# Making sense of the encryption debate

December 22 2015, by Matthew Mcdonald

Credit: AI-generated image (disclaimer)

Last week, candidates in both the Republican and Democratic presidential debates offered some interesting views about the Internet. Whether it was Donald Trump suggesting that parts of the Internet be closed, saying "I would certainly be open to closing areas where we are at war with somebody," or Hillary Clinton calling on government and tech companies to join together in "a Manhattan-like project," tech policy and its place in the national security dialogue took center stage.

To better understand the encryption debate, we spoke with Daniel Wichs, an expert in modern cryptography and an assistant professor in the College of Computer and Information Science at Northeastern.

## Part of the encryption debate seems to center around requests by government for tech companies to build "backdoors" into their encrypted technology. What is an encryption "backdoor"?

An encryption backdoor could be inserted into software and hardware implementations of encryption so as to give the government access to the encrypted data. It is important to keep in mind that sophisticated illegitimate actors could always use unsanctioned implementation of cryptography that don't contain a backdoor and therefore even this solution would not be a silver bullet to allow the government to read all encrypted communication.

## Doesn't creating a backdoor in and of itself defeat the purpose of encryption—which is meant to offer security—thus creating vulnerability for everyone?

In theory, it would be possible to create a backdoor that would only allow a government agency which has a "master secret key" to decrypt all encrypted data. The encrypted data would remain secure from the point of view of everyone else. However, in practice, such solutions would be extremely difficult to implement properly and could result in catastrophic losses of security if the master secret key were ever leaked. It could undermine the public's trust in secure communication and turn people away from technology products made by U.S. firms that would be forced to implement such backdoors.

## During the Democratic presidential debate, Hillary Clinton suggested that tech companies and government join together in "a Manhattan-like project" to address this issue. Is that practical—or even realistic?

People often have a hard time believing that computer security could be more difficult to achieve than building the atom bomb or getting to the moon. But there are good reasons why security is so hard to implement correctly. Most importantly, unlike the other examples, there is no simple "test" to check that security works. We can never be sure. So even if the government claimed that the master secret key is being stored and used securely, the public could never verify this claim.

Provided by Northeastern University