PHYS.ORG

Data encryption in sharp focus after deadly attacks

December 12 2015, by Rob Lever

A view of a makeshift memorial near the Inland Regional Center on December 4, 2015 in San Bernardino, California

With renewed focus on how encrypted messages can be used to plot terrorist attacks, President Barack Obama's administration is stepping up pressure on the tech sector to help in the battle.

Although issues around encryption have been ongoing for decades, the prickly topic has sprung to the fore in recent weeks following killing sprees in Paris and California.

Over the past two years, more sophisticated encryption—notably for smartphones—has become widely available following revelations by former intelligence contractor Edward Snowden about vast US surveillance programs.

But US administration officials as well as local law enforcement are making the case for better access to encrypted data, saying new smartphone and encryption technologies have made it more difficult to thwart "malicious actors."

"We want to strike the right balance. We want to make sure encryption is not used in a way that does allow for dark space for terrorist groups," a White House statement said.

Privacy remains a major counter-argument.

Underlining those concerns, an online petition calling on the administration to avoid weakening encryption got more than 100,000 signatures, requiring a White House reply.

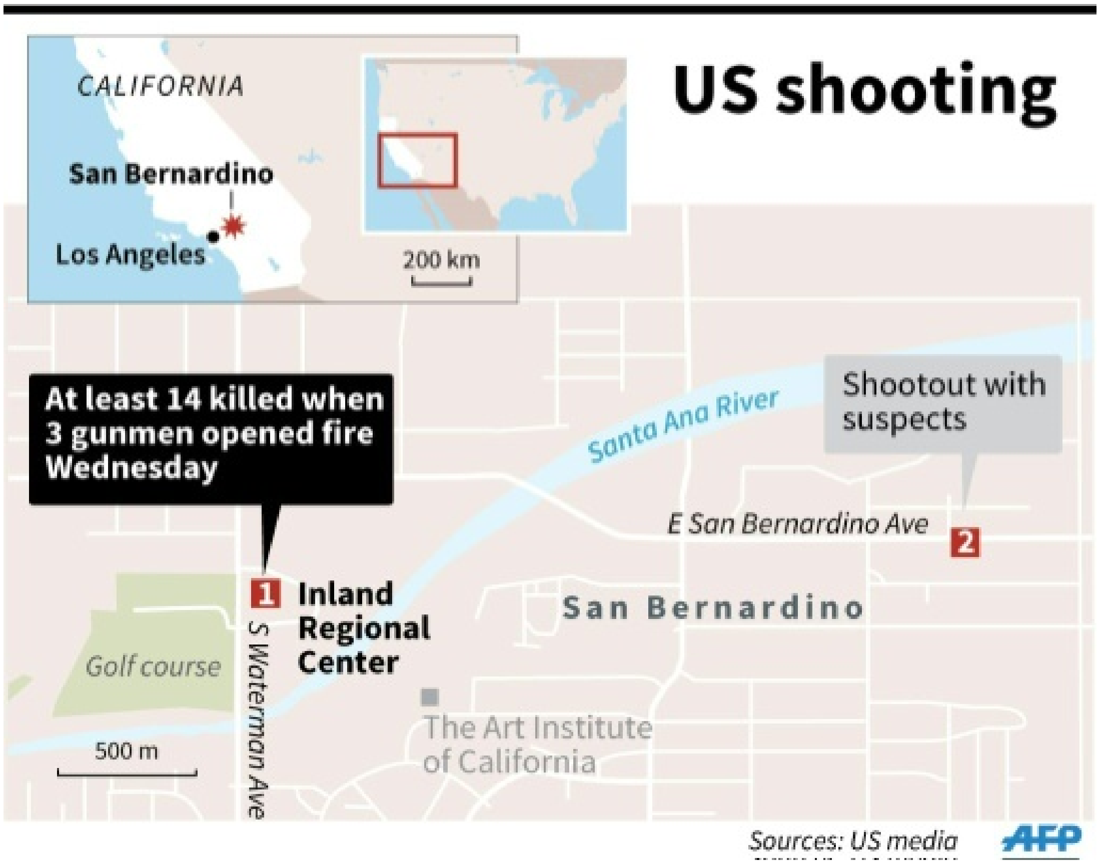
White House chief technology officer Ed Felton and cybersecurity chief Michael Daniel said in response that "American technologists have a unique perspective... and we need them to bring their expertise, innovation and creativity to bear against the threat of terrorism."

Some analysts say the public is though ready to accept improved access for legitimate investigative purposes.

'Back doors'

"This is part of a larger debate since the dawn of the Internet about how much anonymity people should have," said James Lewis, a senior fellow at the Center for Strategic and International Studies, who as a former administration official worked on encryption issues.

Lewis said the debate has been skewed by the use of the term "back door" for law enforcement or intelligence when in fact most tech firms have the ability to decrypt data under certain circumstances.



Updated map of the shooting in the United States in California that left at least 14 killed Wednesday. 90 x 70 mm

"Companies like Google mine this data for advertising purposes," Lewis said.

Darren Hayes, a professor of computer science forensics at Pace University in New York, said one helpful move would be for Apple and Google to roll back their encryption to the level of a year ago to enable access to smartphones with a warrant or court order.

"It worked very well, but Apple somewhere along the line decided it didn't make business sense," he said, adding that tech firms are conscious of their public image and don't want to be seen as tools of law enforcement or the National Security Agency.

At the same time, he said, in New York "there are more than 100 investigations stopped in their tracks because there are phones that can't be analyzed. These are murderers, rapists, pedophiles who are not being prosecuted."

Hayes said that in the current environment, tech firms are not likely to voluntarily make changes to help law enforcement.

"The only way they would be persuaded is through legislation," he said.

FBI Director James Comey told lawmakers the administration "has decided not to seek a legislative remedy at this time," but repeated his warning about "going dark"—losing the ability to track communications over new encrypted messaging systems.

"We believe it must be addressed since the resulting risks are grave in both traditional criminal matters as well as in national security matters," he said.

He added that the government "is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services."

Investigators look at the vehicle involved in a shootout between police and two suspects in San Bernardino, California, on December 3, 2015

Right to privacy

But privacy activists and encryption specialists in the private sector remain firm in resisting efforts to provide special access to investigators.

"Weakening encryption makes us all less secure," says Rainey Reitman of the Electronic Frontier Foundation in a blog post.

"We cannot create a back door, a front door, or any other kind of door for the United States government that cannot be exploited by malicious hackers and other foreign governments."

Activists say encryption offers numerous benefits, such as securing personal or business data and financial transactions, and can help deter smartphone thefts.

Robyn Greene, policy counsel for the Open Technology Institute at New America Foundation, said that "prohibiting companies from selling encrypted devices would not prevent criminals or terrorists from being able to access unbreakable encryption."

Green added that smartphones should have the same privacy protection as other means of communication.

"Police can enter homes with warrants, but there is no requirement that people record their conversations and interactions just in case they someday become useful in an investigation," she said on the Just Security blog.

"The conversations that we once had through disposable letters and in-person conversations now happen over the Internet and on phones. Just because the medium has changed does not mean our right to privacy has."

Citation: Data encryption in sharp focus after deadly attacks (2015, December 12) retrieved 4 May 2024 from https://phys.org/news/2015-12-encryption-sharp-focus-deadly.html