Confluence
INVESTMENT MANAGEMENT

Weekly
Geopolitical Report

*By Bill O'Grady*

*March 14, 2016*

## The Apple Problem

On December 2, 2015, Syed Rizwan Farook and his wife, Tashfeen Malik, attacked a San Bernardino county facility, killing 14 people and seriously injuring 22 others. The couple was subsequently killed by local law enforcement in a shootout several blocks from the facility. The Federal Bureau of Investigation (FBI) opened an investigation into the attack. As part of this work, an Apple (AAPL, 101.20, -0.67) iPhone was discovered that was used by Farook but owned by the county. The FBI wanted to look at the information on his phone, but the encryption built into the device prevented authorities from accessing the data. The government has sued Apple to force the company to circumvent its security; thus far, the company has refused.

In this report, we will discuss the attack and the perpetrators, including the gathering of evidence which included the phone in question. We will explain in non-technical terms how Apple software protects the data on the iPhone. We will compare and contrast the legal positions taken by the company and the government and frame the controversy using the U.S. Constitution, examining the tensions between the Bill of Rights and the problems presented by wartime. As always, we will conclude with market ramifications.

### The Attack and Investigation

Farook and Malik's attack occurred at a San Bernardino County government office. Farook had worked at that office for five years, filling various positions, starting as a seasonal employee, gaining a full-time position as a county food inspector and becoming an environmental health specialist. He was born in the U.S. to parents who had emigrated from Pakistan. He was a devout Muslim.

His wife, Malik, was born in Pakistan to an upper class family. She became a pharmacist, graduating from the Bahauddin Zakariya University in Pakistan. While in this course of study she also attended classes at the Al-Huda International Seminary for Women. This seminary is affiliated with Wahhabi Islam, the conservative version of Sunni Islam practiced mostly in Saudi Arabia. Her family moved to Saudi Arabia and she met Farook through an online dating service. There is some speculation that she was radicalized in Saudi Arabia, although this has been denied by Saudi authorities. There is evidence that suggests she may have become radicalized at the seminary.

When the couple decided to marry, she began the vetting process to enter the U.S. First, she applied and was granted a K-1 (fiancé) visa with a green card. Second, Homeland Security and the State Department conducted three investigations on Malik; these did not turn up any evidence that she was a security threat.

After the attack, the FBI conducted a thorough investigation of the event. The FBI is trying to determine if there were signs that the couple was preparing for a terrorist attack, which may give security officials clues toward the prevention of similar attacks in the future. They are also trying to ascertain if the pair was supported in any way by an outside terrorist organization,

e.g., al Qaeda or Islamic State (IS). We note the latter congratulated them on their attack but there isn't much evidence to suggest IS was involved beyond offering aspirational support.

As part of the investigation, the government gathered the couple's electronics, including cell phones and computers. During this segment of the inquiry, the FBI discovered an iPhone 5c used by Farook but owned by San Bernardino county. The government wanted to review the contents of the device but could not get beyond its security protections. The FBI asked Apple to crack the security; the company refused.

Apple's iOS9 operating system has a feature that locks the device after 10 incorrect attempts to enter the PIN code. This prevents the non-owner from opening the phone using a "brute force" tactic of running through numbers on a computer until the correct PIN code is revealed. Once the phone is locked up, it can only be opened by an internal encryption key that exists on the device itself. Apple could develop a procedure to get around this key but, in doing so, would create a vulnerability that criminals, hackers and other governments could exploit.

After Apple refused to give the government a work-around for its security feature, the FBI sued. So far, Apple has not given the government what it wants and the government is still pressing Apple to create a procedure to bypass the device's security.

**Apple's Argument**

The Fourth Amendment of the U.S. Constitution protects Americans from unreasonable searches and seizures. The courts have interpreted this to mean that the police must have probable cause to search a person, car or dwelling and, in some cases, the authorities must obtain a search warrant to look for an item on the premises. In addition, the courts have suggested that this amendment also gives Americans a right to privacy, which is the basis of Apple's refusal to cooperate. Apple is arguing that the Fourth Amendment cannot compel a private company to assist the government in its quest for evidence. Thus, the company is arguing that it cannot be forced to give the FBI assistance under the Constitution.

In addition, Apple argues that creating this "backdoor" (as we alluded to above) would create security vulnerabilities that would be bad for its products and customers. Being able to buy products in which information can be kept safe from the prying eyes of criminals and governments is a selling point.

History is full of examples of government snooping that were constitutionally questionable. In addition, if Apple gave this power to the U.S. government it would surely be forced to give it to other governments as well. Interestingly enough, some government entities want very secure products (primarily for internal communications) and are more sympathetic to Apple's position.

**The FBI's Argument**

It would appear that the FBI is trying to use this case to set a precedent that would give the government the power to compel companies and private individuals to facilitate the monitoring of others. It is unlikely that there is anything on Farook's phone that would tell the FBI much. However, if there is intelligence that proves an international jihadist organization gave aid and guidance to Farook and Malik, then Apple's behavior is objectionable.

Given the gravity of the attack and the publicity it generated, it creates a

sympathetic case for the government's position. Essentially, the government is trying to weaken the Fourth Amendment.

**The War Problem**

Although the Bill of Rights offers American citizens protection from various forms of government power, there have been periods in American history when these rights were curbed, most commonly during wartime. Some examples include:

- President Lincoln suspended the right of habeas corpus, allowing the government to hold defendants indefinitely without trial. He used this power to arrest Northerners who opposed his policies against the South and were hindering the war effort.

- President Wilson signed both the Espionage Act of 1917 and the Sedition Act of 1918. The former made it illegal to interfere with the war effort or military recruitment. The latter made it illegal to express an opinion that painted the war or the U.S. in a negative light, a clear violation of the First Amendment.

- President Roosevelt interned Japanese-Americans during WWII even though there was scant evidence they were a security risk. He also allowed the FBI to intercept Congressional mail and spy on Americans.

- Presidents Johnson and Nixon used the FBI and CIA to infiltrate and monitor anti-war and civil rights groups in the 1960s and 1970s.

- President Bush essentially denied habeas corpus to suspected Islamic terrorists by detaining them at the U.S. Naval base at Guantanamo Bay. If held in the U.S., these detainees would have Constitutional rights; by holding them offshore, they resided in a legal netherworld that allowed the U.S. to hold them without formally charging them or bringing their case before a judge.

The common thread among these cases is the condition of war. The government and society have generally decided that the risks the country faces during wartime can allow for the suspension of parts of the Bill of Rights. The government has tended to rescind these practices once the conflict ends. Examples include when President Andrew Johnson restored habeas corpus in 1865 after the end of the Civil War, the repeal of the Sedition Act in 1920, a Supreme Court decision that ended the Japanese internment in 1945[1] and the Church Committee investigation that led to restrictions on the Cold War intelligence abuses of the mid-1970s.

The problem is that until the U.S. became a superpower, wars had definite beginnings and endings. However, superpowers are really in a constant state of war. The Cold War spying could probably be justified due to the risks of Soviet espionage. There were a few "hot" wars (e.g., Korea, Vietnam, the Gulf War), but a nation faces lots of enemies when it is a global hegemon. Thus, there will be tensions between the legitimate demands of civil rights and the legitimate demands of security. As the war history shows, navigating these demands is fraught with risk.

The government can reasonably argue that the needs of national security are critically important and so firms and individuals should be forced to cooperate with security

[1] In 1991, President Bush issued a formal apology to those who had been interned and paid $20k to each surviving detainee.

officials or Americans will be at risk. Therefore, weakening the security of electronic devices to uncover terrorist threats should be allowed. Apple can respond that being forced to comply with the government's demands will undermine the value of its products. Not only will criminals be able to gain access to a person's information, but other governments will likely demand similar access. According to Apple, the demands of the government are unconstitutional and will act to undermine the value of the company.

Unfortunately, the American political class has never openly discussed the costs of hegemony. Becoming a superpower was clearly necessary to prevent communism from becoming the dominant economic and political structure for the world. However, this decision came with high costs, one of which was to force the U.S. to change in ways that are not generally appreciated by the American people. Prior to 1940, the U.S. had a small government and, outside of wartime, could protect Americans' Constitutional rights. But, the burdens of hegemony are heavy. It requires a large standing army, the creation of a "military/ industrial complex," a large government to build the military and ensuring enough consumption to fulfill the reserve currency role.

Essentially, we have a Constitution written for a non-hegemonic nation. It is probably not applicable for a superpower. To make it work, the Supreme Court has moved away from a literal reading of the Constitution[2] to a broader interpretation, almost certainly in ways that the founders wouldn't recognize. This is probably because the founders never imagined the U.S. would take on the superpower role.

[2] Famously opposed by the late Justice Antonin Scalia.

**Ramifications**

The market implications of this situation most directly affect technology companies. If the government prevails in this case, foreign governments will (a) worry about the security of their citizens' data on American devices, and (b) want similar provisions for their own security services. Both outcomes will tend to make these devices less attractive to foreign and domestic purchasers.

If Apple prevails, it may make its devices more valuable, although some foreign countries (e.g., China) will be uncomfortable giving their citizens this degree of privacy. The societal tradeoff is that we could be less safe. Terrorists do everything they can to avoid detection. Following the usual procedures of law enforcement are inappropriate if the U.S. is facing an enemy using terrorist tactics that intends to put operatives into the U.S. Law enforcement usually works by arresting a perpetrator after the crime has been committed. That tactic doesn't work in war. The paradox is that this enemy would be using our Constitutional guarantees to directly harm us, which seems like a high cost to bear.

We don't know how this case will be resolved. Both parties have strong arguments. Americans cherish their Constitutional protections. On the other hand, those protections don't mean much if one is dead.

Ultimately, it may simply be a situation where the courts, and society, have to decide (a) what kind of war are we waging against jihadist terrorism, and (b) is it a profound enough threat to weaken our Constitutional protections? As noted above, this issue is tied to an unresolved and mostly unacknowledged hegemonic role that the

United States has undertaken since the end of WWII.

Bill O'Grady
March 14, 2016



## Confluence Investment Management LLC

Confluence Investment Management LLC is an independent, SEC Registered Investment Advisor located in St. Louis, Missouri. The firm provides professional portfolio management and advisory services to institutional and individual clients. Confluence's investment philosophy is based upon independent, fundamental research that integrates the firm's evaluation of market cycles, macroeconomics and geopolitical analysis with a value-driven, fundamental company-specific approach. The firm's portfolio management philosophy begins by assessing risk, and follows through by positioning client portfolios to achieve stated income and growth objectives. The Confluence team is comprised of experienced investment professionals who are dedicated to an exceptional level of client service and communication.