Why government and tech can't agree about encryption

November 25 2015, byBree Fowler And Tami Abdollah

In this July 30, 2014, file photo, Silicon Valley pioneer and Silent Circle co-founder Jon Callas holds up Blackphone with encryption apps displayed on it at the Computer History Museum in Mountain View, Calif. The Paris terrorist attacks have renewed the debate between law-enforcement officials and privacy advocates over whether there should be limits to encryption technology. (AP Photo/Eric Risberg, File)

Your phone is getting better and better at protecting your privacy. But Uncle Sam isn't totally comfortable with that, because it's also

complicating the work of tracking criminals and potential national-security threats.

For decades, tech companies have steadily expanded the use of encryption—a data-scrambling technology that shields information from prying eyes, whether it's sent over the Internet or stored on phones and computers. For almost as long, police and intelligence agencies have sought to poke holes in the security technology, which can thwart investigators even when they have a legal warrant for, say, possibly incriminating text messages stored on a phone.

The authorities haven't fared well; strong encryption now keeps strangers out of everything from your iMessages to app data stored on the latest Android phones. But in the wake of the Paris attacks, U.S. officials are again pushing for limits on encryption, even though there's still no evidence the extremists used it to safeguard their communications.

While various experts are exploring ways of resolving the impasse, none are making much headway. For now, the status quo favors civil libertarians and the tech industry, although that could change quickly—for instance, should another attack lead to mass U.S. casualties. Such a scenario could stampede Congress into passing hasty and potentially counterproductive restrictions on encryption.

"There are completely reasonable concerns on both sides," said Yeshiva University law professor Deborah Pearlstein. The aftermath of an attack, however, "is the least practical time to have a rational discussion about these issues."

Encryption plays a little heralded, yet crucial role in the modern economy and daily life. It protects everything from corporate secrets to the credit-card numbers of online shoppers to the communications of democracy advocates fighting totalitarian regimes.

At the same time, recent decisions by Apple and Google to encrypt smartphone data by default have rankled law enforcement officials, who complain of growing difficulty in getting access to the data they feel they need to build criminal cases and prevent attacks. For months, the Obama administration—which has steered away from legislative restrictions on encryption—has been in talks with technology companies to brainstorm ways of giving investigators legal access to encrypted information.

But technology experts and their allies say there's no way to grant law enforcement such access without making everyone more vulnerable to cybercriminals and identity thieves. "It would put American bank accounts and their health records, and their phones, at a huge risk to hackers and foreign criminals and spies, while at the same time doing little or nothing to stop terrorists," Sen. Ron Wyden, D-Ore., said in an interview Monday.

Lawmakers on the U.S. Senate Select Committee on Intelligence remain on what they call an "exploratory" search for options that might expand access for law enforcement, although they're not necessarily looking at new legislation.

The FBI and police have other options even if they can't read encrypted files and messages. So-called metadata—basically, a record of everyone an individual contacts via phone, email or text message—isn't encrypted, and service providers can make it available when served with subpoenas. Data stored on remote computers in the cloud—for instance, on Apple's iCloud service or Google's Drive—is also often available to investigators with search warrants. (Apple and Google encrypt that data, but also hold the keys.)

Some security experts suggest that should be enough. Michael Moore, chief technology officer and co-founder of the Baltimore, Maryland-

based data security firm Terbium Labs, noted that police have managed to take down online criminals even without bypassing encryption. He pointed to the 2013 take down of Silk Road, a massive online drug bazaar that operated on the "dark Web," essentially the underworld of the Internet.

"The way they figured that out was through good old-fashioned police work, not by breaking cryptography," Moore said. "I don't think there's a shortcut to good police work in that regard."

Others argue that the very notion of "compromise" makes no sense where encryption is concerned. "Encryption fundamentally is about math," said Mike McNerney, a fellow on the Truman National Security Project and a former cyber policy adviser to the Secretary of Defense. "How do you compromise on math?" He called the idea of backdoors "silly."

Some in law enforcement have compromise ideas of their own. The Manhattan District Attorney's office, for instance, recently called for a federal law that would require smartphone companies to sell phones they could unlock for government searches—in essence, forcing them to hold the keys to user data.

In a report on the subject, the office called its suggestion a "limited proposal" that would only apply to data stored on smartphones and restrict searches to devices that authorities had already seized. Privacy advocates and tech companies aren't sold, saying it would weaken security for phones that are already too vulnerable to attack.

Marcus Thomas, the chief technology officer at Subsentio and former assistant director of the FBI's operational technology division, argued that it's too late to turn back the clock on strong encryption, putting law enforcement in a "race against time" to obtain investigatory data

whenever and wherever it can. But he urged security experts to find ways to help out investigators as they design next-generation encryption systems.

The idea of allowing law enforcement secure access to encrypted information doesn't faze Nate Cardozo, a staff attorney for the San Francisco-based Electronic Frontier Foundation—provided a warrant is involved. Unfortunately, he says, cryptographers agree that the prospect is a "pure fantasy."