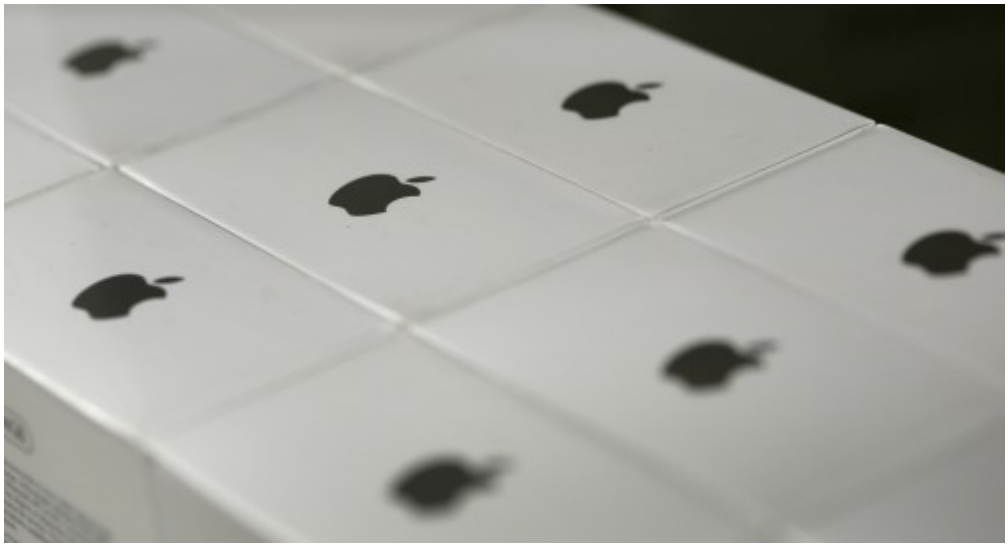
# Apple is right to fight encryption court order as Congress dithers

**Matt A. Mayer**
February 17, 2016 10:52 am | *AEIdeas*

With news yesterday that a US District Court has ordered Apple (http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html) to help the Federal Bureau of Investigation unlock the smartphone of San Bernardino terrorist Syed Rizwan Farook, the battle between the consumer and privacy benefits of encrypted technology and the needs of law enforcement to "see" what terrorists are saying and doing behind the encrypted technology is again being played out publicly.

I simply cannot state in more unequivocal terms that having this critically important debate in public provides far too much clarity to our enemies — the end result being that terrorists will only use the technologies and applications of foreign companies. Encryption won't leave law enforcement in the dark; their lack of subpoena power over those foreign companies will.



REUTERS/Michaela Rehle.

As I stated a month ago, Congress must launch a national commission (https://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf) as soon as possible so we can have this vital discussion in a manner that fully airs the equities of all parties, but in a venue beyond the eyes and ears of terrorists.

Without a full national commission debate on the issues, Apple is right to oppose the FBI's efforts (http://www.apple.com/customer-letter/) in this case. As Apple CEO Tim Cook notes:

> The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. 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.
>
> We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.
>
> …
>
> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.
>
> Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the US government.

If US companies are going to be forced to create back doors or help the federal government hack into the encrypted technology of Americans, that mandate should come from a law passed by Congress and signed by the president. It most certainly should not come from a magistrate judge in a district court in central California based on a statute from the 1700s.

I hope this development spurs Congress to act on the national commission idea.