The Heritage Foundation

ISSUE BRIEF

No. 4531 | MARCH 18, 2016

Encryption Commission: Making Sense of Critical Policy Options

David Inserra, James Jay Carafano, PhD, Charles D. Stimson, Steven P. Bucci, PhD, David Shedd, and Paul Rosenzweig

In the current legal battle between Apple and the FBI over a San Bernardino terrorist's cell phone, critical security, technology, privacy, legal, and counterterrorism issues have all come to a head. As different judges have come to different conclusions on this issue and with Apple and the Department of Justice appealing these cases, Congress has also entered the debate. In a vigorous debate held by the House Judiciary Committee on March 1, no consensus was forthcoming and the issue cut across political lines.[1] It is one that defies simple solutions.

There is agreement, however, that this issue is important and deserves a complete debate. Given the technical nature of this issue and the need for Congress to fully understand the costs and benefits of various courses of action, recent proposals[2] to establish a commission to study this issue are a prudent path forward.

Basics of Apple vs. the FBI

Apple has continually improved the security of its devices. The iPhone 5C used by Syed Farook has encryption that no one can break, including Apple itself. The only way to access the device is to use the proper passcode, which only the user should know. Since the passcode is the only way into this phone, Apple has also built several protections around the passcode, such as an auto-erase protection that deletes the contents of the phone after 10 incorrect passcode attempts and a passcode delay protection that makes a user wait increasingly long times between incorrect attempts.

A court in California ordered Apple to create a new program, which Apple says does not exist, to be uploaded to the iPhone to disable the auto-erase function and other passcode protections.[3] This would enable the FBI to try every passcode combination (1111, 1112, 1113, etc.) in rapid succession until it guesses the correct passcode, a process known as "brute-forcing."

Apple is appealing this order[4] and has won a separate, similar case in New York that involves different versions of iPhones and operating systems.[5] In both cases, the Department of Justice argues that its authority to compel Apple to assist the FBI comes from the All Writs Act (AWA) of 1789. According to the Congressional Research Service, the AWA "performs a gap-filling function,"[6] that, according to the Supreme Court, can be used "to effectuate and prevent the frustration of orders" that are duly issued by courts. But there are limits to this authority. The Supreme Court articulated three limitations in *United States v. New York Tel. Co.*:

1. The order to comply must not be an "unreasonable burden" on the company,
2. The order must be "consistent with the intent of Congress," and
3. The company's assistance must be "essential to fulfillment of the [government's] purpose."[7]

This paper, in its entirety, can be found at **http://report.heritage.org/ib4531**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

The key legal questions will focus on the first two of these limitations: whether the order is an unreasonable burden and whether it is consistent with the intent of Congress, given that Congress has mandated technological help in some areas, but not here. [8]

Going Dark and the Challenges of Encryption

Encryption and strong protections on devices and computers provide consumers with significant security benefits. Cyber breaches and attacks happen regularly, striking individuals, businesses, and governments. Strong encryption and strong device security are essential to keeping important information out of the hands of criminals and hackers.

However, as with any advance in technology, it is usable not only by trustworthy actors but also by malicious ones. Terrorists and criminals are taking advantage of strong encryption, making it much harder and in some cases impossible to investigate bad actors. Nearly everyone understands this to be a significant problem that in some cases makes the U.S. less safe by shielding the communications and data of these bad actors.[9] As a result, the law enforcement community, led by the FBI, has been seeking legislative relief for the better part of 2015 that would give law enforcement some sort of special access or back door to encrypted devices when they are duly authorized by a court order. This is a reasonable and even admirable position that seeks to keep America safe.

Unintended Consequences of What the FBI Wants

Regrettably, this issue is not that simple. Many of the best technical minds and companies have stated that allowing special access or (as in this case) creating software to disable passcode protections could have at least four unintended consequences.

First, some have argued that once this software tool is created, other countries will ask for it as well. While nothing stops other countries from demanding such a workaround, Apple and other technology companies can legitimately claim that they do not have it.[10] That ends once Apple creates the tool. Other countries could use this tool solely for legitimate law enforcement purposes, but they could also turn it against dissidents.

Second, creating software that weakens the protections around devices will result in persistent, widespread technological vulnerability. This software would enable whoever possesses it to unlock any iPhone 5c and possibly other iPhones as well. The FBI could certainly end up requesting such a workaround for other phones and devices. As a result, millions of devices would be vulnerable if the

1. Hearing, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, Committee on the Judiciary, U.S. House of Representatives, 114th Cong., 2nd Sess., March 1, 2016, https://www.youtube.com/watch?v=g1GgnbN9oNw (accessed March 14, 2016).
2. Digital Security Commission Act of 2016, H.R. 4651, 114th Cong., 2nd Sess., https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf (accessed March 14, 2016).
3. U.S. District Court for the Central District of California, "Order Compelling Apple, Inc. to Assist Agents in Search," Politico, February 16, 2016, http://www.politico.com/f/?id=00000152-ecf7-d79c-a57b-fef7defc0001 (accessed March 14, 2016).
4. U.S. District Court for the Central District of California, "Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance," Document Cloud, February 25, 2016, https://assets.documentcloud.org/documents/2722203/Motion-to-Vacate-Brief-and-Supporting-Declarations.pdf (accessed March 14, 2016).
5. United States District Court Eastern District of New York, "In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court," Document Cloud, February 29, 2016, https://assets.documentcloud.org/documents/2728314/Orenstein-Order.pdf (accessed March 14, 2016).
6. Richard M. Thompson II and Chris Jaikaran, "Encryption: Selected Legal Issues," Congressional Research Service *Report for Congress* No. 44407, March 3, 2016, http://www.fas.org/sgp/crs/misc/R44407.pdf (accessed March 14, 2016).
7. *United States v. New York Tel. Co.*, 434 U.S. 159 (1977).
8. See discussion of the Communications Assistance for Law Enforcement Act (CALEA) in Thompson and Jaikaran, "Encryption: Selected Legal Issues."
9. Federal Bureau of Investigation, "Going Dark Issue," March 1, 2016, https://www.fbi.gov/about-us/otd/going-dark-issue (accessed March 14, 2016).
10. Some have raised good questions regarding Apple's security arrangements with China and to what extent they may already have weakened their security in that country. Stewart Baker, "Deposing Tim Cook," Lawfare, February 27, 2016, https://www.lawfareblog.com/deposing-tim-cook (accessed March 14, 2016).

software tool were to fall into the hands of hackers or other countries.

Third, further innovation could stifle the FBI's demands and create an encryption arms race. Apple is already designing upgrades to iPhone that would make it impossible to disable the protections the FBI wants disabled.[11] The FBI would then have to make ever more burdensome and difficult demands on private companies. Of course, bad actors will also respond and the sophisticated ones will use encryption applications like Telegram or WhatsApp.[12] A survey of encryption technologies available today found that there are at least 546 encrypted products designed outside the U.S.[13] The companies designing these products, especially those in foreign countries, are not going to help the FBI work around or through their encryption, which means that bad actors will still have access to encryption regardless of the outcome of this debate.

Fourth, several legal questions have emerged in the San Bernardino case brought by the Department of Justice. These include arguments that forcing Apple to create software would run afoul of the First amendment by forcing Apple to speak.[14] Another concern is what the limiting principle is in this case. If the government can order Apple to develop software to crack its own encryption, what is to stop it from ordering Apple to turn on the audio record function of a suspected criminal? This unclear limit on what the government could force Apple or other technology companies to do under such an AWA precedent is problematic.

The Way Forward

In response to conflicting priorities in a highly technical issue, lawmakers on both sides of the aisle, as well as Apple, have suggested the idea of an encryption commission to leverage the expertise and perspectives of different stakeholders. This issue has important security implications, but regrettably, some have been quick to dismiss the other side and question motivations as less than charitable.

Rather than Members talking past each other, Congress should:

1. **Not rush to a solution.** Given the many implications of this issue, Congress should not rush to a decision based on one difficult case. Cooler heads and deliberation should prevail.

2. **Consider a commission to study the issue of encryption and the going dark problem.** This commission would help Congress and all interested parties to discern what the technical realities are, what the benefits and risks of encryption are, and what the consequences of action or inaction on this issue are. While this commission would not help the FBI right now, it is worth the time to understand this complex issue.[15] Some of these arguments and challenges will not have easy solutions, but a well-balanced commission will provide policymakers with the facts they need to make an informed judgement.

3. **Maintain essential counterterrorism tools.** Support for important investigative tools is essential to maintaining the security of the U.S. and combating terrorist threats. Legitimate government surveillance programs are also a vital component of U.S. national security and should be allowed to continue. The need for effective counterterrorism operations does not relieve

11. Matt Apuzzo and Katie Benner, "Apple Is Said to Be Trying to Make It Harder to Hack iPhones," *The New York Times*, February 24, 2016, http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?_r=0 (accessed March 14, 2016).
12. Matt Apuzzo, "WhatsApp Encryption Said to Stymie Wiretap Order," *The New York Times*, March 12, 2016, http://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html?_r=0 (accessed March 15, 2016).
13. Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Schneier, February 11, 2016, https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf (accessed March 14, 2016).
14. Andrew Keane Woods, "Trust, Apple, and the First Amendment," Lawfare, February 23, 2016, https://www.lawfareblog.com/trust-apple-and-first-amendment (accessed March 14, 2016).
15. In the meantime, the court cases will go forward and the FBI could make use of novel, though difficult, hacking techniques to try to access the information of select iPhones. So-called destructive analysis could be a unique solution to this hard case. Nicholas Weaver, "How to Destroy Pandora's iPhone," Lawfare, February 26, 2016, https://www.lawfareblog.com/how-destroy-pandoras-iphone (accessed March 14, 2016), and Robert McMillan, "Chip Hacking Might Help FBI Unlock iPhones," *The Wall Street Journal*, March 3, 2016, http://www.wsj.com/articles/chip-hacking-might-help-fbi-unlock-iphones-1457050959 (accessed March 14, 2016).

the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well.

Advancing Security

The encryption debate is an important one to have. Factual clarity and an understanding of various perspectives and arguments are important to developing beneficial policies. A commission to study this important but complicated issue would provide such clarity and create the forum for wrestling with important priorities. The deliberate way forward presents a path for advancing policy that will protect the American people and their devices.

*—**David Inserra** is a Policy Analyst for Homeland Security and Cyber Policy in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. **James Jay Carafano, PhD**, is Vice President of the Davis Institute and E. W. Richardson Fellow at The Heritage Foundation. **Charles D. Stimson** is Manager of the National Security Law Program and Senior Legal Fellow in the Davis Institute. **Steven P. Bucci, PhD**, is Director of the Allison Center. **David Shedd** is Visiting Distinguished Fellow in the Davis Institute. **Paul Rosenzweig** is a Visiting Fellow in the Davis Institute.*