Attacks revive debate on encryption, surveillance

November 17 2015, by Rob Lever

The latest carnage in France has revived concerns that law enforcement and intelligence lack the ability to tap into new communications technologies, such as on smart phones, even with appropriate legal authorization

The deadly Paris attacks have reignited debate on encrypted communications by terror cells and whether law enforcement and intelligence services are "going dark" in the face of new technologies.

The exact means of communication in Friday's strikes were not immediately clear, but media reports have said the Islamic State organization has increasingly turned to encrypted communications and applications to avoid detection.

The latest carnage in France has revived concerns that law enforcement and intelligence lack the ability to tap into new communications technologies, even with appropriate legal authorization.

CIA Director John Brennan, speaking at a Washington forum Monday, warned that some technologies—without specifically mentioning encryption—"make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it."

Brennan echoed concerns voiced by leaders of the FBI and National Security Agency that terrorists are using encryption to hide their tracks.

"I think what we're going to learn is that these guys are communicating via these encrypted apps, right, the commercial encryption, which is very difficult, if not impossible, for governments to break," former deputy CIA director Michael Morell told the CBS program "Face the Nation."

New York City Police Commissioner William Bratton echoed those concerns, saying his department is often frustrated by encryption—which has increased with new smartphones powered by Apple and Google software that provides only the users with keys to unlock data.

"We're encountering that all the time," Bratton told broadcaster MSNBC Monday.

"We have a huge operation in New York City working closely with the

Joint Terrorism Task Force and we encounter that frequently. We are monitoring (suspects) and they go dark. They are going onto an encrypted app, they are going onto sites that we cannot access. The technology has been purposely designed by our manufacturers so that even they cannot get into their own devices."

So far, the major US technology companies have spurned appeals from officials to enable access for key investigations and have stepped up encryption efforts following the 2013 leaks about vast surveillance capabilities of the US National Security Agency.

'Game changing'

Analysts believe there will be renewed debate among security organisations on surveillance and encryption in the wake of the Paris attacks

But in light of the bloodletting in France, the debate may change, observers say.

"Evidence that terrorists were, in fact, using strong end-to-end encryption to kill people could be game-changing in a debate that has heretofore been defined by anxieties about NSA," said Benjamin Wittes, a Brookings Institution fellow who edits the blog Lawfare.

"The tech companies won the first round of the current encryption battles in large measure because the concerns the intelligence and law enforcement community have about 'going dark,' while acutely real to them, are pretty hypothetical on public evidence," he added.

"All that could change in an instant were it to emerge that the Paris attackers were using technology specifically chosen to secure their communications from those charged with stopping terrorist attacks."

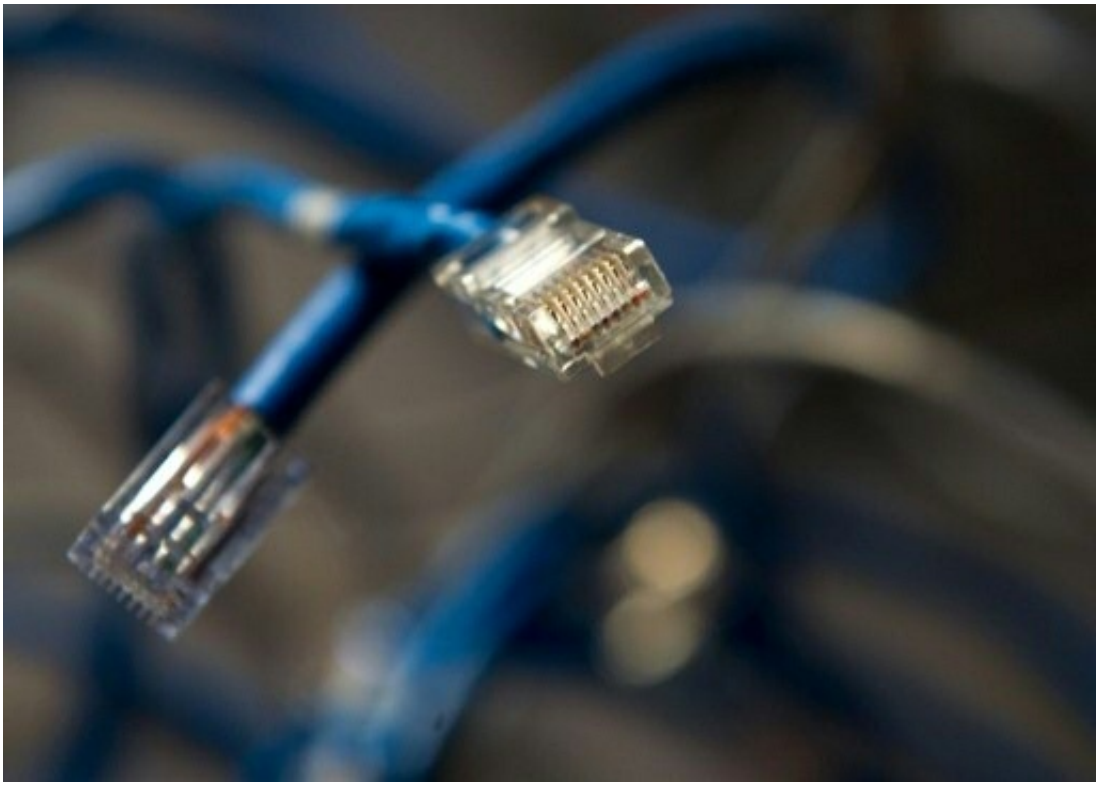
Steve Vladeck, an American University law professor and editor of the Just Security blog, said there will be renewed debate on surveillance and encryption in the wake of the Paris attacks.

"I don't think we know nearly enough yet to assess whether anything about the Paris attacks ought to tilt the scales in the ongoing debate over encryption," he said.

"The most immediate focus of post-Paris discussions of national security law and policy reform is going to be surveillance, with a special focus on encryption and back doors."

But many technology experts and civil liberties activists say allowing special access to law enforcement would weaken online security overall—and could mean activists, journalists and people living under authoritarian regimes would lack the ability to freely communicate.

Good guys, bad guys



Many technology experts and civil liberties activists say allowing special access to law enforcement would weaken online security overall

"We've never been able to create a 'back door' that can discriminate between good guys and bad guys," said Joseph Hall at the digital rights group Center for Democracy & Technology.

Creating special access "would mean engineering vulnerabilities" into these systems, Hall told AFP.

Mark Rotenberg, president of the Electronic Privacy Information Center, said that "there is no evidence so far that encryption thwarted an

investigation" into the Paris attackers.

"It may well be that it was a failure of human intelligence."

Bruce Schneier, a cryptographer who is a fellow at the Harvard Berkman Center for Internet and Society and chief technology officer at the security firm Resilient Systems, said the Paris attacks may be used "to scare people" to weaken encryption.

Schneier said leaked emails from September suggest that the US administration would seek to use a terror attack to get more public support for surveillance.

"They are going to use this to convince people we need back doors," he told AFP.

"It might change the debate because people are scared."