Techies vs. NSA: Encryption arms race escalates

November 29 2013, by Martha Mendoza

Encrypted email, secure instant messaging and other privacy services are booming in the wake of the National Security Agency's recently revealed surveillance programs. But the flood of new computer security services is of variable quality, and much of it, experts say, can bog down computers and isn't likely to keep out spies.

In the end, the new geek wars, between tech industry programmers on the one side and government spooks, fraudsters and hacktivists on the other, may leave people's PCs and businesses' computer systems encrypted to the teeth but no better protected from hordes of savvy code crackers.

"Every time a situation like this erupts you're going to have a frenzy of snake oil sellers who are going to throw their products into the street," says Carson Sweet, CEO of San Francisco-based data storage security firm CloudPassage. "It's quite a quandary for the consumer."

Encryption isn't meant to keep out hackers, but when it's designed and implemented correctly, it alters the way messages look. Intruders who don't have a decryption key see only gobbledygook.

A series of disclosures from former intelligence contractor Edward Snowden this year has exposed sweeping U.S. government surveillance programs. The revelations are sparking fury and calls for better encryption from citizens and leaders in France, Germany, Spain and Brazil who were reportedly among those tapped. Both Google and

Yahoo, whose data center communications lines were also reportedly tapped, have committed to boosting encryption and online security. Although there's no indication Facebook was tapped, the social network is also upping its encryption systems.

"Yahoo has never given access to our data centers to the NSA or to any other government agency. Ever," wrote Yahoo CEO Marissa Mayer in a Nov. 18 post on the company's Tumblr blog announcing plans to encrypt all of its services by early next year. "There is nothing more important to us than protecting our users' privacy."

For those who want to take matters into their own hands, encryption software has been proliferating across the Internet since the Snowden revelations broke. Heml.is—Swedish for "secret"—is marketed as a secure messaging app for your phone. MailPile aims to combine a Gmail-like user friendly interface with a sometimes clunky technique known as public key encryption. Younited hopes to keep spies out of your cloud storage, and Pirate Browser aims to keep spies from seeing your search history. A host of other security-centered programs with names like Silent Circle, RedPhone, Threema, TextSecure, and Wickr all promise privacy.

Many of the people behind these programs are well known for pushing the boundaries of privacy and security online. Heml.is is being developed by Peter Sunde, co-founder of notorious file sharing website The Pirate Bay. Finland's F-Secure, home of Internet security expert Mikko Hypponen, is behind Younited. Dreadlocked hacker hero Moxie Marlinspike is the brains behind RedPhone, while Phil Zimmerman, one of the biggest names in privacy, is trying to sell the world on Silent Circle. Even flamboyant file sharing kingpin Kim Dotcom is getting in on the secure messaging game with an encrypted email service.

The quality of these new programs and services is uneven, and a few

have run into trouble. Nadim Kobeissi, developed encrypted instant messaging service Cryptocat in 2011 as an alternative to services such as Facebook chat and Skype. The Montreal-based programmer received glowing press for Cryptocat's ease of use, but he suffered embarrassment earlier this year when researchers discovered an error in the program's code, which may have exposed users' communications. Kobeissi used the experience to argue that shiny new privacy apps need to be aggressively vetted before users can trust them.

"You need to be vigilant," he says. "We're two years old and we're just starting to reach the kind of maturity I would want."

Heml.is also encountered difficulties and angered users when its creators said they wouldn't use open source—or publicly auditable—code. And Silent Circle abruptly dropped its encrypted email service in August, expressing concern that it could not keep the service safe from government intrusion.

"What we found is the encryption services range in quality," says George Kurtz, CEO of Irvine, California-based CrowdStrike, a big data, security technology company. "I feel safe using some built by people who know what they are doing , but others are Johnny-come-latelies who use a lot of buzzwords but may not be all that useful."

Even so, private services report thousands of new users, and nonprofit, free encryption services say they have also see sharp upticks in downloads.

And for many users, encryption really isn't enough to avoid the U.S. government's prying eyes.

Paris-based Bouygues Telecom told its data storage provider Pogoplug in San Francisco that it needs the data center moved out of the U.S. to get

out from under the provisions of U.S. law. So this month, PogoPlug CEO Daniel Putterman is keeping Bouygues as a client by shipping a multi-million dollar data center, from cabinets to cables, from California to France.

"They want French law to apply, not U.S. law," says Putterman, who is also arranging a similar move for an Israeli client.

Bouygues spokesman Alexandre Andre doesn't draw a direct connection with the Patriot Act, and says Bouygues' arrangement with Pogoplug is driven by concerns over performance and privacy. Andre says Bouygues wants the data stored in France, but it was up to Pogoplug to decide whether this would be done on Bouygues' own servers or Pogoplug's.

"There is a general worry in France over data security, and storing data in France permits us to reassure our clients," Andre says. The arrangement also helps improve the service's performance, Andre says, another reason for the move.

For Pogoplug, business is booming—it's garnered close to 1 million paid subscribers in its first year—and Putterman says the company is anxious to accommodate concerned clients. And this month, Pogoplug launched a $49 software package called Safeplug that prevents third parties, from the NSA to Google, from learning about a user's location or browsing habits.

But many warn that encryption offers a false sense of security.

"The fundamental designers of cryptography are in an arms race right now, but there are a series of weaknesses and missing oversights that have nothing to do with encryption that leave people vulnerable," says Patrick Peterson, CEO of Silicon Valley-based email security firm Agari. And many that do work, bog down or freeze computers, forcing

"a trade-off between security and convenience," he says.

In any case, most attacks don't happen because some cybercriminal used complicated methods to gain entry into a network, he adds.

"Most attacks occur because someone made a mistake. With phishing emails, it just takes one person to unwittingly open an attachment or click on a malicious link, and from there, cybercriminals are able to get a foothold," Peterson says.

In addition, experts agree that with enough time and money, any encryption can be broken. And already the NSA has bypassed —or altogether cracked— much of the digital encryption that businesses and everyday Web surfers use, according to reports based on Snowden's disclosures. The reports describe how the NSA invested billions of dollars, starting in 2000, to make nearly everyone's secrets available for government consumption.

Meanwhile, the U.S. government's computing power continues to grow. This fall, the NSA plans to open a $1.7 billion cyber-arsenal—a Utah data center filled with super-powered computers designed to store massive amounts of classified information, including data that awaits decryption.