Apple was instructed by the FBI to build a version of IOS that would let the FBI install that version on a terrorist's phone enabling it to use a brute force method of pushing through every possible combination of passwords into the phone until it unlocked the phone. The goal is to find out if there is anything of value to the FBI's investigation into a horrific terrorist act.

If Apple were to comply with the order, it is important to note that there is no certainty that anything at all would be accomplished.

If the terrorists in possession of the phone used a variety of letters, numbers and symbols in their password, it could take minutes (if very lucky) or years to uncover the pin and unlock the phone.

Even if they were able to unlock the phone, there is no assurance that any 3rd party applications that the terrorists used were not still further encrypted and not defeat able. The FBI would be able to get into anything hosted by Apple's apps and systems, but not necessarily the 3rd party apps or systems. So while Apple has taken on the responsibility of the first step, theirs is potentially not the last step.

All of this is moot right now because Apple has refused to comply with the order. Here is Apple's response .

Here is my response to Apple's refusal:

**Amen. A standing ovation**. They did the exact right thing by not complying with the order. They are exactly right that this is a very, very slippery slope. And while the FBI is attempting to be very clear that this is a one off request, there is no chance that it is. This will not be the last horrific event whose possible resolution could be on a smart phone. There will be many government agencies that many times in the future, point to Apples compliance as a precedent. Once this happens, we all roll down that slippery slope of lost privacy together.

To those that say that Apple should comply, I say this:

**Every tool that protects our privacy and liberties against oppression, tyranny, madmen and worse can often be used to take those very precious rights from us. But like we protect our 2nd Amendment Right, we must not let some of the negatives stand in the way of all the positives. We must stand up for our rights to free speech and liberty**.

**Speech can only be free when it is protected. We are only free when we can say what we feel we must in any manner of private or public that we choose. We have a right to protect our speech from those, domestic or otherwise, who may watch or monitor us. Which is why encryption is vitally important to all of us.**

**If you think its bad that we can't crack the encryption of terrorists, it is far worse when those who would terrorize us can use advanced tools to monitor our unencrypted conversations to plan their acts of terror.**

I'm not being paranoid. Encryption is easy. It is like wearing a seatbelt in your car. For years we didn't. Then we did and it was smart. Encryption is a simple step that Apple and others have helped us take to protect us. It's not paranoia. It is smart.

Now back to Apple. What I thought was particularly interesting about Apple's letter to its customers was the opening it left when it wrote:

"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 U.S. government."

**Apple is signaling to us that the real problem here is the use of the All Writs Act**. According to this article on the All Writs Act:

**"The All Writs Act is only applicable if no statute, law or rule on the books to deal with the specific issue at hand.**"

This of course makes the Act a catch all for anything for which there is no law. **What is the solution to this problem ? Pass a law that deals with this issue.**

The issue is not Apple's. It is not even the FBI's. The issue is that as often happens, technology speeds past our ability to adapt or create new laws that match the onslaught of daily technological change. Typically, I am for fewer laws rather than more, but I'm also pragmatic. We should be asking our lawmakers to enact a law that fits the need of this situation and situations like this so rather than being on an eternally slippery slope of privacy violations hidden behind the All Writs Act, we have a law that will truly limit the circumstances where companies like Apple can be compelled to help a government agency crack a device.

What I would propose is this:

A company can only be compelled to remove any type of security or encryption from a smartphone or tablet, and only a smartphone or tablet, under the following circumstances:

1. There has been an event, with casualties, that has been declared an Act of Terrorism
2. There is reason to believe that the smartphone was possessed by a participant in the Act of Terrorism.
3. The smartphone must have been on premise during the event.
4. The terrorist who was in possession of the smartphone or tablet must be deceased.

It would seem to me that if such a law could be proposed and passed, then the All Writs Act would no longer apply. By eliminating the All Writs Act as a catch all then we significantly flatten out the slippery slope. I'm not saying we will completely eliminate all privacy issues. We won't. I'm not saying there isn't risk of unintended consequences. There always are when we ask politicians to fix complex problems.

I'm also cognizant of the possible hypocrisy of saying that we need to protect our privacy and liberty even when its painful and at the same time suggesting that we create a law that could reduce those protections.

And for the sake of discussion, let me give you a hypothetical to think about.

**What if Apple had started a business that charged $100 to unbrick stolen phones ? Would anyone have complained ?  No one but the most astute privacy advocates would even notice. No one in the general public would care. No one would be talking about it or debating it. It would be a non-event.**

Even so, this is not an easy topic  and there are no easy solutions.  But we certainly learn more when we talk about it than when we shout about it. I'm hoping this blog post gets us talking.

As always, I'm happy to discuss on Cyber Dust at BlogMaverick