

Apple Strikes Back

By Kevin Castillo, J.D. Candidate 2017 | February 29, 2016

On February 25, 2016, Apple moved to vacate Magistrate Judge Sheri Pym’s [order](#) forcing the company to write computer code that would allow the FBI to break into the iPhone of Syed Farook, one the San Bernardino shooters that killed fourteen people last year. The FBI has been unable to access the information on Farook’s iPhone through its own efforts.

According to [Apple CEO Tim Cook](#), “The government suggests this tool could only be used once, on one phone. But that’s simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks—from restaurants and banks to stores and homes.”

In its [motion](#), Apple argued that, unlike what the government says, the [1789 All Writs Act](#), signed by President George Washington, does not apply. At its core, the Act gives federal judges the power to issue orders to compel people to take certain actions, so long as those actions are legal and necessary. However, the company contends that forcing Apple to write source code would extend beyond those legal powers. The company contends that “the government could argue that it should be permitted to force citizens to do all manner of things ‘necessary’ to assist it in enforcing the laws, like compelling a pharmaceutical company against its will to produce drugs needed to carry out lethal injection in furtherance of a lawfully issued death warrant, . . . or forcing a software company to insert malicious code in its auto-update process that makes it easier for the government to conduct court-ordered surveillance.”

Even if the Act does apply, Apple argued that Magistrate Pym’s order violates its rights under the [First](#) and Fifth Amendments. Citing cases that support the idea that source code is protected speech, Apple contended that forcing it to write code would be “compelled” speech, which is subject to exacting scrutiny by the courts. According to Apple, because the FBI can only speculate that Farook’s iPhone may have relevant information, the government cannot meet that heightened standard.

Whatever the outcome, this case will almost certainly have domestic and [global](#) implications on the legal future of data encryption. A ruling in the FBI’s favor, for example, may encourage other sovereign governments to ask the same of Apple.