The Heritage Foundation

ISSUE BRIEF

No. 4459 | SEPTEMBER 04, 2015

Encryption and Law Enforcement Special Access: The U.S. Should Err on the Side of Stronger Encryption

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

A debate is currently raging between FBI Director James Comey and much of the technology community over whether law enforcement should have some sort of special access, which has been called a backdoor, into encrypted communications and data.[1] In this "Crypto War," the FBI contends that special access is needed to access the communications and data of criminals and terrorists. However, many in the technology community argue that this will undermine the cybersecurity of all communications and will not work because some users will find alternative services to encrypt their communications.

Given these constraints and competing security demands, no decision on special access will satisfy legitimate but competing interests. Heritage scholars have long supported the use of lawful tools by law enforcement and the intelligence community in order to keep the U.S. safe, but we cannot ignore technological advances. The case for special access by law enforcement to encrypted materials is one with noble objectives and intentions, but the reality is that technology has changed as to make this policy detrimental to cybersecurity and data integrity, with no guarantee of success. Given these cybersecurity realities, the U.S. should not require technology and communication companies to provide law enforcement with special access to encrypted materials.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4459

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

Encryption 101

Encryption is the process by which data, be they words, numbers, photographs, etc., are coded so that anyone who acquires the data is unable to read it without knowing and then applying the algorithm that was used to encode it. Encryption has been used since ancient times as messages were written in a code that only someone with the key could decipher. More recently, in the 1840s, Samuel Morse developed a code (which bore his name) that assigned a set of dots and dashes to each letter of the alphabet and then was used to transmit messages across telegraph lines. The universal international distress signal for ships, SOS ("save our ship") was expressed in Morse code as ••• ——— •••.

As computers advanced, so too has the ability to create ever more complicated codes, effectively surpassing the ability of decryption techniques to break an encryption. This point is important to emphasize as it is a dramatic change from the past. Today, *properly encrypted data cannot be cracked*, at least not efficiently enough to be of use in a criminal or terrorist investigation.[2] Director Comey recently agreed, stating, "We cannot break strong encryption."[3]

Encryption can be used to ensure that communication between two parties is protected or to protect data at rest, that is, data residing on a hard drive. Many communications and technology firms may encrypt users' communications that pass through or reside on their servers, but the firms hold the key to decrypt the data. With end-to-end encryption, though, only the computers at each end of a communication have the encryption keys and only they can read the messages, with the service provider itself unable to read the data.

What the FBI Wants and Why It Is Problematic

The FBI wants some sort of special access to encrypted systems, which will give law enforcement access to a master encryption key (or keys) needed to decrypt data residing on or passing through a system. This special access creates a single point of vulnerability into systems, exactly what organizations and individuals are increasingly trying to avoid. According to a recent report produced by encryption experts, special access not only undermines the confidentiality of data, but also its authenticity, i.e., hackers who acquire the master keys would be able to forge communications and make them look legitimate.[4]

At the crux of this debate is the fact that special access provided to law enforcement undermines the security of systems. If true, then this is a zero-sum situation: Either cybersecurity is paramount or law enforcement gets special access to catch bad guys. That said, legitimate questions have been raised about just how absolute is this trade-off. Brookings Institution scholar Ben Wittes points out that Google "retains the ability to decrypt Gmail and Gchat communications for its own business reasons; that's how it routes you ads based on the contents of your material. To my knowledge, Google does not take the position that this service is insecure, nor do I know of any particular security issues that have arisen as a result of it."[5] Is Google currently less secure than an amateur's end-to-end encryption?[6] The security vulnerability resulting from special access is one of the fundamental points in this debate, and technologists should clarify the reality of that vulnerability.[7]

Even if Congress mandates some sort of special access, there is no guarantee that it would be the effective solution law enforcement wants, since criminals and terrorists could just buy different products that do not have a backdoor. American-based Apple and Google may be required to provide special access, but what about a company outside U.S. jurisdiction that sells end-to-end encryption communications applications? Will the United States try to ban them on the app stores for iTunes and Google Play? Will we ban the import of encryption technology and search for such technology at U.S. ports of entry to ensure forbidden applications are not smuggled into our country? Will the United States employ a national firewall, similar to China, to block the downloading or use of such applications?[8] The answers to these questions should be

1. James Comey, "Encryption, Public Safety, and 'Going Dark'," Lawfare, July 6, 2015, http://www.lawfareblog.com/encryption-public-safety-and-going-dark (accessed September 1, 2015).
2. Matt Buchanan, "Hard to Crack: The Government's Encryption Conundrum," *The New Yorker*, August 15, 2013, http://www.newyorker.com/tech/elements/hard-to-crack-the-governments-encryption-conundrum (accessed September 1, 2015). Quantum computing, which uses unique properties of quantum mechanics, could change this status quo, but it is not yet available in a practical form. "Quantum Computing 101," Institute for Quantum Computing, University of Waterloo, https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101 (accessed September 1, 2015); Mary-Ann Russon, "NSA Worried that Quantum Computing Will Foil the Cryptography Protecting All Data to Date," *International Business Times*, August 24, 2015, http://www.ibtimes.co.uk/nsa-worried-that-quantum-computing-will-foil-cryptography-protecting-all-data-date-1516795 (accessed September 1, 2015).
3. Dina Temple-Raston, "FBI Director Says Agents Need Access To Encrypted Data To Preserve Public Safety," *NPR*, July 8, 2015, http://www.npr.org/sections/thetwo-way/2015/07/08/421251662/fbi-director-says-agents-need-access-to-encrypted-data-to-preserve-public-safety (accessed September 1, 2015).
4. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, July 6, 2015, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf (accessed September 1, 2015).
5. Benjamin Wittes, "Five Hard Encryption Questions," Lawfare, August 7, 2015, https://www.lawfareblog.com/five-hard-encryption-questions (accessed September 1, 2015).
6. Even if a large service provider is less secure, the solution (i.e., end-to-end encryption) may be difficult for an individual or small organization to operate effectively. If this is the case, continuing to rely on the superior resources and expertise of the large provider may still be the most cost-effective option.
7. Stewart Baker, "Encryption: If This Is the Best His Opponents Can Do, Maybe Jim Comey Has a Point," *The Washington Post*, July 12, 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/12/encryption-if-this-is-the-best-opponents-can-do-maybe-jim-comey-has-a-point/ (accessed September 1, 2015).
8. Harold Abelson et al., "Keys Under Doormats."

"no," as we cannot prevent the spread of this technology and it would be futile to try. Some criminals and terrorists will not use encrypted technologies, but others will.

Adapting to Change

In light of these realities, Congress should not support special access for law enforcement. The current debate indicates that such access will substantially weaken cybersecurity and incent criminals and terrorists to switch from U.S. applications to foreign ones. Former intelligence and homeland security policymakers also have concluded that.[9] The only circumstance under which special access should be considered is if it can be done while maintaining an extremely high level of security. Different potential solutions that have been suggested include:

- **Biometrics.** The use of encryption with a biometric lock provides decent protection for the decryption key. This allows law enforcement to break an encryption through direct interaction with the individual being investigated or charged.[10]

- **Dividing the law enforcement key among several organizations.**[11] This was a solution proposed by Admiral Michael Rogers, the Director of the National Security Agency, which ensures that no one person or agency can decrypt data. While breaking up the key may improve some aspects of security and privacy, it will likely introduce additional complexity and vulnerabilities to the encryption process. It is also unclear how communication across different countries would work.[12]

- **Requiring that any potential solution be publically and extensively tested.** Rather than develop a specific solution, perhaps a good compromise would be to require that any potential solution be made publically available and tested for a year. If it cannot be cracked, then it can be used for special access.[13]

This list is not exhaustive nor are its proposals perfect. Technologists and policymakers alike should explore other proposals. Further investigation of the issue could reveal that large technology service providers like Google are able to securely hold the special access keys, making law enforcement special access to encrypted communications possible without jeopardizing the security of that data. Until this is determined or other solutions present themselves, however, the cybersecurity stakes are too high to provide special access.

Setting a high bar for special access means that law enforcement and the intelligence community need all other lawful tools at their disposal to track and prevent threats to the United States.[14] Given the growing threat of terrorism, these tools are needed now more than ever.[15]

Special access to encrypted systems and communications, however, cannot be one of those tools, at least until the security of such access is assured. The United States can and should see if it is possible to maintain both cybersecurity and special access. In the meantime, one of these important priorities has to give. Keeping the U.S. homeland safe and secure from multiple, dynamic threats is not easy, but policymakers should err on the side of not providing special access, while providing our defenders with all other lawful tools.

9. Mike McConnell, Michael Chertoff, and William Lynn, "Why the Fear over Ubiquitous Data Encryption Is Overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?postshare=5691438283703237 (accessed September 1, 2015).
10. Paul Rosenzweig, "Encryption, Biometrics, and the Status Quo Ante," Lawfare, July 6, 2015, http://www.lawfareblog.com/encryption-biometrics-and-status-quo-ante (accessed September 1, 2015).
11. Ellen Nakashima and Barton Gellman, "As Encryption Spreads, U.S. Grapples with Clash between Privacy, Security," *The Washington Post*, April 10, 2015, https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html (accessed September 1, 2015).
12. Harold Abelson et al., "Keys Under Doormats."
13. Paul Rosenzweig, "Testing Encryption Insecurity: A Modest Proposal," Lawfare, July 7, 2015, http://lawfareblog.com/testing-encryption-insecurity-modest-proposal (accessed September 1, 2015).
14. James Jay Carafano et al., "Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward," Heritage Foundation *Backgrounder* No. 3018, May 21, 2015, http://www.heritage.org/research/reports/2015/05/section-215-of-the-patriot-act-and-metadata-collection-responsible-options-for-the-way-forward.
15. David Inserra, "Terror in Paradise: 73rd Terrorist Plot Highlights Need to Act," Heritage Foundation *Issue Brief* No. 4449, August 4, 2015, http://www.heritage.org/research/reports/2015/08/terror-in-paradise-73rd-terrorist-plot-highlights-need-to-act.

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