NSA row sparks rush for encrypted email

May 18 2014, by Rob Lever

A new push to encrypt email, keeping messages free from government snooping, is gaining momentum

A new push to encrypt email, keeping messages free from government snooping, is gaining momentum.

One new email service promising "end-to-end" encryption launched on Friday, and others are being developed while major services such as Google Gmail and Yahoo Mail have stepped up security measures.

A major catalyst for email encryption were revelations about widespread online surveillance in documents leaked by Edward Snowden, the former National Security Agency contractor.

"A lot of people were upset with those revelations, and that coalesced into this effort," said Jason Stockman, a co-developer of ProtonMail, a new encrypted email service which launched Friday with collaboration of scientists from Harvard, the Massachusetts Institute of Technology and the European research lab CERN.

Stockman said ProtonMail aims to be as user-friendly as the major commercial services, but with extra security, and with its servers located in Switzerland to make it more difficult for US law enforcement to access.

Encryption is a tool that can help dissident activists avoid detection in places like China or Iran, but the movement has also gained credence in the United States among those who want to stay clear of snooping from the NSA or other intelligence services.

Making encryption easy

"Our vision is to make encryption and privacy mainstream by making it easy to use," Stockman told AFP. "There's no installation. Everything happens behind the scenes automatically."

Even though email encryption using special codes or keys, a system known as PGP, has been around for two decades, "it was so complicated," and did not gain widespread adoption, Stockman said.

After testing over the past few months, ProtonMail went public Friday using a "freemium" model—a basic account will be free with some added features for a paid account.

"As our users from China, Iran, Russia, and other countries around the world have shown us in the past months, ProtonMail is an important tool for freedom of speech and we are happy to finally be able to provide this to the whole world," the company said in a blog post.

Google and Yahoo recently announced efforts to encrypt their email communications, but some specialists say the effort falls short.

"These big companies don't want to encrypt your stuff because they spy on you, too," said Bruce Schneier, a well-known cryptographer and author who is chief technology officer for CO3 Systems.

"Hopefully, the NSA debate is creating incentives for people to build more encryption."

Stockman said that with services like Gmail, even if data is encrypted, "they have the key right next to it .. if you have the key and lock next to each other, so it's pretty much useless."

By locating in Switzerland, ProtonMail hopes to avoid the legal woes of services like Lavabit—widely believed to be used by Snowden—which shut down rather than hand over data to the US government, and which now faces a contempt of court order.

Even if a Swiss court ordered data to be turned over, Stockman said, "we would hand over piles of encrypted data. We don't have a key. We never see the password."

'Dark Mail Alliance'

Lavabit founder Ladar Levison meanwhile hopes to launch a new service with other developers in a coalition known as the "Dark Mail Alliance."

Levison told AFP he hopes to have a new encrypted email system in testing within a few months and widely available later this year.

"The goal is to make it ubiquitous, so people don't have to turn it on," he said.

But he added that the technical hurdles are formidable, because the more user-friendly the system becomes, "the more susceptible it is to a sophisticated attacker with fake or spoofed key information."

Levison said he hopes Dark Mail will become a new open standard that can be adopted by other email services.

Jon Callas, a cryptographer who developed the PGP standard and later co-founded the secure communications firm Silent Circle, cited challenges in making a system that is both secure and ubiquitous.

"If you are a bank you have to have an email system that complies with banking regulations," Callas told AFP, which could allow, for example, certain emails to be subject to regulatory or court review.

"Many of the services on the Internet started with zero security. We want to start with a system that is totally secure and let people dial it down."

The new email system would complement Silent Circle's existing secure messaging system and encrypted mobile phone, which was launched earlier this year.

"If we start competing for customers on the basis of maximum privacy, that's good for everybody," Callas said.