New privacy app takes a page from NSA technology

June 1 2015

The National Security Agency (NSA) headquarters at Fort Meade, Maryland has developed encryption software that will coming to the public in a new app

Before the National Security Agency began complaining about being shut out of encrypted devices, it helped develop software for secure communications that could be adapted by the private sector.

That technology is hitting the public this month in the form of a smartphone application called Scrambl3 from a California startup which

claims its "dark Internet tunnel" thwarts snooping on voice calls and messages.

Scrambl3 was launched Monday as a stand-alone app for Android devices by the startup, USMobile, which describes it as a way to create "trusted connections on untrusted networks."

The system creates the smartphone equivalent of a virtual private network to make messages invisible on the Internet, according to USMobile president and co-founder Jon Hanour.

"We want to provide the most private and most secure mobile program on the market," Hanour told AFP.

"We think we have the best combination of anything that's available today."

Hanour says Scrambl3 adds an extra layer of encryption compared with other secure messaging apps, using a technology stemming from the NSA "Fishbowl" project—technical specifications of which were released in 2012 by the agency.

"The only other network using this is one at the Department of Defense for classified communications," he said.

"If you are not protecting encrypted traffic within a highly encrypted VPN, then you are not secure in today's environment."

No 'backdoor'

While the system was developed in collaboration with the NSA, it has no "backdoor" access for the intelligence agency, according to USMobile.

"We believe the NSA cannot break our encryption," Hanour said.

The Scrambl3 encryption was launched for Android devices first

USMobile will not store voice mails or messages on its servers and will not use the public telephone network, allowing users to bypass surveillance and making data inaccessible to law enforcement or other investigations.

Because of its strong encryption, the software requires a special US export license and cannot be sold to countries such as North Korea, Syria or Iran on a list of sponsors of terrorist activity.

Interestingly, the NSA and FBI in recent months have complained that encryption used by Apple and Google, which will not retain access keys,

would make it more difficult to track down criminals and terrorists.

But Hanour said society has a greater interest in protecting sensitive data such as trade secrets, from snooping.

"If the government has a master key, then it going to make everyone less secure," Hanour said.

"In our brave new world where the details of our lives and businesses are becoming increasingly public through social media, sophisticated marketing techniques and government surveillance, we are seeing a trend toward protecting our privacy."

Hanour and his colleagues began working on the project in 2011 with the telephony group Cyvergence Corporation and decided to spin off an independent company for the effort.

A lawyer's laptop with a sticker reading " National Security Agency monitored device" lies on a table in the courtroom at the Administrative Court in Cologne, western Germany

The effort began before the 2013 revelations from documents leaked by former NSA contractor Edward Snowden.

But he said the Snowden revelations and news of other data breaches underscores the need for better security, for companies, government

agencies and individuals who deal with sensitive information.

"We think there are many state and local and federal agencies, and especially police forces, who would use this," he said.

In addition to the mobile app, USMobile will be able to install encryption software on corporate servers to create secure messaging platforms. Pricing has not been determined, but Hanour said he hopes to offer the service for individual users at around $10 a month.

Bruce Schneier, a cryptographer with Resilient Systems and a fellow at Harvard's Berkman Center, said it was not surprising to see strong encryption technology coming from the NSA.

"From its beginnings NSA has worked on security systems so good that the NSA can't tap into it," Schneier told AFP.

In recent years, however, he said the NSA "has largely been choosing surveillance over security. The exception is the systems they design."