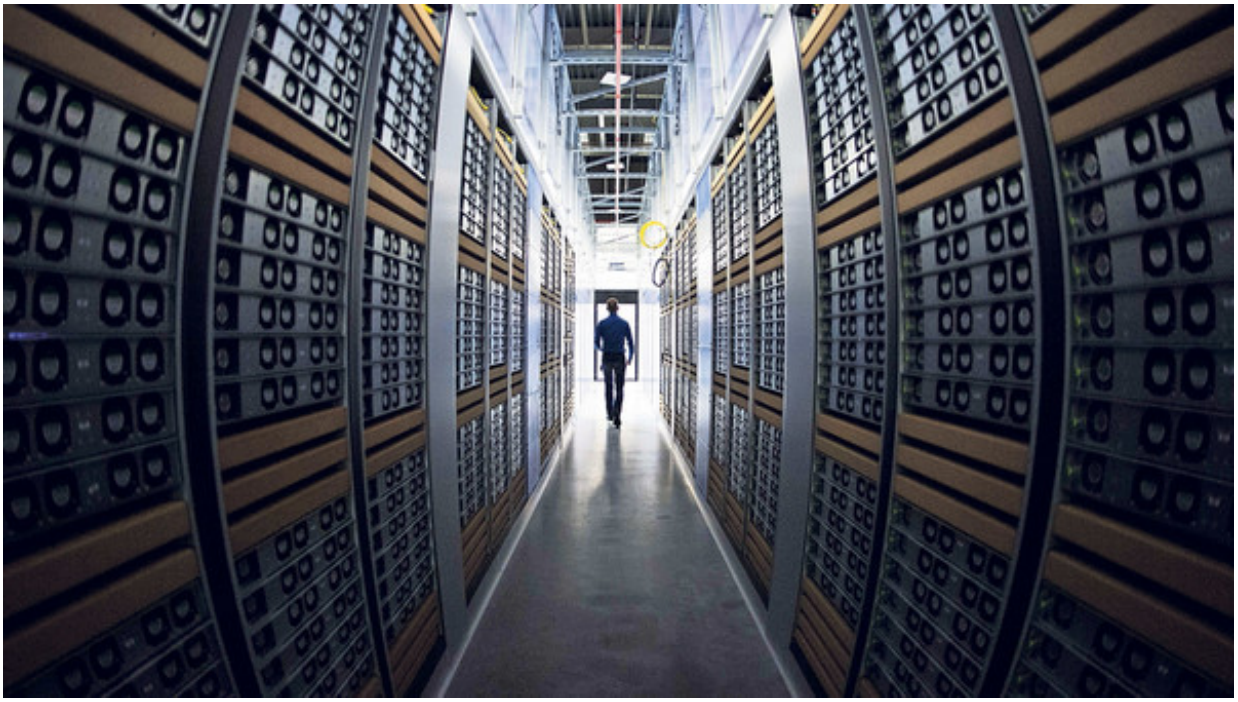
US warns on terrorists' use of encryption

Geoff Dyer in Washington



The Paris attacks are reviving the debate about whether terrorists are taking advantage of encryption technologies that make their communications impossible for law enforcement to read.

The Obama administration said last month that the time was not right for legislation that would force technology companies to find ways to decode messages after facing stiff resistance from the industry.

However, with intelligence agencies in both Europe and the US facing questions about how such a multi-pronged attack could have been planned without detection, the administration and some of its allies in Congress stepped up their criticism on Monday of the proliferation of encrypted messaging.

Since the Edward Snowden revelations in 2013 about snooping by the National Security Agency, technology companies including Apple and Google have strengthened encryption on products used by millions of people and which the companies themselves cannot break.

Industry executives and privacy advocates believe that encryption provides consumers with the best defence against hackers. However, law enforcement agencies have complained that they cannot read messages of terror or criminal suspects even with a court order.

Asked on Monday why the Paris attacks had gone undetected, John Brennan, director of the US's Central Intelligence Agency, warned that there were "a lot of technological capabilities that are available right now that make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need".

He added that it was time for Europe and the US "to take a look and see whether or not there have been some inadvertent or intentional gaps that have been created in the ability of intelligence and security

services to protect the people".

Dianne Feinstein, the California senator and the leading Democrat on the Senate intelligence committee, delivered a scathing criticism of the tech sector on Monday. "I have actually gone to Silicon Valley. I have met with the chief counsels of most of the big companies. I have asked for help and I haven't gotten any help," she said. "If you create a product that allows evil monsters to communicate in this way, to behead children, to strike innocents, whether it's at a game in a stadium, in a small restaurant in Paris, [to] take down an airliner, that's a big problem."

Adam Schiff, another California politician who is the ranking Democrat on the House intelligence committee, said that it was too early to say whether the Paris terrorists had access to encrypted communications but the fact that "we may be going dark" was an "increasing issue".

"Something this big, this sophisticated, with this many players and these kind of devices is something that we should have seen," he said. "But we didn't."

Attorney-general Loretta Lynch is scheduled to testify on Tuesday morning before the House Judiciary Committee, which will question her about the Paris attacks and what steps the agency is taking to help prevent such an event in the US. As part of the hearing Ms Lynch is expected to highlight the problem of encrypted communications and the challenges they pose to law enforcement agencies in pursuing terrorists.

The Federal Bureau of Investigation has been warning for more than a year that the greater availability of encryption technologies was making it harder to track suspects. However, James Comey, the FBI's director, said last month that the administration had "decided not to seek a legislative remedy now", although he said that it "makes sense to continue the conversations with industry".

In depth

As online threats race up national security agendas and governments look at ways of protecting their national infrastructures a cyber arms race is causing concern to the developed world

An email from Robert Litt, the intelligence community's leading counsel, obtained in September by the Washington Post said that the climate in Congress for a law about encryption was "hostile". However, he said that the political mood "could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement".

In recent days, western intelligence officials have been searching databases for information about the suspected attackers and their links with Isis in Syria but have not established firm conclusions about how communications were conducted.

Nathan White, senior legislative manager at Access, a human rights group focusing on digital issues, said that it was "premature and misguided" to be already linking the Paris attacks to encryption.

Initial reporting had suggested that several of the attackers were already on the radar of the intelligence community. "The question should be, 'Why were we not able to connect the dots', not 'How do we get more dots,'" he said.

"