In this country we have rights. Under the 6th Amendment we have very specific rights

“In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.“

In the current case facing Apple, the terrorists who had possession of the phone are deceased. However, in one of the next times Apple is called upon to open up a phone to enable access, chances are good that the person in possession of a phone during an illegal and possibly heinous act will be alive, be an American citizen and demand “to have the Assistance of Counsel for his defence”

In the event Apple loses the current case to the FBI, setting a precedent that they can be compelled to unlock phones for the FBI and other government agencies, each and every defendant in such cases will have the assistance of counsel for their defense. W**hat do you expect every defense lawyer to do in order to protect their client who has had a phone opened** ?

Once the phone is “cracked” by Apple or any device or Operating System developer, **whatever is found by the FBI or whatever government agency is involved, is going to be labeled “planted” or false evidence.** The defendants lawyer is going to scream as loud as they can that whatever was found was not originated by their client. That Apple, in cahoots with the government agency, modified their software to not only unlock the phone, but to also write to the device everything the government agency needs to gain a conviction. Pictures. Texts. Logs. Files. Videos. All originated and/or imported by the code in order to gain a conviction.

The best way to disprove this allegation by the defense attorney ?

Line by line publication of the code used to open it. Reviewed by who knows how qualified and how many “experts” who will pass judgement based upon who paid them. Possibly a line by line presentation of the code to a jury of the defendant’s peers.

Yes, the FBI and Apple would do everything possible to try to stop this presentation, but what if they can not ?

Which is exactly why Apple must win the current case against the FBI. There is a near ZERO chance that the code created by Apple to break into their phones can stay private under current laws.

I also want to address the notion that we let the police or government agents into our homes or that we allow some of our digital data to be acquired using warrants and subpoenas. The difference is in the ability for a defense attorney to be able to determine whether or not physical or digital evidence is false evidence.

With physical evidence, there are always risks of planted evidence, but the processes are in place to contest that evidence.

With digital evidence as direct data, the best, if not only way to prove that the code was not written to plant digital evidence is by showing the code. Which is exactly why I think this Apple vs the FBI case is nothing like any of the current search and seizure examples being given in the media.

In those examples, the software that creates, collects or aggregates that data can be presented to an open court without risk.

Want to see the devices, code and databases that collect, process and store your Easy Pass driving data ? No problem. Seeing the process doesn’t open a door for you to hack into it and change it. A defense attorney can question the credibility or accuracy of that data and no one else except Easy Pass users are impacted or care. The same concept can be applied to the phone meta data about us that is collected by the phone companies, our social media footprint, whatever. We may not like it. In fact we may hate it, but reviewing and questioning the process or the data doesn’t create risk if that specific code or process is presented in court.

If Apple, or any digital device or Operating System provider has to write code that breaks into their own phones and then present that code in open court to prove that the code is clean and has not planted digital evidence, then the door is wide open for bad actors to do as they please to our devices. No one can play whack a mole with code fast enough to keep them out.

All that said, there is a possibly better option if we only had lawmakers who cared more about solutions than grandstanding. We have 3 Senators running for President and not one has moved a fingernail to even begin to deal with this issue let alone find a solution. That is sad in and of itself.

What should they propose ? As I wrote in a previous blog post, lawmakers should be working very quickly to write and get passed a law that limits the scope of what Apple must respond to. Here is what I suggested:

“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, currently at the heart of the Apple vs FBI dispute 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.

More importantly, passing this law or something similar gives both Apple and the FBI a means to resolve the dilemma they face. Apple could comply with at least the hope that the circumstances under which they will be forced to create software to open a device is strictly limited in scope.

As always, this is my opinion. I'm not an attorney, so I welcome all constructive criticism and feedback so i can become smarter about the subject at hand. You can reach me to discuss 1 on 1 on the Cyber Dust app under user name Blogmaverick