen record growth.

"I think since the story broke, people have been seeking out privacy alternatives," said DuckDuckGo founder Gabriel Weinberg.

"No one from law enforcement has ever come to us for data, but if they

did we wouldn't have it."

Graham Cluley, a British-based independent security consultant, said people who use privacy tools should not be viewed as criminals.

"What would be troubling is if society begins to slide toward a viewpoint that paints the use of encryption and other tools that aim to protect our privacy as somehow 'dark arts,'" he said.

Meinrath of the New America Foundation said it would be ludicrous to try to ban online privacy tools.

"You would have to make illegal the pen or the computer or just about any other communication tool ever devised," he said.

The US Postal Service cannot open mail without probable cause "and yet the government is saying that if that is an electronic communication they have a right to surveillance," he said.

"The privacy of our correspondence is fundamental to our democracy."