

Tech giant [Apple is standing firm behind](#) its decision to [refuse a US court order](#) to help the FBI gain access to the iPhone used by one of the shooters in last year's mass killing in California.

Fourteen people were killed and 22 seriously injured in a shooting in San Bernardino, on December 2, 2015. The incident was declared an [act of terrorism](#) .

The FBI has an iPhone 5C belonging to one of the shooters, but it does not have the necessary security code set by the user to unlock the phone. It wants Apple to create and provide it with [firmware](#) that would allow it to bypass the security features that protect the privacy of iPhone users.

Apple CEO Tim Cook has published “ [A Message to Our Customers](#) ” explaining why the company is not complying with the request.

Heated debate

It's a topic that has been the subject of much debate over the past few days, with supporters for both sides. Many of Apple's tech rivals have sided with the company, though Microsoft founder Bill Gates says companies [should be forced to cooperate](#) with law enforcement agencies in terrorism investigations.

From the FBI's perspective, the contents of the phone may provide crucial clues, evidence and possibly even contact information of other terrorists and extremists.

From Apple's point of view, creating firmware that has a backdoor could have significant impact on the security and privacy of its customers, because the US government would then have the ability to gain access to any iPhone in its possession.

In the wrong hands, this special firmware could be used to gain access to sensitive information

on any iPhone. These devices are more versatile than ever before and are likely to contain anything from email, messages and contacts, to financial and credit card information.

Understandably Apple is firmly opposing compliance with this order. Because compliance could affect its reputation and result in loss of consumer confidence. There may also be international implications; would this firmware only work on US-issued devices? How might this affect international privacy laws?

We've had back doors before

This wouldn't be the first time the US government has had a back door into secure systems.

In the 1980s, the US National Security Agency (NSA) developed an algorithm called “[Skipjack](#)”. Using an encryption device called the [Clipper chip](#), which had a built in back door, Skipjack allowed law enforcement agencies to gain access to encrypted data and was intended for use by telecommunications providers.

The chip was introduced in 1993 and met with significant backlash and low adoption. It was defunct by 1996.

And in 2013, the [New York Times](#) published a story about how an encryption algorithm, called Dual Elliptical Curve Deterministic Random Bit Generator (Dual_EC_DRBG) contained a back door for the NSA.

People who used the algorithm, which could be any organisation that had the algorithm included as part of security devices or software they acquired, such as those that utilised the [RSA Security BSAFE encryption libraries](#), were urged to stop using it.

What now for the FBI?

What other options does the FBI have? Could there be a place for ethical hackers to attempt to

Hacking the terror suspect's iPhone: what the FBI can do now Apple says 'no'

Written by The Conversation USA

break into the iPhone? Would commissioning ethical hackers for this purpose itself be ethical?

Although Apple's iOS firmware has already undergone significant testing by both Apple and the public, it is possible that vulnerabilities still exist.

One such vulnerability, which allows hackers to [bypass the lock screen](#) using Siri, was revealed last September. Although it only provided access to contacts and photos, it demonstrates that flaws in firmware can exist. In the FBI case at hand, photos and contacts may be useful evidence.

There is also the possibility that an ethical hacker may be able to reverse engineer the firmware. Doing this is explicitly forbidden by the [Apple iOS Software license agreement](#) so the ethics of doing it would be questionable.

Could it be justified given the US government would back the effort for the sake of national safety?

Any attempt to break into the device comes with its risks. Simply trying to brute force the security code by inputting every password combination would likely result in the [device being erased](#), so it is important to preserve the device.

It would at least be necessary to maintain the current state of the device in some way. So, if a way of duplicating the device was created, it would be possible to use a brute force attack against its copies, without affecting the original phone.

Maintaining the forensic integrity of the device and not damaging it is of the utmost importance, something that [was not demonstrated](#) when the FBI attempted to access the iCloud account of the perpetrators.

It is also necessary for Apple to be able to prove that the back door maintains the integrity of the data. If this process becomes part of any court proceeding, it is highly likely that Apple would be called upon to prove this in open court.

It must already realise this and be very concerned about having to do so, as it would expose a great deal of proprietary information that it would not want to see in the public arena.

No hacking by the FBI?

One must ask why the FBI (or US government) doesn't already have the ability to gain access to the encrypted data. It seems likely that with the supercomputers in its arsenal, and the funding available to it, the agency can take a copy of the encrypted data and attempt to decrypt it.

Given the standard encryption on iOS devices is [AES-256](#) (approved and used by the NSA for storing top-secret data), and the key is fused in an unreadable format to the device, the amount of time to decrypt and the costs involved are likely to be the issue.

It's also important to consider whether there should be any automatic right for any government to be able to read (or decrypt and read) any communications or stored data.

Whenever government ministers are interviewed, they seem to start with the presumption that they have the right to do this, yet that right is not established.

So it's probably easier and more cost effective for the US government to try to get Apple to create a back door, despite the problem of Apple refusing to do so.

Creating this precedent would allow this process to be repeatable and to occur whenever the US government required. Perhaps Apple doesn't want the same fate as Clipper and Dual_EC_DRBG.

Hacking the terror suspect's iPhone: what the FBI can do now Apple says 'no'

Written by The Conversation USA

Georg Thomas is affiliated with ISC2, ISACA, ISSA EC-Council & ACS.

Read more <http://theconversation.com/hacking-the-terror-suspects-iphone-what-the-fbi-can-do-now-apple-says-no-55135>