Growing backlash to government surveillance

Martha Mendoza
October 12, 2013

From Silicon Valley to the South Pacific, counterattacks to revelations of widespread National Security Agency surveillance are taking shape, from a surge of new encrypted email programs to technology that sprinkles the Internet with red flag terms to confuse would-be snoops.

Policy makers, privacy advocates and political leaders around the world have been outraged at the near weekly disclosures from former intelligence contractor Edward Snowden that expose sweeping U.S. government surveillance programs.

"Until this summer, people didn't know anything about the NSA," said Center for International Security and Cooperation at Stanford University co-director Amy Zegart. "Their own secrecy has come back to bite them."

Activists are fighting back with high-tech civil disobedience, entrepreneurs want to cash in on privacy concerns, Internet users want to keep snoops out of their computers and lawmakers want to establish stricter parameters.

Some of the tactics are more effective than others. For example, Flagger, a program that adds words like "blow up" and "pressure cooker" to web addresses that users visit, is probably more of a political statement than actually confounding intelligence agents.

Developer Jeff Lyon in Santa Clara, Calif., said he's delighted if it generates social awareness, and that 2,000 users have installed it to date. He said, "The goal here is to get a critical mass of people flooding the Internet with noise and make a statement of civil disobedience."

University of Auckland associate professor Gehan Gunasekara said he's received "overwhelming support" for his proposal to "lead the spooks in a merry dance," visiting radical websites, setting up multiple online identities and making up hypothetical "friends."

And "pretty soon everyone in New Zealand will have to be under surveillance," he said.

Electronic Frontier Foundation activist Parker Higgins in San Francisco has a more direct strategy: by using encrypted email and browsers, he creates more smoke screens for the NSA. "Encryption loses its' value as an indicator of possible malfeasance if everyone is using it," he said.

And there are now plenty of encryption programs, many new, and of varying quality.

"This whole field has been made exponentially more mainstream," said Cryptocat private instant messaging developer Nadim Kobeissi.

This week, researchers at Carnegie Mellon University released a smartphone app called SafeSlinger they say encrypts text messages so they cannot be read by cell carriers, Internet providers, employers "or anyone else."

CryptoParties are springing up around the world as well. They are small gatherings where hosts teach attendees, who bring their digital devices, how to download and use encrypted email and secure Internet browsers.

"Honestly, it doesn't matter who you are or what you are doing, if the NSA wants to find information, they will," said organizer Joshua Smith. "But we don't have to make it easy for them."

Apparently plenty agree, as encryption providers have seen a surge in interest.

Pretty Good Privacy, or PGP, a free encryption service was being loaded about 600 times a day in the month before Snowden's revelations broke. Two months later, that had more than doubled to 1,380, according to a running tally maintained by programmer Kristian Fiskerstrand.

Andrew Lewman, executive director of TOR, short for The Onion Router, said they don't track downloads of their program that helps make online traffic anonymous by bouncing it through a convoluted network of routers to protect the privacy of their users.

But, he said, they have seen an uptick.

"Our web servers seem more busy than normal," he said.

Berlin-based email provider Posteo claims to have seen a 150 percent surge in paid subscribers due to the "Snowden effect."

Posteo demands no personal information, doesn't store metadata, ensures server-to-server encryption of messages and even allows customers to pay anonymously cash in brown envelopes-style.

CEO Patrick Loehr, who responded to The Associated Press by encrypted email, said that subscriptions to the 1 euro ($1.36) per month program rose to 25,000 in the past four months. The company is hoping to offer an English-language service next year.

Federation of American Scientists secrecy expert Steven Aftergood said it is crucial now for policymakers to clearly define limits.

"Are we setting ourselves up for a total surveillance system that may be beyond the possibility of reversal once it is in place?" he asked. "We may be on a road where we don't want to go. I think people are correct to raise an alarm now and not when we're facing a fait accompli."

U.S. Sen. Ron Wyden, who introduced a bipartisan package of proposals to reform the surveillance programs last month, told a Cato Institute gathering Thursday that key parts of the debate are unfolding now.

"It's going to take a groundswell of support from lots of Americans across the political spectrum," he said, "communicating that business as usual is no longer OK, and they won't buy the argument that liberty and security are mutually exclusive."