THE HILL

December 14, 2015, 11:00 am

Paris, San Bernadino, law enforcement and encryption

By Rep. Jerry McNerney (D-Calif.), Rep. Bill Foster (D-Ill.), Ronald Rivest and Martin Hellman

The terrorist attacks in Paris followed by the Dec. 2 mass shooting in San Bernardino have sickened us all and forced us to ask what more might be done to prevent future such disasters. One concern that has been raised is that terrorists and criminals may have used encryption to "go dark," so that our law enforcement and national security personnel could not listen in on what they were planning. The Paris attacks led FBI Director James Comey, CIA Director John Brennan, Manhattan DA Cyrus Vance, and others to renew their call for "exceptional access" – the ability to unlock encrypted data on devices made by companies such as Google and Apple.

Sounds reasonable, right? But, closer examination reveals that providing that kind of access may not be possible, and if it were, it would open up vulnerabilities that would make us less safe in other ways. Let us explain.

Security agencies must precisely define and specify what they want. So far, this is not the case. Neither we nor any others who have studied cyber security can see how to accomplish what the agencies say they want.

The current request has many characteristics in common with one made twenty years ago by the Clinton administration, but was rejected by a National Research Council (NRC) committee convened at the request of Congress. The NRC committee included a former deputy director of the National Security Agency and a former attorney general, so both law enforcement and intelligence interests were represented.

One of us (Hellman) served on that committee, and remembers spending a significant amount of time trying to decipher that earlier proposal – then dubbed "key escrow." Then, as now, the government's request was reasonable sounding but did not provide enough details. The committee's final recommendation reflected the need for more information: "To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses." Basically, the committee suggested that the government design such a system for use in its programs and come back if it could figure out how to solve several problems. It never did.

We see four major challenges that must be addressed by the current demands for exceptional access.

First, how would it work internationally? Twenty years ago, the US would have been happy to hold everyone's escrowed keys, but it's highly unlikely that other nations would have agreed to that. In today's world, it is not clear who should have the power to grant exceptional access and how that power would be shared internationally.

Second, if our government were able to demand exceptional access when allowed by its laws, then governments with poor human rights records would seem able to do the same to suppress legitimate dissent.

Third, exceptional access introduces vulnerabilities to otherwise secure systems. A July report ("Keys Under Doormats"), authored by 15 cyber security researchers including one of us (Rivest), noted that exceptional access would add significant complexity, and thereby increase the risk of unforeseen cyber weaknesses. For example, a set of backdoor keys is a very high value target for bad actors.

And lastly, if American companies implement exceptional access in their devices, how greatly would that damage their international markets? How many customers would move to products made outside the US, without exceptional access? This would cost jobs and, more importantly for preventing future terrorist attacks, make it more difficult for US agencies to obtain information in appropriate circumstances.

Proponents of exceptional access may disagree with our concerns. For example, the just released Manhattan DA's report claims that even repressive foreign governments, "also would have to go through lawful processes in the U.S." to gain access to encrypted information.

Rather than trying to settle such complex questions in dueling op-eds written in the emotionally charged aftermath of the recent attacks, we recommend that national security will best be served by a deliberative but expedited study, undertaken by experts in cyber security.

Fortunately, just such an NRC study was in the planning stages prior to the recent tragic events. This new NRC study, like the one twenty years ago, will have a balanced committee, representing law enforcement, national security, commercial, and privacy interests.

Waiting for the results of that study will reduce the risk of harming our national security by taking hasty action while logic is overpowered by our emotional response to the horrific tragedies that just unfolded.

McNerney represents California's 9th Congressional District and has served in the House since 2007. He sits on the Energy and Commerce and the Veterans' Affairs committees. Foster represents Illinois' 11th Congressional District and has served in the House since 2008. He sits on the Financial Services and the Science, Space and Technology committees. McNerney and Foster) are the only members of Congress with Ph.D.'s in technical subjects (math and physics respectively). Rivest and Hellman led the two teams of researchers, at MIT and Stanford, that revolutionized modern encryption.