In the Government vs. Apple, Who Wears the Black Hat?

Source: Robert Levine *The New York Times*, February 21, 2016

THE dispute between the Justice Department and Apple over access to the phone of Syed Rizwan Farook, one of the gunmen in the San Bernardino massacre, comes down to this question: Shouldn't the government have more legal and moral authority to weigh complicated issues of privacy and national security than a company that makes phones?

It should. After all, nobody ever elected Tim Cook, Apple's chief executive, to public office. The legal case seems clear enough: The Federal Bureau of Investigation has a warrant, Mr. Farook is dead, and his iPhone, which he used for work, is the property of San Bernardino County, which consented to having it searched. The data on the phone could yield valuable intelligence, making its content a legitimate matter of national security.

Apple had obeyed a demand to provide the government with the information in Mr. Farook's iCloud account. But then it was asked to undermine the phone's security system so the F.B.I. could try as many passcodes as possible to open the phone without erasing the stored data. Apple refused. On Friday, the Justice Department filed a motion saying that Apple's objections had little to do with security but appeared "to be based on its concern for its business model and public brand marketing strategy."

The government, not Apple, should guarantee our privacy rights. But this dispute has arisen precisely because the government hasn't done so. Instead, it squandered much of its legal and moral authority when the National Security Agency engaged in widespread surveillance of American citizens for so long. Some N.S.A. abuses targeted Silicon Valley directly.

In one project, revealed in October 2013 by journalists tipped off by Edward Snowden, the N.S.A., along with its British counterpart, essentially hacked into fiber-optic cables that connected the data centers of Google and Yahoo outside the United States. Under American law, the agency already had access to some of the information, but it tapped the lines anyway.

Silicon Valley companies love to celebrate the hacker spirit, but they don't like being on the receiving end. By November 2013, both Google and Yahoo announced that they were encrypting data traveling between its server centers. By the following September, Apple announced that its new phones would by default encrypt data stored on the device in such a way that even the company itself couldn't get at it.

At the time, this seemed like a hopelessly geeky version of Mad magazine's "Spy vs. Spy," with opponents one-upped with algorithms rather than cartoon bombs. But the fight led directly to Tuesday's ruling by a federal magistrate judge in California that Apple must help the F.B.I. unlock Mr. Farook's phone. The laws governing online privacy are woefully out-of-date. To compel Apple to help execute a warrant, the judge cited the All Writs Act of 1789, enacted before there was electricity.

In Apple's public response, the company said it was fighting the F.B.I.'s demands not because it objected to the government unlocking Mr. Farook's phone but because the government could then ask Apple to undermine the security of other iPhones and because such software could potentially help criminals and repressive governments hack iPhones.

By analogy, the company doesn't have a key to the phone so the government is asking it to make the lock weaker. Apple is being asked to undermine not only the security of its products but also potentially its corporate reputation and even its business. The company is especially concerned that a victory for the government would set an informal precedent for other countries to demand that Apple unlock encrypted data. It's hard to have any sympathy for Mr. Farook, but the line between terrorism and criticism of the government can be far fuzzier in other countries, like China, where Apple sold tens of millions of iPhones in the last quarter of 2015. Apple's phones are also sold in Pakistan, where homosexual acts can send people to prison, and in Saudi Arabia, where adultery is punishable by lashing or stoning and apostasy punishable by death.

The United States government may have a reasonable case when it comes to Mr. Farook, but a victory here would open a Pandora's box that can't be closed in the United States or anywhere in the world. Cracking the phone open also may not help as much as we think: Would-be terrorists can use encrypted communication services that operate in other jurisdictions.

What we really need is a robust public conversation around strong privacy laws that would apply to the government and private companies alike and clear limits on what should be done with data. Important choices about the future of technology and privacy should be made by the American people and their representatives, not by Silicon Valley, where even the noblest intentions are mixed with huge financial stakes. If the government wants the power to compel companies to undermine their own security systems, it should go to Congress and ask for it.

Until then, we are left with Silicon Valley executives making engineering decisions that could determine what information the government can and can't have. That's both bad policy and fundamentally undemocratic.

But the current choice is between a government that doesn't seem to recognize limits to its own power to access personal information and a technology company that does. It's a bad choice, but an obvious one. While nobody elected Mr. Cook to protect our privacy, we should be glad someone is.

Possible Response Questions (Answer ONE):

- Do you trust the government to make the right decisions about privacy and security? Do you trust a corporation more or less? What do you think should happen in this case?
- What do you think about the scenarios Apple envisions if it is forced to comply with the FBI? Do you think the benefits of breaking the encryption outweigh the drawbacks to various people around the world?
- The government used the All Writs Act of 1789 to try to force Apple to break their encryption. What updates to the law do you think are necessary to reflect the realities of life in the 21st century?
- Select any passage and respond to it.