The Washington Post

The Post's View

Paris attacks fuel a fresh debate over encryption

By Editorial Board November 19

THE TERRORIST attacks in Paris have sparked fresh debate about the risks and rewards of encrypted communications in smartphones and other devices and whether law enforcement should have what's called "extraordinary access" in pursuit of criminals and terrorists. President Obama recently decided not to seek legislation to provide such access, but the thorny mix of technology, policy, commerce and privacy concerns remains unresolved and deserves further scrutiny.

Encryption — scrambling messages so they are unreadable except to a person with the key to unscramble them — can protect the large majority of users from cybertheft, intrusions and disruption. The tech giants Apple and Google, as well as some independent software-makers, are creating products with built-in encryption that cannot easily be cracked by law enforcement agencies even with a warrant, although they possess some workarounds. Apple's popular iMessage system over the iOS8 operating system encrypts messages, and the unlock keys are held only by the end users, not by Apple. The tech companies say customers want to protect privacy. But encryption also can protect the communications of terrorists and other criminals.

In the past, the Islamic State has used a heavily encrypted free program known as Telegram for promotion and recruitment. Telegram said it is trying to close down the accounts, but it has not been entirely successful. Little is known about how the Paris terrorists plotted their murder spree; they may have evaded detection by using encrypted means or by avoiding digital channels altogether. The Paris police found an unencrypted smartphone in a trash bin near the Bataclan concert hall that contained the text message "Let's go, we're starting."

Immediately after the attacks, the CIA director, John Brennan, became the latest official to decry encryption on smartphones and other devices, saying terrorists "have gone to school on what it is that they need to do in order to keep their activities concealed from the authorities." The same worry has been expressed by FBI Director James B. Comey. Manhattan District Attorney Cyrus Vance Jr. this week called for legislation giving law enforcement extraordinary access; he said encryption has hindered 111 investigations by his office.

The technology giants and their allies have resolutely insisted that giving law enforcement any kind of extraordinary access would be disastrous, weakening encryption for all. When we suggested earlier that there must be some kind of technical compromise, we were told bluntly: No compromise exists, period. We understand the benefit of encryption, including for citizens living under authoritarian regimes. But we also do not underestimate the risks to the public that terrorists and other criminals may pose. It seems obvious that, if there is a terrible attack in the United States, privacy advocates and tech companies instantly will lose this argument.

We don't have a solution, but it would be in everyone's interest to keep looking for one, before the next catastrophe.

Read more:

The Post's View: The next steps for the White House on encryption

The Post's View: Compromise needed on smartphone encryption

Mike McConnell, Michael Chertoff and William Lynn: Why the fear over ubiquitous data encryption is overblown

---