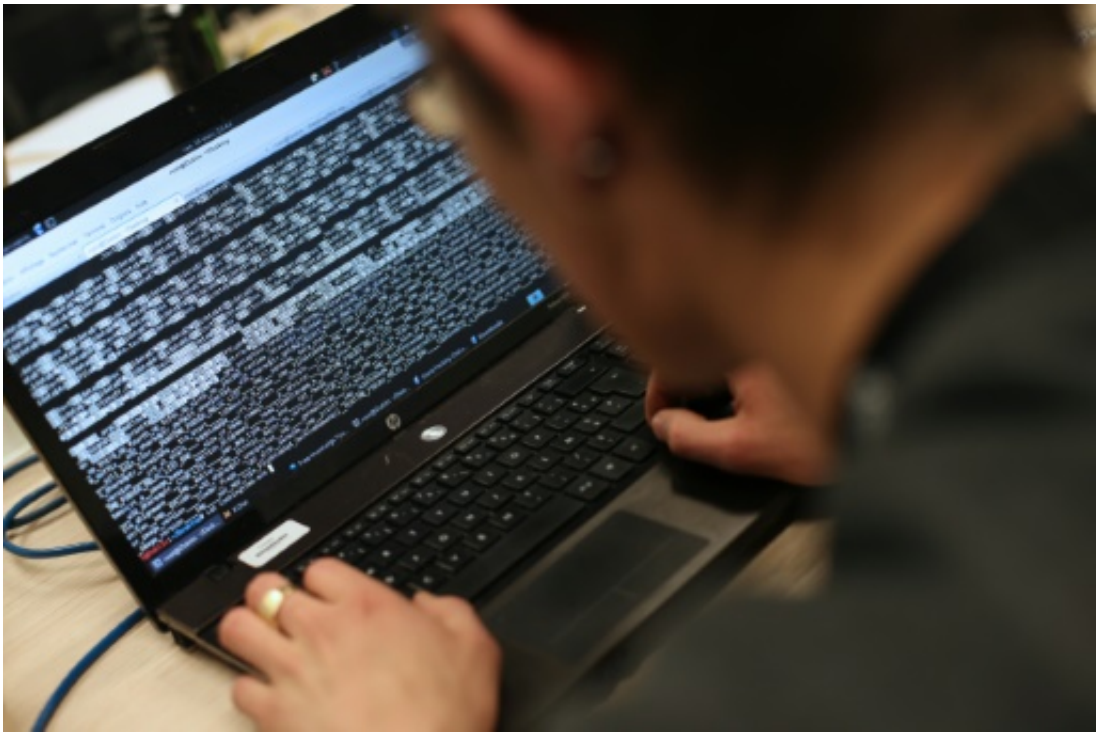
In fight on terror, encryption is double-edged sword

November 21 2015, by Rob Lever



The technology for encryption can keep data and conversations private, making it a double-edged sword that can equally be used by democracy campaigners or violent extremists

Encryption can be a terrorist's tool. But it's also a key for those hunting attackers, and for many others.

The technology for encryption can keep data and conversations private,

making it a double-edged sword that can equally be used by democracy campaigners, law enforcement or violent extremists.

The November 13 attacks in Paris spurred calls for better tools for investigators to track criminals who rely on encrypted communications.

But no solution is readily available that would avoid major impacts on privacy, civil liberties and a wide range of online communications including electronic commerce.

The US government is both a supporter of encryption—funding projects aimed at helping pro-democracy activists—while at the same time pressing for ways to gain access to encrypted data for certain investigations.

"That schizophrenia is inherent in the NSA (National Security Agency) itself," said Sascha Meinrath, who heads the digital rights group X-Lab.

"The NSA is tasked both to secure our communications and to survey our communications."

Interest in encryption has been growing since revelations in documents leaked in 2013 by former US intelligence contractor Edward Snowden describing the NSA's vast abilities to sweep up data.

But officials from the CIA, NSA and FBI as well as lawmakers and local law enforcement leaders have complained that they are "going dark," unable to tap into new encrypted apps and smartphones which may be locked down with keys available only to users.

'We need Silicon Valley'

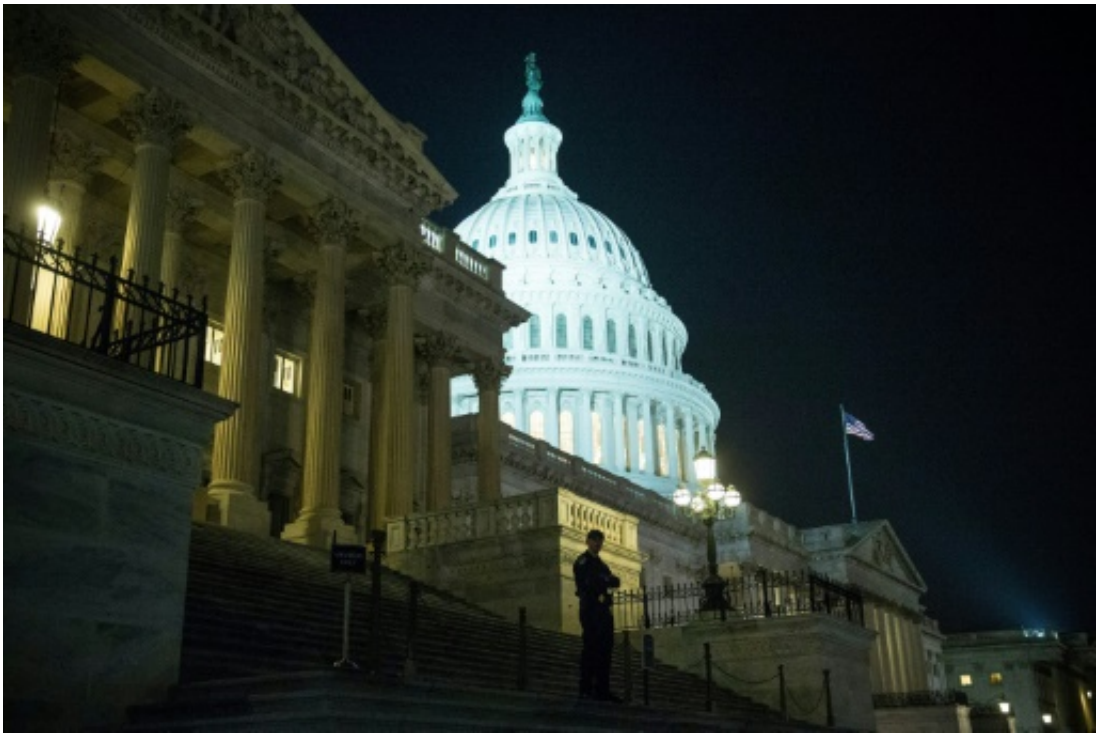
Democratic presidential candidate Hillary Clinton joined the debate,

saying "we should take the concerns of law enforcement and counterterrorism professionals seriously."

"They have warned that impenetrable encryption may prevent them from accessing terrorist communications and preventing a future attack."

Clinton said Thursday that "we need Silicon Valley not to view government as its adversary."

"We need to challenge our best minds in the private sector to work with our best minds in the public sector to develop solutions that will both keep us safe and protect our privacy," she said.



The US government supports encryption while pressing for ways to gain access to encrypted data for certain investigations

But technology specialists in the private sector argue that any "back door" allowing authorities to gain access to encrypted data, could also be exploited by a hacker, or used by repressive regimes as well as democratic ones.

"Anytime you introduce a back door you can't just program it so only one entity can grab that data," said Mike Janke, chief executive of Silent Circle, an app featured on a "safe" list recently circulated by the Islamic State organization.

"Hackers can get into it better than anybody."

Pressure to act

Technology players defend the principles of encryption, saying it is legitimately used to keep data confidential by Fortune 500 companies, government leaders, journalists and dissidents around the world.

Meinrath said encryption "is one of the world's most used technologies for routing around censorship. It enables millions of people to access information and news that they would otherwise not see."

The US government has acknowledged this need by funding projects for secure and encrypted communications through the Open Technology Fund led by Radio Free Asia, and which Meinrath has advised.

Illustrating the complexity of the issue, however, the fund provided more than $1.3 million to the Open Whisper project—whose Redphone and Signal apps have been deemed "safe" by IS for its members to use.

The US military also created the Tor network for encrypted communications, which was developed for secret military communications but is also used now for underground "Darknet"

markets.

Under pressure to act following the Paris attacks, Silent Circle and others took some steps to make it harder for terrorists to use their services.

Janke told AFP the Swiss-based company was "enacting more aggressive back-end payment technology to reduce the likelihood of evildoers" like IS using the service.

Hillary Clinton gives a speech on her approach to defeating the Islamic State terrorist network across the Middle East on November 19, 2015

Telegram, a secure communications app created by Russian Internet guru Pavel Durov, said it had blocked dozens of accounts associated with

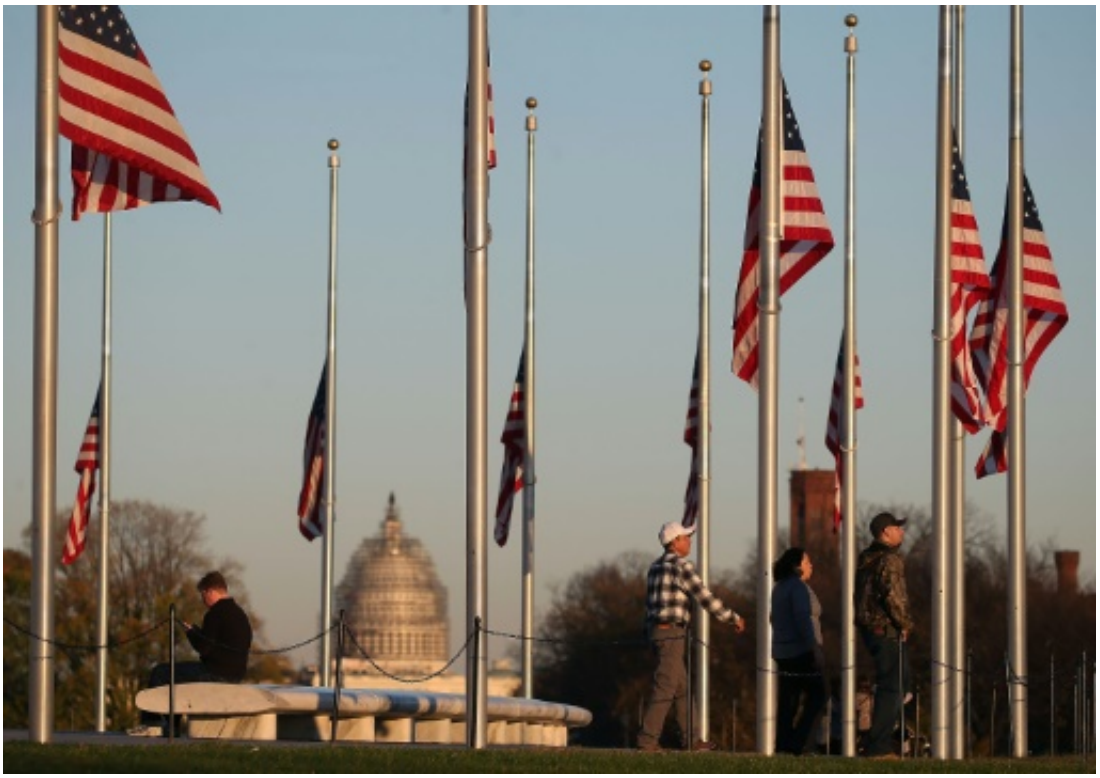
IS that were reportedly being used to spread extremist propaganda.

Activists say the current debate revives the 1990s "crypto war" battle when the government sought a special "key" for Internet communications, before throwing in the towel.

For good or evil

Encryption backers say it is like any other technology—whether it is a car, telephone or gun—which can be used for good or evil.

"Encryption is a security tool we rely on everyday to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety," said Dean Garfield of the Information Technology Industry Council, which represents major tech firms.



The US military created the Tor network for encrypted communications but it is also used now for underground "Darknet" markets

"We deeply appreciate law enforcement's and the national security community's work to protect us," he said.

"But weakening encryption or creating back doors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy."

Jason Healey, a former White House advisor who is now a Columbia University researcher and Atlantic Council fellow, said any new laws on encryption are unlikely to be effective.

"If the terrorists are clever enough to avoid NSA-monitored technology, won't they be smart enough to avoid future NSA-backdoored cryptography and devices?" he wrote in The Christian Science Monitor.

"They will simply switch to non-US software that has more privacy safeguards or is difficult to monitor."