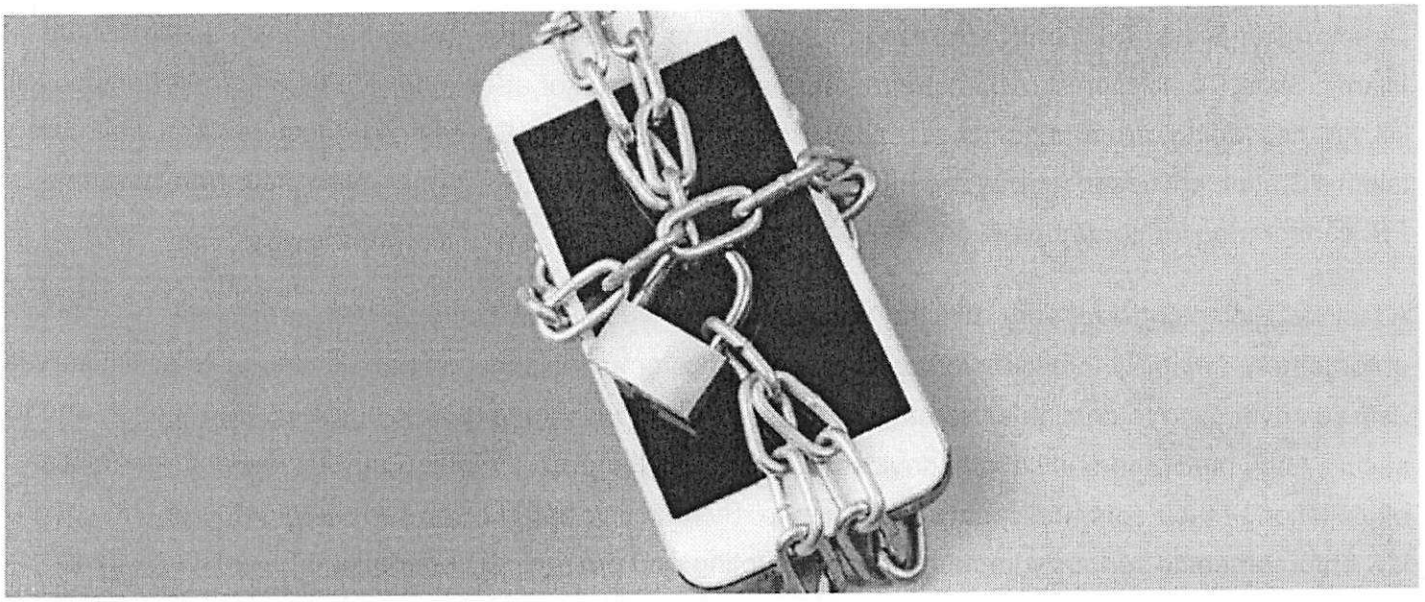
Apple Versus the FBI: Who wins?

March 14, 2016



A

s we have witnessed over the past few weeks, the debate between Apple and the FBI—regarding accessing encrypted communications—has intensified significantly. The issue at hand—privacy versus security—is one in which we all have a vital stake. The law enforcement challenge of accessing encrypted information has been simmering for quite a while. It came to a head in recent weeks when Apple refused to provide encrypted data to the FBI pursuant to legal process through a federal court. In turn, Apple has gone to the federal court to challenge the legal process.

The case at the center of the controversy is the San Bernardino terrorist attack. The FBI served Apple with a court order to open the encrypted iPhone of terrorist Syed Rizwan Farook. The FBI is seeking information critical to determining where Farook and his wife were between the time of the shootings and their encounter with law enforcement where they were killed. Determining where Farook and his wife went and if Farook communicated with anyone is of paramount importance to the FBI in completing their investigation of the San Bernardino attack. Apple has staunchly denied to provide access contending that it would violate their customers' right to privacy and also undermine security for encrypted communications devices.

So, who wins? In the short term, the winners are not the general public, not the FBI and law enforcement, and not Apple and communications providers. Sadly and alarmingly, the immediate winners are the criminals, terrorists and violent homegrown extremists aspiring to be terrorists, who hide behind encryption and use it to facilitate their illicit activity. When new technology was introduced offering more secure encryption, an element of criminals, terrorists and aspiring terrorists quietly took advantage of encryption in furtherance of their nefarious activities. FBI Director James Comey has been sounding

the alarm about criminals and terrorists taking advantage of encryption and "going dark" for some time now. Director Comey described "going dark" to mean that law enforcement could not monitor encrypted communications. That is particularly troubling considering the constant threat of terrorism and the rise of homegrown extremists recruited to be foreign fighters or to commit acts of terrorism at home.

Director Comey has frequently expressed his concerns about the Internet recruitment practices of the Islamic State. Their sophistication, their relentless 24/7 pursuit of at-risk individuals and their nonstop kill, kill, kill messaging, are all significant reasons for concern. Director Comey has described that when the Islamic State identifies a serious recruit, they direct that individual to an encrypted platform where the FBI cannot monitor communications, thereby "going dark."

A fact we should consider very concerning is that the constant media attention regarding law enforcement's inability to circumvent encryption and communications companies' refusal to assist serves as free advertising to criminals, terrorists and aspiring terrorists to take advantage of the situation and to secure encrypted communications devices. The biggest vulnerability to bad guys is law enforcement's exploitation of their communications and finance. By enabling bad guys to take advantage of encryption, law enforcement is seriously impeded from disrupting and preventing criminal and terrorist activities.

I am not an attorney or a technical expert; thus, I will leave the legal debate and technical discussion to those who are experts in those areas. I am an expert in dealing with criminals and terrorists, having spent over 40 years investigating and assessing them firsthand. Without question, criminals, terrorists and aspiring terrorist are, and will increasingly, take advantage of using encryption to facilitate their illicit activities.

During the past two weeks, Director Comey has stated in congressional hearings that privacy and security issues must be decided by the American people and Congress. In view of the free advertising for encryption bad actors have been receiving, Congress needs to act quickly to address and resolve this issue. The American people deserve to be the ultimate winners in this debate—not the criminals, terrorists and aspiring terrorists. To truly accomplish this, Apple and other communications providers must work with the FBI and law enforcement to find an acceptable middle ground that ensures the citizenry, and not the bad guys, are the real winners. In doing so, privacy and security interests can be balanced.

As a former FBI agent, I have a law enforcement bias. I understand the critical importance of law enforcement access to communications without being impeded by encryption. Likewise, as a former FBI agent, I understand and respect the right to privacy, as does Director Comey and the current generation of FBI agents. Director Comey has been particularly conscientious in his statements about the balance between privacy and security. In his appearance before the House Judiciary Committee regarding encryption on March 1, 2016, Director Comey stated: "We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us

safe."[1]

On February 29, 2016, General Keith Alexander, the former National Security Agency (NSA) Director, was interviewed by *Bloomberg Business News* regarding the ongoing debate between Apple and the FBI. General Alexander commented that both Apple and the FBI were right in their arguments and that they needed to find a middle ground to work together to enable the FBI to obtain encrypted information while protecting civil liberties, privacy and security. General Alexander called for a reasoned approach and not going through a back door to obtain encrypted data but going through a transparent front door.[2]

Moreover, General Alexander was asked if there was a terrorism case in the last 10 years, that had encryption been used, could have been a successful terrorism attack in the U.S. Without hesitation, General Alexander referred to the case of Najibullah Zazi. Zazi is an Afghan American who was arrested in September 2009. He pled guilty for being part of an al-Qaeda plot to conduct suicide bombings on the New York City subway system. According to General Alexander, NSA identified telephone conversations between an al-Qaeda member in Pakistan and Zazi. The NSA was able to go to the communications provider and obtain conversations between the two men. It was determined that Zazi was planning a bombing and the NSA turned the information over to the FBI. General Alexander stated that if the al-Qaeda member and Zazi had been using encrypted equipment, the NSA would not have been able to obtain the content of the conversation and all that would have been known was that a discussion took place. In that scenario, it would have been likely that Zazi and his co-conspirators could have successfully detonated suicide bombs in the New York City subway system.[3]

It is incumbent that Apple and other communications providers step up and strike a balance between privacy and security as called for by Director Comey and General Alexander. Instead of digging in their heels and defying law enforcement and, in so doing, protecting bad actors in the guise of protecting the general public, Apple, et al, should be working with law enforcement to identify the middle ground to provide law enforcement with sensitive information needed in significant criminal and terrorist investigations while safeguarding privacy and security considerations.

Know Your Customers

Interestingly, the current debate lends itself to another discussion that has not yet taken place. Apple and other communications providers have been adamant about protecting the privacy and security of their customers. Yet, do they know who their customers are? Communications providers have no requirement to know their customers and to report suspicious activity to law enforcement. Anyone can purchase encrypted communications devices and use them as they see fit. Being that criminals, terrorists and aspiring terrorists benefit from encryption, why should communications companies not be required to know their customers and to deny high-risk customers from encrypted services?

Financial institutions are required by law to have anti-money laundering (AML) programs reasonably designed to identify suspicious financial transactional activity. An important component of an AML

program is to know your customer. Higher risk customers require greater scrutiny. Higher risk customers also cause a financial institution to explain and defend why they service high-risk customers and not exit those relationships. There is a regulatory expectation that financial institutions take a risk-based approach to identify criminal exploitation of the financial system. Why should communications providers not be held to a similar standard?

The point for thoughtful discussion is: Should communications providers who offer encrypted communications devices to customers be required to know their customers and take steps to mitigate criminal misuse of encryption?

When communications providers push back from this discussion—for reasons including that the cost of knowing their customers would be prohibitive, the process would be impractical, and that it would violate customer privacy—they should be pointed to financial institutions. Financial institutions face cost challenges for knowing their customers, practical challenges in conducting due diligence and privacy considerations. Yet, financial institutions are required to identify and report suspicious activity. Communications companies who provide the ability for criminals, terrorists and aspiring terrorists to circumvent law enforcement scrutiny through encryption should be required to be accountable for identifying and reporting the bad actors they facilitate.

As stated by Director Comey regarding the encryption debate, this is a discussion that should ultimately include the American public and Congress. If Apple and other communications providers want to protect the privacy and security of their customers, they should know their customers. High-risk customers should be denied encryption service or their providers should be required to justify the risk of providing service to such customers.

In today's world, the issue we have to address far exceeds freedom of speech, privacy or security—it deals with risk. That appears to be the one factor Apple and their supporters fail to address. Let us hope they address it before an aspiring terrorist takes advantage of their service to force the issue.

Dennis M. Lormel, CAMS, internationally recognized CTF expert, president & CEO, DML Associates LLC, Lansdowne, VA, USA, dlormel@dmlassocllc.com

1. "Director Comey Discusses Investigative Challenges in Light of New Methods of Electronic Communication," FBI, March 1, 2016, https://www.fbi.gov/news/news_blog/director-comey-discusses-investigative-challenges-in-light-of-new-methods-of-electronic-communication
2. "Apple and the FBI: Bloomberg West," *Bloomberg Business News*, February 29, 2016, http://www.bloomberg.com/news/videos/2016-03-01/apple-and-the-fbi-bloomberg-west-full-show-02-29
3. Ibid.

Like? Share with your friends.