Written by Marco Attard
19. February 2016

An encrypted iPhone stands in the way of the FBI investigation over the 2 December 2015 San Bernardino mass shooting-- one Apple refuses to unlock in the name of protecting user data.

To put a long story short, following the discovery of ISIS involvement in the San Bernardino attack the FBI found an iPhone belonging to one of the attackers. As law enforcement agencies tend to, the FBI wants to go through the data inside the device, but it requires a means to break the iPhone's built-in encryption, specifically by modifying iOS security to allow unlimited unlocking attempts, as well as allowing "brute force" attacks to discover the correct PIN.

The FBI insists the software will be used once on just the device in question, but Apple refuses to uphold such a request, saying it creates a precedent in the breaking of its devices' security.

“The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers,” Apple CEO Tim Cook writes in an open letter to customers. “We oppose this order, which has implications far beyond the legal case at hand.”

Cook minces no words in his description of the FBI's demands-- he says they not only represents a "chilling" privacy breach, but would lead to the building of a "dangerous" iPhone security backdoor.

“The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe," the letter continues.

In turn the US Justice Department appears to paint the company as something of a terrorist sympathiser, stating "it is unfortunate that Apple continues to refuse to assist the department in obtaining access to the phone of one of the terrorists involved in a major terror attack on U.S. soil."

Thankfully Apple has a number of allies on its side-- including Google CEO Sundar Pichai, who took to Twitter to show his support.

"We know that law enforcement and intelligence agencies face significant challenges in protecting the public against crime and terrorism," Pichai says. "We build secure products to keep your information safe and we give law enforcement access to data based on valid legal orders. But that's wholly different than requiring companies to enable hacking of customer devices & data. Could be a troubling precedent."

Also showing support is the Information Technology Industry Council (ITI), stating "our fight against terrorism is actually strengthened by the security tools and technologies created by the technology sector, so we must tread carefully given our shared goals of improving security, instead of creating insecurity."

Will world governments back down in their requests for security weak enough for their law enforcement agencies to crack? Surely not. So it is heartening that Apple is fighting the good fight for backdoor-free encryption, and letting regular customers know there is no such thing as a means for securing supposed good guys' data secure while keeping bad guys in plain sight...

Go Apple Message to Customers

Go DOJ Asking Apple for Access to One Device (Reuters)

Go Sundar Pichai on Twitter

Go ITI Responds to Apple Court Order Ruling