Written by **C. Mitchell Shaw** on October 19, 2016

DOJ Gets Warrant to Force People to Use Fingerprints to Unlock Their Phones

As more and more people use encryption to protect their data, surveillance hawks at all levels — local, state, and federal — continue to seek ways around the privacy protections offered by that encryption. A recently published court filing from California shows that the hawks are stooping to new lows in their treatment of the constitutional protections afforded to people's data.

Forbes is reporting on an application for a warrant by U.S. Attorney Eileen Decker in the U.S. District Court for the Central District of California on May 9, 2016 to allow "law enforcement" officers serving the warrant to "depress the fingerprints and thumbprints of every person who is at located at the subject premises during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the subject premises and falls within the scope of the warrant."

Although the warrant itself and the other court documents are not available to the public, the memorandum is more than enough to show that the hawks have overstepped any reasonable line of protection in their attempt to get around both the Fourth and Fifth Amendments. Since those who have been used to taking the easiest path of mass surveillance see encryption as "a threat to law enforcement efforts" and "a boon to dangerous criminals," they demonstrate that they are more than willing to sacrifice liberty and privacy to attack that encryption. Never mind that normal, everyday non-criminals use encryption to protect their data from both criminal hackers and overreaching government agents.

After it became obvious that the FBI would lose its case to force Apple to create a backdoor into the encryption of devices running iOS 8 and above, the agency backed down. It is obvious, though, that the surveillance hawks simply continued to look for ways to pervert the law in their quest for circumventing encryption. This new low, though, is so far off track and without precedent that it should be seen on its face as an attack on the very fabric of the Constitution.

Besides the fact that the application for the warrant seeks to force people to "depress the[ir] fingerprints and thumbprints" and unlock their devices (which in and of itself would violate the Fourth and Fifth Amendments), the memorandum itself admits that the warrant is for a fishing expedition to

gain evidence the government does not even know about from the unknown devices of suspects it cannot even identify. The document states:

> While the government does not know ahead of time the identity of every digital device or fingerprint (or indeed, every other piece of evidence) that it will find in the search, it has demonstrated probable cause that evidence may exist at the search location, and needs the ability to gain access to those devices and maintain that access to search them.

That is a far cry from the Fourth Amendment, which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Electronic Frontier Foundation's senior staff attorney, Jennifer Lynch, agrees. She told *Forbes*, "It's not enough for a government to just say we have a warrant to search this house and therefore this person should unlock their phone. The government needs to say specifically what information they expect to find on the phone [and] how that relates to criminal activity." She added, "The warrant has to be particular in how it describes the place to be searched and the thing to be seized and limited in scope. That's why if a government suspects criminal activity to be happening on a property and there are 50 apartments in that property, they have to specify which apartment and why, and what they expect to find there."

Furthermore, considering that judges issue warrants for intrusive searches based on no more probable cause than a suspect drinking tea and shopping at a gardening store, it is clear that warrants aren't what they used to be.

Forbes reported that the Department of Justice refused to comment, but the warrant was served. Whether anything of value was found is both unknown and irrelevant. This miscarriage of justice demonstrates a lack of respect for the rule of law.

This appears to be part of a new tactic by the surveillance hawks. Last month a case presented itself as an opportunity for the FBI to try again where it had failed after the San Bernardino shooting. After Dahir Adan stabbed 10 people in a Minnesota mall on September 17, 2016, the FBI recovered his iPhone, which was encrypted. In a press conference on October 6, FBI special agent Rich Thorton indicated that there would be more attempts to force Apple to provide a backdoor into its iOS platform. He said, "Dahir Adan's iPhone is locked. We are in the process of assessing our legal and technical options to gain access to this device and the data it may contain." Translation: Brace yourselves for another round of FBI vs. Apple.

This warrant application from May is a clear sign that the hawks have no respect for either the rule of law or the liberty of the people they claim to want to protect. If this becomes the norm and is not met with determined resistance by Americans concerned about liberty, the erosion of that liberty may soon reach the point where the FBI would have little trouble forcing companies to comply next time.

There are, of course, some questions which may shine a ray of hope on this recent development. Could law enforcement actually *physically* force someone to press their finger or thumb on a device to unlock it if the person refused? If so, what would the courts say about the evidence obtained? What would the reaction of the public be when — as would likely be the case — time after time, those searches produced no evidence of any value? How likely is it that tech companies and the tech community will

simply create a way for one fingerprint to unlock the device and another to either lock it or wipe it clean? Tech is, after all, an equal opportunity tool.

And if the watchers aren't going to protect the rights of people, those people will have to do it themselves.