# THE OPM HACK IS ONE BIG REASON APPLE COULDN'T GUARANTEE ITS ABILITY TO KEEP FBIOS SAFE

Underlying the legal debate about whether the government can demand that Apple write an operating system that will make it easier to brute force Syed Rizwan Farook's phone is another debate, about whether the famously secretive tech company could keep such code safe from people trying to compromise iPhones generally.

The government asserted, in its response to Apple's motion to overturn the All Writs Act order, that Apple's concerns about retaining such code are overblown.

> [C]ontrary to Apple's stated fears, there is no reason to think that the code Apple writes in compliance with the Order will ever leave Apple's possession. Nothing in the Order requires Apple to provide that code to the government or to explain to the government how it works. And Apple has shown it is amply capable of protecting code that could compromise its security. For example, Apple currently protects (1) the source code to iOS and other core Apple software and (2) Apple's electronic signature, which as described above allows software to be run on Apple hardware. (Hanna Decl. Ex. DD at 62-64 (code and signature are "the most confidential trade secrets [Apple] has").) *Those* —which the government has *not* requested—are the keys to the kingdom. If Apple can guard them, it can guard this.

> Even if “criminals, terrorists, and hackers” somehow infiltrated Apple and stole the software necessary to unlock Farook’s iPhone (Opp. 25), the only thing that software could be used to do is unlock Farook’s iPhone.

That’s explicitly a citation to this passage from Apple’s original motion.

> The alternative—keeping and maintaining the compromised operating system and everything related to it—imposes a different but no less significant burden, i.e., forcing Apple to take on the task of unfailingly securing against disclosure or misappropriation the development and testing environments, equipment, codebase, documentation, and any other materials relating to the compromised operating system. Id. ¶ 47. Given the millions of iPhones in use and the value of the data on them, criminals, terrorists, and hackers will no doubt view the code as a major prize and can be expected to go to considerable lengths to steal it, risking the security, safety, and privacy of customers whose lives are chronicled on their phones.

In pointing to that passage, DOJ ignored the first passage in the Apple motion that addresses the danger of hackers: one that notes the government itself can’t keep its secrets safe as best exemplified by the Office of Personnel Management hack.

> Since the dawn of the computer age, there have been malicious people dedicated to breaching security and stealing stored personal information. Indeed, the government itself falls victim to hackers, cyber-criminals, and foreign agents on a regular basis, most famously when foreign hackers breached

> Office of Personnel Management databases and gained access to personnel records, affecting over 22 million current and former federal workers and family members.

By arguing that Apple can keep its secrets safe while ignoring the evidence that the government itself can't, the government implicitly conceded that Apple is *better* at keeping secrets than the government.

Of course, it's not that simple. That's because the millions of private sector employees who play a role in the secretive functions have clearances too. They were *also* compromised in the OPM hack. Thus, by failing to keep its own secrets, the government has provided China a ready made dossier of information it can use to compromise all the private sector clearance holders, in addition to the government personnel.

Which is why — in addition to his comment that it was "not reasonable to draw such a conclusion [that hackers could not hack iPhones from the lock screen] based solely on publicly released exploits" — I find this passage from Apple Manager of User Privacy Erik Neuenschwander's supplemental declaration, submitted to accompany Apple's reply, to be rather pointed.

> Thus, as noted in my initial declaration (ECF No. 16-33), the initial creation of GovtOS itself creates serious ongoing burdens and risks. This includes the risk that if the ability to install GovtOS got into the wrong hands, it would open a significant new avenue of attack, undermining the security protections that Apple has spent years developing to protect its customers.
>
> There would also be a burden on the Apple employees responsible for designing and implementing GovtOS. Those employees, if identified, could

> themselves become targets of retaliation, coercion, or similar threats by bad actors seeking to obtain and use GovtOS for nefarious purposes. I understand that such risks are why intelligence agencies often classify the names and employment of individuals with access to highly sensitive data and information, like GovtOS. The government's dismissive view of the burdens on Apple and its employees seems to ignore these and other practical implications of creating GovtOS.

From the briefing in this case, we know that Neuenschwander was part of the then-secret discussions about how to access Farook's phone before DOJ started leaking to the press about an impending AWA order. That means he almost certainly has to have clearance (and may well deal with more sensitive discussions related to FISA orders). We also know that he would be involved in writing what he calls GovtOS. You would have to go no further than Neuenschwander to identify a person on whom China has sensitive information that would also have knowledge of FBiOS (though there are probably a handful of others).

So he's not just talking about nameless employees when he talks about the burden of implementing this order. He's talking about himself. Because of government negligence, his own private life has been exposed to China. And, in part because DOJ chose to conduct this fight publicly, his own role (which admittedly was surely known to China and other key US adversaries before this fight) has been made public in a way NSA's own engineers never would be.

FBI's request of Apple — particularly coupled with OPM's negligence — makes people like Neuenschwander a target. Which is why, no matter how good Apple is at keeping their own secrets, that may not be sufficient to keeping this code safe.