NEW AMERICA

August 2019

Brief: Separating the Fact from Fiction

Attorney General Barr is Wrong About Encryption

Andi Wilson Thompson

Last edited on August 12, 2019 at 9:28 a.m. EDT

About the Author(s)

Andi Wilson Thompson is a senior policy analyst at New America's Open Technology Institute where she focuses on issues including digital security, vulnerabilities equities, encryption, and internet freedom.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Attorney General Barr is Wrong About Encryption 5

Attorney General Barr is Wrong About Encryption

This piece is supported by Access Now, Center for Democracy & Technology, Electronic Frontier Foundation, Engine, Internet Society, New America's Open Technology Institute, and TechFreedom.

Attorney General William Barr's recent remarks on encryption at the International Conference on Cyber Security were full of misleading statements and misguided reasoning.[1] Strong digital encryption is the bedrock infrastructure that allows everyday people, businesses, and our government to trust technology for critical needs. Barr's demand that tech companies give law enforcement special access to encrypted devices would seriously violate that trust, compromising the security of potentially billions of people by creating a vulnerability that criminals and terrorists could easily exploit. Moreover, research indicates that the targets mentioned in Barr's remarks would quickly migrate to new encrypted services, ensuring law enforcement receives no benefit from the public's concession of privacy.

Read on to learn the facts when it comes to encryption, and how they refute the fiction from Barr's speech.

1) The barriers to law enforcement posed by encrypted communications have been greatly exaggerated.

> ***Fiction:*** *"Because, in the digital age, the bulk of evidence is becoming digital, this form of "warrant proof" encryption poses a grave threat to public safety by extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes. It allows criminals to operate with impunity, hiding their activities under an impenetrable cloak of secrecy. As you know, some refer to this eclipsing of the Government's investigative capabilities as "going dark."*[1]

FACT: This familiar talking point has been repeatedly debunked. During the *Apple v. FBI* litigation, the FBI claimed that relevant and critical communications data resided on a locked phone that they could not access due to encryption.[2] A subsequent Office of Inspector General report detailed that the FBI could have gotten into the phone with the help of a private contractor, but chose to sue Apple to compel them to develop a workaround that would have circumvented the security on all their devices.[3] Moreover, press reporting has made it known that after the FBI unlocked the phone, there was no useful data.[4]

FACT: The only statistics that the FBI has put forward to illustrate the cost of encryption were grossly inflated. In 2018, the FBI was forced to admit that they overstated the number of phones they claimed were inaccessible due to

encryption. FBI Director Wray's claim to Congress that, in 2017, the FBI had seized 7,800 phones that were inaccessible to encryption was subsequently contradicted when an internal FBI estimate of 1,200 phones became public.[5] Though the FBI promised to provide new data, it has been over a year and they still have not produced a revised number.

FACT: A survey of law enforcement investigators shows that encryption is not the biggest digital evidence challenge they face. In fact, it is often much simpler—police officers don't know what data is available, which provider has it, and how to go about getting and making sense of it. According to the Center for Strategic & International Studies, their survey of federal, state, and local law enforcement officials "suggests that challenges in accessing data from service providers—much of which is not encrypted—the biggest problem that they currently face in terms of their ability to use digital evidence in their cases."[6] In fact, there is an enormous amount of unencrypted data available to law enforcement that has not been available in the past. For example, encryption typically does not protect metadata, providing access to information like e-mail addresses, mobile-device location information, IP address, browsing data, and other information that can be extremely valuable to investigators.[7]

FACT: Many private contractors advertise products to law enforcement agencies that can unlock any device on the market. Just recently, the company Cellebrite bragged that its technology can bypass the security of any iPhone.[8] According to reports, many U.S. agencies, including the FBI, the Secret Service, and Immigration and Customs Enforcement, have purchased similar technology.[9]

2) If companies build law enforcement access mechanisms into encrypted products, targets of investigations will simply move to using different encrypted services.

> ***Fiction:*** *"We also found that the cartel had used WhatsApp for the specific purpose of coordinating the murders of Mexico-based police officials. The cartel ended up murdering hundreds of these police officers. Had we been able to gain lawful access to the chat on a timely basis, we could have saved these lives."*

FACT: Any proposal that undermines user trust penalizes the overwhelming majority of technology users while permitting those few bad actors to shift to readily available products beyond the law's reach. It is a reality that encryption products are available all over the world and cannot be easily constrained by territorial borders. Thus, while the few nefarious actors targeted by the law will still be able to avail themselves of other services, average users—who may also choose different services—will disproportionately suffer the consequences of degraded security and trust.

3) Encryption backdoors in consumer products could have serious cybersecurity and national security implications.

> ***Fiction:*** *"Particularly with respect to encryption marketed to consumers, the significance of the risk should be assessed based on its practical effect on consumer cybersecurity, as well as its relation to the net risks that offering the product poses for society. After all, we are not talking about protecting the Nation's nuclear launch codes. Nor are we necessarily talking about the customized encryption used by large business enterprises to protect their operations. We are talking about consumer products and services such as messaging, smart phones, e-mail, and voice and data applications."*

FACT: To suggest there is a difference between consumer encryption and other types of encryption is seriously misguided. Critical infrastructure runs on consumer products and services and is protected by the same encryption that protects individual consumers of those products and services. Every day, millions of people connect to the nation's critical infrastructure—the power grid, transportation systems, the financial system—via their phones or computers. Employees at these entities often connect to internal sites to manage operations or exchange sensitive information that enables the smooth operation of lifeline services. The same encryption present on your smartphone or tablet protects these interactions and is vital to the security of the nation's critical infrastructure. Moreover, employees of the federal government, including at agencies like the FBI, CIA, and NSA, rely on consumer devices to communicate sensitive information. In fact, the NSA developed a program called Commercial Solutions for Classified that allows Department of Defense officials to transmit classified information using commercial encryption solutions. It is patently false to suggest that weakening consumer encryption would have no effect on national security.[10]

FACT: A backdoor is a method of bypassing normal authentication or encryption. The same backdoors that allow special access to law enforcement agencies would also provide an opportunity for terrorists, criminals, and other parties to gain unauthorized access. History has shown us that once backdoors are created, it's only a matter of time before other parties gain access to them as well.

4) Strong encryption protects us from both online *and* physical threats.

> ***Fiction:*** *"Hackers are a danger, but so are violent criminals, terrorists, drug traffickers, human traffickers, fraudsters, and sexual predators. While we should not hesitate to deploy encryption to protect ourselves from cybercriminals, this should not be done in a way that eviscerates society's ability to defend itself against other types of criminal threats."*

FACT: Encryption protects the public not just against cybercrimes, but also against crimes that cause physical injury and death. At a recent conference on encryption policy, Cindy Southworth, the executive vice president at the U.S. National Network to End Domestic Violence (NNEDV), cautioned against introducing an exceptional access mechanism for law enforcement, in part, because of how it could threaten the safety of victims of domestic and gender-based violence. Specifically, she warned that "[w]e know that not only are victims in every profession, offenders are in every profession...How do we keep safe the victims of domestic violence and stalking?"[11]

FACT: Vulnerable populations like journalists and activists use encryption to protect themselves, their sources, and their community. For example, in June 2019 protesters in Hong Kong used the encrypted messaging app Telegram to coordinate actions and protect themselves from government interception of communications.[12] A lack of digital security for these individuals can have very real physical consequences. Not only can governments with less respect for human rights take advantage of intentional vulnerabilities to surveil these populations, but the lives of at-risk individuals could be in danger without the ability to communicate securely. In a recent example, Amnesty International filed a lawsuit against a spyware company, which had exploited a vulnerability in WhatsApp to develop special software used by intelligence agencies to covertly take control of a person's phone.[13]

5) A lack of motivation isn't the reason that much of the tech community has expressed unwillingness to build law enforcement access mechanisms into encrypted products.

> ***Fiction:*** *"It is well past time for some in the tech community to abandon the indefensible posture that a technical solution is not worth exploring and instead turn their considerable talent and ingenuity to developing products that will reconcile good cybersecurity to the imperative of public safety and national security."*

FACT: The tech community has repeatedly engaged with governments and law enforcement agencies around the world to understand the challenges they face and evaluate any lawful access proposals offered. To suggest that the tech community's obstinance is the reason that a technical "solution" hasn't been developed is false and conveniently ignores the facts. There is no way to provide government access to encrypted data without creating vulnerabilities that malicious actors can exploit. Even the Attorney General acknowledges that allowing for extraordinary access creates security risks.

FACT: Technologists cannot build systems that can inherently tell when "bad" people use them, just as engineers cannot design sidewalks and highways to

crumble underneath the feet of certain people, because in both cases there is a chance that we'll build something that is unsafe for all users. It is no different in communications infrastructure, where widely available engineered backdoors or exceptional access mechanisms could be used by unauthorized parties, malicious hackers, or governments that do not share a commitment to human rights.

6) Protecting software signing keys presents different challenges from managing decryption-capable keys.

> ***Fiction:*** *"Such encryption regimes already exist. For example, providers design their products to allow access for software updates using centrally managed security keys. We know of no instance where encryption has been defeated by compromise of those provider-maintained keys. Providers have been able to protect them."*

FACT: The types of systems that tech companies have developed to permit software updates do not provide models for exceptional access because protecting signing keys for updates is fundamentally different than safeguarding decryption keys, and they present different and unique challenges. When stolen, a decryption key would give bad actors carte blanche access to sensitive data with no risk of discovery.

FACT: A software update is both revocable and remediable, while unlocking a device and extracting data is neither. If someone managed to steal signing keys that are used for software updates, their ability to abuse them could be constrained once it was discovered. For example, the software provider can issue a new software update signing key and revoke any old compromised keys. Every user who receives this update will be protected against future attacks that use the old compromised keys. Moreover, software update signing keys also typically have time-limited windows of utility by default, and are changed regularly. No such expiry is possible with exceptional access decryption keys—once encrypted data is publicly exposed (e.g. sent in transit), decryption capability cannot be revoked. If a decryption-capable "extraordinary access" key is compromised, *all* data ever encrypted to that key can be decrypted by the attacker as long as they have a copy of the ciphertext.

FACT: Barr's statement that he knows of no instances where provider-maintained keys have been compromised is dangerous and disingenuous, because there have been several high-profile and very destructive examples of attacks that leverage compromised certificate signing keys. Stuxnet, for instance, which reportedly targeted an Iranian nuclear facility but propagated globally, exploited software signing keys from JMicron and Realtek as part of its attack mechanism. Those certificates were subsequently revoked, because their misuse was detected when Stuxnet was exposed.

Several months ago, hackers reportedly broke into computer hardware company ASUS and used compromised signing keys to distribute malware to a million users.[14] In 2017, researchers found 189 malware samples bearing valid digital signatures created by compromised certificates used to sign legitimate software.[15]

7) Other countries' proposals to weaken encryption are bad models for effective U.S. policy and do not provide safe mechanisms for law enforcement access.

> ***Fiction:*** *"Some good minds have already started to focus on this, and some promising ideas are emerging. Our colleagues from GCHQ have proposed "Virtual Alligator Clips" which allow a provider to respond to a warrant by adding a silent law enforcement recipient to an otherwise secure chat."*

FACT: The proposal by GCHQ, the U.K.'s intelligence agency, involves adding a "ghost" user into encrypted chats. This proposal would require messaging providers to suppress normal notifications to users, meaning users would be unaware when a law enforcement participant had been added and could see the plaintext of their encrypted conversation. Although the GCHQ officials claim that "you don't even have to touch the encryption" to implement their plan, the "ghost" proposal would pose serious threats to cybersecurity. Among other problems, it would undermine authentication systems, so that people could no longer know who they were communicating with.[16] The ghost proposal would introduce a security threat to all users of a targeted encrypted messaging application since the proposed changes could not be exposed only to a single target. In order for providers to be able to suppress notifications when a ghost user is added, messaging applications would need to rewrite the software that every user relies on. This means that any mistake made in the development of this new function could create an unintentional vulnerability that affects every single user of that application.

FACT: The expectation that other countries will not make similar demands of companies is unrealistic. For example, countries like China have sought access to encrypted messaging, and if the United States requires companies to provide access to law enforcement, it provides ammunition for foreign governments to push for access as well. Governments could also be incentivized to exploit vulnerabilities that companies include in their products in order to give U.S. agencies access to their users' data.

Ultimately, Barr's case for an encryption backdoor fails to recognize reality. In exchange for fundamentally compromising digital security, law enforcement will likely receive little to no investigative benefit. Furthermore, Barr's aims would

hurt U.S. national security and threaten the human rights of people around the world.

Law enforcement is equipped with a vast array of effective tools for pursuing successful investigations; it does not need to attack the public's basic digital privacy protections only to make us all worse off in the end.

Notes

1 Attorney General William P. Barr, “Keynote Address at the International Conference on Cyber Security,”New York, NY, Tuesday, July 23, 2019. All included quotations from Attorney General Barr’s remarks
are available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

2 Aaron Pressman, “The Secret History of the FBI’s Battle Against Apple Reveals the Bureau’s Mistakes,” Fortune, March 27, 2018, https://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/.

3 Office of the Inspector General U.S. Department of Justice, “A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation,” March, 2018, available at https://oig.justice.gov/reports/2018/o1803.pdf.

4 Russell Brandom, “The FBI has gotten no new leads from the San Bernardino iPhone,” *The Verge,* April 19, 2016, https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads.

5 Devlin Barrett, “FBI repeatedly overstated encryption threat figures to Congress, public,” *Washi ngton Post*, May 22, 2018, https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.ade0540be964.

6 William A. Carter and Jennifer C. Daskal, “Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge,” *Center for Strategic and International Studies*, July 2018, available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN.

7 Zittrain, Jonathan L., Matthew G. Olsen, David O'Brien, and Bruce Schneier. 2016. "Don't Panic: Making Progress on the “Going Dark” Debate." Berkman Center Research Publication 2016-1, available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

8 Andy Greenberg, “Cellebrite Says It Can Unlock Any iPhone for Cops,” *Wired*, June 14, 2019, https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/.

9 Joseph Marks, “The Cybersecurity 202: Federal Agencies are Spending Millions to Hack into Locked Phones,” *Washington Post,* May 13, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/13/the-cybersecurity-202-federal-agencies-are-spending-millions-to-hack-into-locked-phones/5cd8bc5b1ad2e544f001dcce/?utm_term=.985c1bce2b48.

10 “Four Future Trends in Tactical Network Modernization,” U.S. Army, January 14, 2019, https://www.army.mil/article/216031/four_future_trends_in_tactical_network_modernization.

11 “How Encryption Saves Lives and Fuels our Economy,” New America, Nov. 27, 2018, https://www.newamerica.org/oti/events/how-encryption-saves-lives-and-fuels-our-economy/.

12 Danny Vincent, “How Apps Power Hong Kong's 'Leaderless' Protests,” June 30, 2019, https://www.bbc.com/news/technology-48802125.

13 Dan Sabbagh, “Israeli Firm Linked to WhatsApp Spyware Attack Faces Lawsuit,” *The Guardian*, May 18, 2019, https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit.

14 Zack Whittaker, “Hackers dropped a secret backdoor in Asus’ update software,” *Tech Crunch*, March 25, 2019, https://techcrunch.com/2019/03/25/asus-update-backdoor/.

15 Kim, Doowon, Bum Jun Kwon, and Tudor Dumitras, ‘Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI,” Proceedings of the 2017 ACM SIGSAC Conference on Computerand Communications Security (2017), CCS ’17, available at http://users.umiacs.umd.edu/~tdumitra/papers/CCS-2017.pdf.

16 Open Coalition Letter to GCHQ Regarding the “Ghost” Proposal, May 22, 2019, available at https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

• **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.