Apple, the FBI and free speech: Column

David B. Rivkin, Jr., and Andrew M. Grossman

February 19, 2016

It would be one thing if Apple could carry out a court order that it unlock an iPhone used by the San Bernardino terrorists simply by waving a magic wand. But encryption isn't magic; the order requires Apple to write and digitally sign a security-degraded version of its iOS operating system. That raises serious First Amendment concerns because the order amounts to a government-compelled speech.

The FBI picked this fight to set a precedent. For years, it's been locked in a "crypto war" with Silicon Valley over how to provide law enforcement access to users' data. So far, Apple, Google, and other companies have rebuffed demands to implement government back doors that defeat encryption and other security measures, arguing that such bypasses weaken security and facilitate abuses by criminals, corporate spies and foreign governments.

Apparently unable to identify a true ticking-time-bomb scenario to bring to court, the FBI settled for the next best thing: obtaining encrypted data off the workplace phone of shooter Syed Farook. The phone's encryption is keyed to a passcode, and Apple's software erases data after ten incorrect passcode attempts. So the government, relying on an aggressive reading of the 1789 All Writs Act, obtained an order directing Apple to "bypass or disable the auto-erase function" and make it possible to cycle through all possible passcodes.

While the FBI has previously obtained warrants requiring Apple to extract unencrypted data from devices running older software, this appears to be the first time that it has sought to conscript a company to write new software to circumvent security features. If it prevails, such a precedent will govern future cases.

That makes it all the more important that the courts get the legal principles right this time around. Overlooked so far in this debate is the First Amendment's prohibition on compelled speech. The Supreme Court has affirmed time and again that the right to free speech includes the right not only decide what to say but also what not to say. Representative cases have upheld the right of parade organizers to bar messages they disapprove and of public employees to refuse to subsidize unions' political speech.

Computer code can be speech: no less than video games (which the Supreme Court found to be protected), code can convey ideas and even social messages. A new encryption algorithm or

mathematical technique, for example, does not lose its character as speech merely because it is expressed in a computer language instead of English prose.

That's not to say that all code is absolutely protected. But there's a strong case to be made where code embodies deeply held views on issues of public policy and individual rights -- such as the right to be free from government surveillance. Forcing a person to write code to crack his own software is little different from demanding that he endorse the principle of doing so.

And that leads to the most troubling aspect of the court order: it does, in fact, demand that Apple endorse the government's views by requiring that it digitally sign the software so that it can run on an iPhone. A signature speaks volumes: agreement, endorsement, trust, obligation. Apple says all those things when it decides to sign a new version of its operating system.

The government can't force a person to sign a petition and endorse a political view. But that is exactly what it demands here: to compel Apple to endorse a version of its own software that runs precisely counter to its values. At the very least, that is one more reason for a court to reject the government's aggressive legal position in this case.

Andrew M. Grossman is an adjunct scholar of the Cato Institute. Both are lawyers in Washington D.C.