DAILY NEWS

Apple, the FBI and the future: Seemingly by accident, the government hit upon a far more promising approach to cracking increasingly sophisticated encryption

Julian Sanchez

March 30, 2016

The epic showdown between the FBI and Apple has ended with a fizzle for now. With help from a mysterious "outside party" — which many believe to be the Israeli mobile forensics firm Cellebrite — the Bureau has been able to unlock the work iPhone of deceased San Bernardino shooter Syed Farook.

That means the government is dropping its legal fight to force the tech titan to write it a hacking tool that bypasses the phone's security features — though at least a dozen other similar cases remain open at the federal level alone, and the technique used to access Farook's phone may not work on newer models.

This latest development certainly doesn't mark the end of the larger debate over how to best reconcile the public's need for secure devices with the demands of law enforcement, but it may provide a model for a more productive general approach.

In this case, the government had sought to compel Apple to write and, critically, use its tightly-guarded cryptographic key to "sign" specialized passcode-hacking software that would be accepted by Farook's phone as a legitimate Apple update.

The company, backed by many security experts and a who's-who of Silicon Valley technology powerhouses, warned that such a move would set a dangerous precedent. A flood of similar requests from law enforcement agencies around the world was certain to follow, creating an unacceptable risk that hackers or repressive foreign regimes would obtain a copy of the software, compromising the security of millions of users.

A better way

Similar objections have been raised against proposals to require companies to design their products with security vulnerabilities or "backdoors" built in up front. Creating truly secure hardware and software turns out to be a surprisingly difficult task — with frequent software updates and patches needed to close a neverending train of newly discovered security vulnerabilities — and many experts insist that a requirement to provide backdoors for governments would render that all but impossible.

But maybe we don't need to "balance" the security of our data against the needs of law enforcement at all. Instead of demanding that companies create new security vulnerabilities, weakening the safeguards that protect ordinary users along with criminals and terrorists, the FBI could do what it has done here: Invest in identifying the existing vulnerabilities that will inevitably be found in any complex hardware or software.

Then, critically, the vulnerability can be disclosed to the developer and patched, letting the government access the devices it already has in hand — while protecting innocent users against malicious hackers exploiting the same loophole.

That’s something security researchers had suggested since the FBI’s legal dispute with Apple became public, pointing to a variety of approaches that might enable access to the phone’s data. The FBI had insisted, both to the public and the courts, that no such alternatives existed, making it “necessary” to conscript Apple’s assistance.

Yet the relatively rapid emergence of just such an alternative suggests that the whole messy battle might have been avoided if the Bureau had cast a wider net in its initial search for solutions, almost certainly at a lower cost than suing Apple.

It’s also the broader approach several prominent computer scientists recommended in a 2014 paper on “Lawful Hacking.” As the authors explain, “the choice is between formalizing (and thereby constraining) the ability of law enforcement to occasionally use existing security vulnerabilities — something the FBI and other law enforcement agencies already do when necessary without much public or legal scrutiny — or living with those vulnerabilities and intentionally and systematically creating a set of predictable new vulnerabilities that despite best efforts will be exploitable by everyone.”

It’s easy to see why law enforcement finds it tempting to look for a single “magic bullet” solution to the problem of accessing encrypted data. Building the necessary in-house capability to do “lawful hacking” doubtless seems far more cumbersome, costly, and uncertain than simply passing a law that offloads the problem on tech companies. But, like most simple-seeming solutions to hard problems, it comes with unacceptably high hidden costs over the long term.

In recent years, intelligence officials have warned that our vulnerability to cyberattack the most serious national security threat the United States faces — and as mobile devices increasingly hold the credentials needed to access secure networks, smartphones are definitely part of that threat.

Against that background, the FBI should to stop talking about “balancing” data security against their investigative goals and shift their focus, and their resources, to an approach that serves both at once.

Julian Sanchez is a senior fellow at the Cato Institute.