THE WALL STREET JOURNAL.

The FBI vs. Apple

The White House should have avoided this legal and security showdown.

February 19, 2016 | Editorial Board

The encryption cold war that for two years has pitted Silicon Valley against law enforcement finally turned hot this week, as a California judge ordered Apple to unlock an iPhone used by the San Bernardino terrorists. Perhaps public safety and modern digital security methods were bound to collide, but the danger as always in such conflicts is that both sides end up annihilated.

The Federal Bureau of Investigation is attempting to bypass the security system on an iPhone recovered from Syed Rizwan Farook, who with his wife Tashfeen Malik killed 14 people and injured 22 others. The problem is that no one knows the phone's password.

Apple has turned over information that Farook stored to its cloud servers, but he did not back up his phone for several weeks preceding the attack. The FBI wants to retrieve this encrypted data that exists only on the device itself, which potentially include text messages, photos, location tracking or connections to the Islamic State or perhaps even other terror cells that could be operating in the U.S.

Apple's iOS operating system is designed to automatically erase local data after too many incorrect passcode attempts. Because iPhones can only run software with Apple's proprietary cryptographic signature, the FBI wants Apple to create and upload a custom version of iOS to Farook's device that overrides this mechanism. The bureau can then hook up an external computer that will make unlimited guesses to unlock the phone's contents, known as "brute forcing." Magistrate Judge Sheri Pym agreed.

In a public letter, Apple CEO Tim Cook refused to comply with this "unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority" and said the company would appeal. "The U.S.

government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone," he wrote.

***

Yet the reality seems to be more complicated than either Mr. Cook or the FBI allow. The encryption debate began in 2014 when Apple released a feature that generates random security "keys" that are unknown to Apple and in combination with the user's passcode to decrypt the device's data. Without such mathematical formulas, the data are unreadable.

This two-step "full disk" encryption process makes iPhones more secure, but it also means Apple can't unlock its own products. Neither can Google after adopting the same practice. Encrypted communication platforms have been available since the early 1990s, but Apple and Google have now made them the default for the 96% of global customers who use their operating systems.

The fear among law enforcement and the national-security agencies is that jihadists and criminals are going dark. FBI chief James Comey and Manhattan District Attorney Cy Vance warn they are losing the capacity to execute bona fide search warrants granted under the Fourth Amendment. So they support a mandate that the U.S. tech industry install a master security key—the "backdoor" Mr. Cook invokes—to unlock any device.

The CEO has a strong case when he says that backdoors create more problems than they solve. Introducing security vulnerabilities that third parties like cops and spooks can use as needed can also be exploited by hackers, crooks and spies. Nations can mandate backdoors, but there will always be some encrypted channels outside of their jurisdiction where the likes of ISIS can plot. The result would be weaker products for law-abiding consumers that leave U.S. companies less competitive with little security benefit.

Stronger cybersecurity is more important than ever in a world of corporate espionage, millions of compromised credit-card numbers and the stolen identities at the Office of Personnel Management. Encryption may lead to fewer antiterror intercepts, though the universe of signals that can be tapped has expanded radically and on balance more secure phones are a major advance for human freedom. Ask the

Chinese pastors or Russian dissidents who are targeted by authoritarian regimes and want encrypted iPhones.

***

One question is whether the San Bernardino terror case should be an exception to Mr. Cook's strong argument against backdoors. In this case Apple is not being ordered to create a universal backdoor for all phones, and some digital security experts believe it is technologically possible to assist the FBI in the San Bernardino investigation with a unique iOS to brute-force this single device.

"Apple does not dispute that it has, in prior instances, complied with data extraction demands that have been contained in the body of search warrants or, less often, All Writs Act orders," Apple conceded in a New York court filing last year. The government is citing this to show that its request is reasonable.

But in those cases the company's engineers have never been conscripted to create a new architecture to defeat their own security measures. Apple believes that if it caves even once, every prosecutor in America will be lining up for forensic help with misdemeanors. A supposedly one-time emergency fix in an antiterror case could well become a de facto backdoor in practice over time.

There's also the question of whether the government currently has the legal authority to force Apple to become the government's agent. Safe manufacturers are not obligated to crack their own locks when the FBI calls. Apple contends the All Writs Act has never been used to compel what the government now wants from Apple, and the question is far from clear-cut. The litigation to settle this could take months or years.

It's an understatement to say that Apple is taking a risk by challenging the Administration in a high-profile domestic terror incident with unpredictable politics. "Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Arkansas Republican Tom Cotton, and Donald Trump has been no more subtle.

But for the same reason, the Administration ought to have resolved the situation confidentially before it reached legal and political Defcon One. Terror cases by their nature are different from run-of-the-mill law enforcement, and San Bernardino requires more than the government's typical show of incompetence.

The White House never supplied Congress with specific backdoor statutory language even as Mr. Comey made the public rounds, only for President Obama to renounce any attempt at forging a legislative solution. Yet spokesman Josh Earnest defended the FBI and Justice Department on Wednesday. Is there a grownup in the White House?

***

So a word on behalf of Michael McCaul, the Chairman of the House Homeland Security Committee, who has proposed convening an expert panel on technology and security in the modern era. Blue-ribbon commissions are usually a form of Beltway escapism, but in this case a detailed report and recommendations from leading minds in technology, law, computer science, police and intelligence could help shape a rough consensus—or at least establish a common set of facts. Such a halfway house might also help calm political tempers and marginalize the absolutists.

A mature democracy—if America still is one—ought to be able to work out these crucial matters of national security through legislative deliberation. The public interest on encryption is best served with a rational debate, not the ad hoc nuclear legal exchange that the Administration is inviting.