Free markets. Real solutions.

CONTENTS

R STREET POLICY STUDY NO. 133
March 2018

POLICY APPROACHES TO THE ENCRYPTION DEBATE

Charles Duan, Arthur Rizer, Zach Graves and Mike Godwin

INTRODUCTION

A fierce debate has been ongoing for many years over strong computer encryption of communications and data, which can both deliver security and privacy for individuals but also make it difficult for the intelligence and law enforcement communities to perform their surveillance and investigative duties. In particular, the question of whether encryption systems should be required to have a "backdoor" to give the government special access to encrypted information remains divisive.[1]

Views on the question seem diametrically opposed: law enforcement communities contend that crime and terror will reign if the government cannot read all encrypted messages and information; by contrast, companies, technologists and civil liberties advocates decry the devastation to individual rights and public security if strong encryption is compromised. These polarized views have left policymakers at an impasse.

However, such seemingly irreconcilable perspectives on either side of the debate arise primarily because encryption policy is treated as a thought experiment, often with oversimplified facts coupled with a great deal of certainty. For example, the most commonly employed hypothetical scenario involves the following: an encrypted message or communication that—if only the government were able read it—would reveal the secrets required to stop a deadly attack or to bring a terrorist to justice.

This resembles another famous thought experiment: the "ticking time bomb," where torturing a suspect is the guaranteed and only means to defuse the bomb.[2] While this latter conundrum has also generated volumes of polarized debate, its most pragmatic solution is one that can also be applied to the issue of encryption, which is to reject the hypothetical's frame. This requires the realization that the thought experiment's simplified assumptions are not consistent with reality, accompanied by a shifted focus onto real-world questions about whether and how actual systems might be implemented.

Consistent with this pragmatic analysis, we believe that the right approach to the encryption debate is to consider three questions that must be answered before any encryption backdoor could possibly be advisable: whether there is empirical

1. "*Don't Panic: Making Progress on the 'Going Dark' Debate*," Berkman Center for Internet and Society, Feb. 1, 2016, pp. 5–7. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf; "Decrypting the Encryption Debate: A Framework for Decision Makers," National Academy of Sciences, 2018, pp. 6–7. https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers.

2. See, e.g., Fritz Allhoff, "A Defense of Torture: Separation of Cases, Ticking Time-Bombs, and Moral Justification," International Journal of Applied Philosophy 19:2 (2005), p. 243. http://files.allhoff.org/research/A_Defense_of_Torture.pdf.

evidence of a need for and benefit of a backdoor; whether there is a satisfactory technical solution; and whether law and policy can implement that technical solution. In contrast to the purely theoretical nature of the issue currently, each of these is amenable to experimentation, evidence-based debate and thoughtful discussion. Nevertheless, given the facts known today, it is unlikely that the associated hurdles will be overcome. Moreover, it is nearly impossible to overcome them all. That said, there is at least a way forward if stakeholders are willing to explore the three-part, real-world framework of cost–benefit analysis, adversarial testing of technology and policy implementation.

Accordingly, the present study provides background on encryption, backdoors, the "going dark" problem and the current debate. It then reviews each of these three prongs, develops a portion of the analytical framework, applies the facts as known today, and identifies policy proposals and points of future study in order to advance the discussion past its current stalemate.

ENCRYPTION: AN OVERVIEW

Encryption is a method by which a message or other information is converted by a mathematical process such that the original message can only be recovered with a "key," usually a numerical value that can undo the code.[3] For example, a simple form of encryption would be to systematically replace letters in a message with other letters. In this case, the encryption key would be the table of letter replacements.[4]

The purpose of modern encryption is largely twofold. First, it prevents eavesdroppers from listening in on private conversations. Second, it provides those participating with assurance that they are talking with the people they expect.[5] This makes modern encryption an important tool for numerous private applications. For example, e-commerce transactions are encrypted to prevent thieves from stealing credit card numbers. Email and cell phone calls are encrypted to stop eavesdropping, and data stored on computers and mobile devices are encrypted to prevent sensitive information from being accessed if those devices are lost or stolen.[6] Data encryption has thus become essential to basic economic life and societal participation, as it gives the public confidence to store and transmit personal and financial data on computer systems.

Perhaps more importantly, encryption is an important tool of free speech and individual liberty. Repressive governments often use surveillance of communications to keep tabs on their citizens and encryption can offer a degree of freedom from that surveillance.[7] As a recent United Nations Educational, Scientific and Cultural Organization (UNESCO) report explains, "restriction of the availability and effectiveness of encryption as such constitutes an interference with the freedom of expression and the right to privacy."[8]

The flipside of that individual liberty, however, is that encryption can be used to oppose government power, such as in military conflict against the nation, acts of terrorism or criminal behavior. As a result, governments have long had an interest in "breaking" encryption—that is, in applying various measures to obtain encryption keys or otherwise decipher encrypted messages. During the Second World War, for example, British computer scientist Alan Turing famously invented a mathematical engine that broke the German "Enigma" encryption.[9]

Encryption thus holds substantial value to individuals, but governments also see it as a threat that adversaries may deploy against the national interest. It is this tension that leads to the current debate over "going dark."

THE "GOING DARK" PROBLEM AND THE BACKDOOR DEBATE

A term used in the law enforcement field, particularly by the Federal Bureau of Investigation, "going dark" refers to the process by which encryption or other techniques obscure information in ways that prevent the government from accessing it, even in situations wherein the government is otherwise authorized by law to do so.[10] With the increasing prevalence of encryption, the FBI has expressed a "fear of missing out" on preventable crimes or prosecutable criminals, arguing that it cannot access the necessary evidence.[11]

3. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1137 (9th Cir. 1999).

4. Julius Caesar famously used this sort of encryption. See Suetonius, *De Vita Caesarum*, tr. J.C. Rolfe (William Heinemann: 1914), I, sec. 56. https://catalog.hathitrust.org/Record/001182041.

5. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1137.

6. S. Kelly, "*Security Implications of Using the Data Encryption Standard (DES),*" Internet Engineering Task Force RFC 4772, pp. 7–8, Dec. 2006. https://www.rfc-editor.org/rfc/rfc4772.txt.

7. Andy Greenberg, "Encryption App 'Signal' Is Fighting Censorship with a Clever Workaround," *Wired*, Dec. 21, 2016. https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround.

8. Wolfgang Schulz and Joris van Hoboken, "*Human Rights and Encryption*," UNESCO Series on Internet Freedom, 2016, p. 55. http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.

9. "The Enigma of Alan Turing," *Central Intelligence Agency*, April 10, 2015. https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html.

10. Testimony of Amy Hess, Executive Assistant Director, Federal Bureau of Investigation, Subcommittee on Information Technology of the House Committee on Oversight and Government Reform, "Encryption Technology and Potential U.S. Policy Responses," 114th Congress (GPO, 2015), p. 9. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

11. James B. Comey, Director, Federal Bureau of Investigation, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", Brookings Institution, Oct. 16, 2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

It is, of course, not novel to use encryption to thwart the prying eyes of government agents. Jefferson and Madison themselves encrypted their letters to prevent them from being read during the French Revolution.[12] Nevertheless, today's widespread adoption of encryption-enabled technology has led law enforcement to call vociferously for a technical solution to the problem of going dark.

The most commonly proposed solution is the installation of a "backdoor," or a generalized change to current encryption technologies that enables the government or law enforcement to read encrypted communications and stored data.[13] In 2015, for example, the FBI argued that it needs a "way to access encrypted systems and data," or else "many investigations could be at a dead end."[14] The problem, however, is that while there can be little objection to a theoretically perfect backdoor that only the government may access in permitted situations, no such perfect backdoor exists. Technology cannot inherently distinguish between good guys and bad guys, and thus any backdoor will open at least some possibility that hackers and rogue government officials will gain access.

Encryption backdoors are not a new idea within the federal government: There have been several historical examples of calls for—and even the successful installment of—backdoors in standard encryption systems, often at the behest of the National Security Agency. For example, the Data Encryption Standard (DES), which IBM developed in the 1970s with the NSA's input, has been alleged to include a form of backdoor—namely an encryption key size sufficiently small that "a $20 million machine can be built to break the proposed standard in about 12 hours of computation time."[15] The unsuccessful Clipper Chip proposal was another attempt to require a backdoor for government access.[16] And the Dual EC algorithm, adopted as part of federal encryption standards between 2006 and 2014, was widely suspected to have included one that gave the NSA a secret edge in guessing encryption keys.[17] This suspicion was confirmed by internal NSA documents later leaked by Edward Snowden.[18]

But the problem of going dark has attracted a great deal of recent attention, in part due to recent investigations of terrorist attacks involving encrypted cell phones,[19] and in part due to the introduction of default device encryption and new encryption services around 2014.[20] Indeed, as late as 2011 the FBI was not advocating for encryption backdoors. In fact, its representative testified to Congress that year that "[a]dressing the Going Dark problem does not require fundamental changes in encryption technology."[21] Today's narrative has shifted substantially. For example, this year, current FBI Director Christopher Wray called the need to redesign encryption-based systems to assist law enforcement "an urgent public safety issue."[22]

Debate over encryption backdoors is polarized. Law enforcement proponents that call for extensive access to encrypted data are firmly pitted against companies and civil society advocates who contend that any backdoor will fundamentally weaken technology, communications, the Internet and global competition.

Advocates on the law enforcement side have claimed that, with increasing prevalence of "default-on" encryption, to deny law enforcement a mechanism to access encrypted information will lead to more crimes going unsolved and further threats to public safety. James Comey, then-director of the FBI, remarked in 2014 that "encryption threatens to lead all of us to a very dark place."[23] Deputy Attorney General

12. John A. Fraser, III, "The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution," *Virginia Journal of Law and Technology* 2:1 (1997), p. 2. http://vjolt.org/wp-content/uploads/2017/Articles/vol2/issue/vol2_art2.html.

13. The term "backdoor" is used throughout only because it is the colloquial term currently used in policy discussions. See, e.g., John Leyden, "We Need to Talk About Mathematical Backdoors in Encryption Algorithms," *The Register*, Dec. 15, 2017. https://www.theregister.co.uk/2017/12/15/crypto_mathematical_backdoors. Other commentators have used phrases such as "extraordinary access" or "privileged access." But these are not necessarily preferable because they have other meanings in the information technology field. See, e.g., Sandra Henry-Stocker, "Unix: Controlling Privileged Access," *Network World*, July 28, 2014. https://www.networkworld.com/article/2696974/operating-systems/unix---controlling-privileged-access.html.

14. Testimony of Amy Hess, "Encryption Technology and Potential U.S. Policy Responses," p. 11. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

15. Whitfield Diffie and Martin E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, June 1977, p. 74. https://stacks.stanford.edu/file/druid:kf335sp7778/kf335sp7778.pdf.

16. A. Michael Froomkin, "The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution," *University of Pennsylvania Law Review* 143:3 (1995), p. 709. http://scholarship.law.upenn.edu/penn_law_review/vol143/iss3/3.

17. Bruce Schneier, "Did NSA Put a Secret Backdoor in New Encryption Standard?", *Wired*, Nov. 15, 2007. https://www.wired.com/2007/11/securitymatters-1115.

18. Nicole Perlroth, "Government Announces Steps to Restore Confidence on Encryption Standards," *The New York Times*, Sept. 10, 2013. https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards.

19. Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *The Washington Post*, April 12, 2016. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

20. Apple and Google announced default encryption for their devices in 2014, and an encrypted communications app, Signal, was released the same year. See Joe Miller, "Google and Apple to Introduce Default Encryption," *BBC News*, Sept. 19, 2014. http://www.bbc.com/news/technology-29276955; and Andy Greenberg, "Your iPhone Can Finally Make Free, Encrypted Calls," *Wired*, July 29, 2014. https://www.wired.com/2014/07/free-encrypted-calling-finally-comes-to-the-iphone.

21. Testimony of Valerie Caproni, General Counsel, Federal Bureau of Investigation, Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," 112th Congress (GPO, 2011), p. 12. http://judiciary.house.gov/_files/hearings/printers/112th/112-59_64581.pdf.

22. Christopher Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation," FBI International Conference on Cyber Security, Jan. 9, 2018. https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

23. Comey. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Rod Rosenstein has similarly warned: "Encrypted communications and devices pose the greatest threat to public safety when they are part of mass-market consumer devices and services that enable warrant-proof encryption by default."[24] Another FBI employee reportedly called Apple developers "jerks" and "evil geniuses" for making iPhone passwords more difficult to guess.[25]

The solution that law enforcement seeks has generally been a blanket obligation on software or device vendors to enable the government to retrieve unencrypted data or intercept unencrypted communications. The Manhattan District Attorney's Office has proposed federal legislation that requires smartphone and tablet manufacturers to render those devices "capable of being accessed by the designer in unencrypted form pursuant to a search warrant or other lawful authorization."[26] During his tenure as FBI director, Comey called instead for "a regulatory or legislative fix" to enable law enforcement to overcome encryption.

Denouncements of such proposals have been equally vigorous. In 2015, a group of fifteen computer scientists and security experts posited that encryption backdoors "are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm."[27] Cybersecurity experts have also warned that any encryption backdoor "may result in adverse collateral effects, affecting the competitiveness of American businesses and U.S. national security."[28] Representative Ted Lieu (a Stanford computer science graduate) has also quipped: "Creating a pathway for decryption only for good guys is technologically stupid. You just can't do that."[29]

Given such strong opinions about backdoors, opponents have largely expressed unwillingness to explore proposals on the subject. A 2015 letter signed by civil society organizations, companies, trade associations, and security and policy experts thus called on the Administration "to reject any proposal that U.S. companies deliberately weaken the security of their products."[30]

However, to a degree, such narrow, largely theoretical debates are oversimplifications. The question of whether we should or should not have backdoors for law enforcement must be predicated on a deliberate analysis of whether or not they are actually necessary and useful, technologically possible and/or implementable in the first place. These are practical questions about real-world systems, and more importantly they are amenable to evidence-based testing and discussion. Accordingly, the following sections analyze these three main questions that should be answered before any backdoor could be advisable.

QUESTION ONE: IS A BACKDOOR NECESSARY OR USEFUL?

No backdoor should be forced upon encrypted systems unless the benefits outweigh the costs. The costs are well known and established in other literature and include risks to national security,[31] increased public exposure to thieves and hackers,[32] injury to economic and global competitiveness,[33] and diminishment of individual privacy and liberty.[34]

The benefits of a backdoor should also be quantifiable. For example, statistics can be produced on the number of crimes that go unsolved or criminals who are not prosecuted successfully because key evidence was available but remained encrypted. If that quantitative evidence were produced, policymakers would then be faced with the likely difficult task of balancing the costs and benefits.

Lack of empirical evidence

As it stands, such evidence has not surfaced in the first place. The benefits of an encryption backdoor that proponents have

24. Rod J. Rosenstein, Deputy Attorney General, "Remarks at the U.S. Naval Academy," Oct. 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

25. Lorenzo Franceschi-Bicchierai, "FBI Hacker Says Apple Are 'Jerks' and 'Evil Geniuses' for Encrypting iPhones," *Vice: Motherboard,* Jan. 10, 2018. https://motherboard.vice.com/en_us/article/59wkkk/fbi-hacker-says-apple-are-jerks-and-evil-geniuses-for-encrypting-iphones.

26. "Smartphone Encryption and Public Safety: An Update to the November 2015 Report," Manhattan District Attorney's Office, November 2016, p. 32. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

27. Peter G. Neumann et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Communications of the ACM 58:10* (October 2015), p. 1. http://www.csl.sri.com/users/neumann/cacm237.pdf.

28. "*The Ground Truth About Encryption and the Consequences of Extraordinary Access," The Chertoff Group,* 2016, p. 17. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

29. "Encryption Technology and Potential U.S. Policy Responses," p. 69. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

30. "Letter from civil society organizations, companies, trade associations, and security and policy experts, to President Barack Obama," May 19, 2015, p. 1. https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

31. See, e.g., Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science and Technology Law Review* 13:2 (2012), pp. 454–57. http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization.

32. See, e.g., Kevin Bankston, "The Numbers Don't Lie: How Smartphone Encryption Will Help Cops More Than It Hurts Them," *Slate*, Aug. 18, 2015. http://www.slate.com/articles/technology/future_tense/2015/08/default_smartphone_encryption_will_stop_more_crimes_than_it_permits.html. A study by security firm Symantec found that those who find lost phones almost always try to access personal information on those phones, which suggests that unencrypted and unlocked phones are vulnerable to information or identity theft. See "*The Symantec Smartphone Honey Stick Project," Symantec*, 2012, pp. 12–13. http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf.

33. See, e.g., Swire and Ahmad, pp. 457–59. http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization.

34. See, e.g., Froomkin, pp. 811–12. http://scholarship.law.upenn.edu/penn_law_review/vol143/iss3/3.

offered so far are currently only theoretical and are most often presented within the scenario of a hypothetical criminal or terrorist using secure lines and encrypted phones. Although there have been several anecdotal suggestions that encryption interferes with investigations or crime prevention, proponents of backdoors have not yet demonstrably quantified their need.

With respect to wiretaps, for example, encryption is responsible for thwarting law enforcement in a relatively small percentage of cases. The Administrative Office of the U.S. Courts produces an annual report of Title III wiretapping.[35] For 2016, it shows that out of 3,168 wiretaps conducted, encryption was encountered in only 125 instances, and could not be decrypted in 101 cases—only roughly 3.2% of all wiretaps.[36] Certainly the meaningfulness of that statistic is limited by self-selection bias (most investigators probably do not ask for court orders to wiretap likely encrypted information), but it does at least show that many wiretaps are successful and not rendered ineffective by encryption specifically.

Regarding encrypted devices such as smartphones, several law enforcement offices have reported large numbers of devices seized that "remain inaccessible due to default device encryption."[37] But conspicuously missing from these reports are indications of how many such devices were the linchpin of investigations, as opposed to merely being devices that were seized routinely but were ultimately unnecessary in view of other evidence. Recently, the Manhattan district attorney identified a handful of anecdotes that described investigations possibly blocked due to encryption (none of which, curiously, were within his jurisdiction),[38] but reliance on anecdotal evidence seems to imply that the statistics are just not there.

Indeed, the case most often cited in favor of the need for a backdoor is the San Bernardino shooting and attempted bombing on December 2, 2015.[39] While the FBI strenuously argued for a court order to compel Apple to build a backdoor to unlock an iPhone that belonged to one of the shooters,[40] soon thereafter, it withdrew its request. Instead, it hired an outside firm to exploit a security vulnerability in the phone to gain access.[41] This is a case, then, where a backdoor ultimately proved to be unnecessary.[42]

It appears that efforts to collect evidence in support of the need for a backdoor today are in the works: A joint partnership between the FBI and local law enforcement, the National Domestic Communications Assistance Center (NDCAC), is now operating a Statistics Collection Tool to collect example cases "where evidence in a smart phone is unattainable due to encryption, but could have been critical in solving cases."[43] Nevertheless, the evidence so far is certainly insufficient.

Such a conspicuous lack of evidence contrasts sharply with another debate over encryption. In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which included a provision that required telecommunications providers to offer certain assistance to law enforcement in decrypting communications.[44] In the hearings that led to the passage of that law, the FBI was able to "presen[t] a variety of statistics and categories" including those "regarding the thwarting of investigations across federal law enforcement as well as state and local law enforcement,"[45] and the Government Accounting Office performed similar research.[46] This suggests that it is certainly possible for law enforcement to quantify their assertions of need, but in this case they have simply failed to do so.

Legal restrictions

There is good reason to believe that law enforcement has not produced such evidence because a backdoor is, in fact, not useful—at least to the extent that the law would allow it to be used. The Fourth Amendment prohibits the federal

35. 18 U.S.C. § 2519(3). https://www.law.cornell.edu/uscode/text/18/2519.

36. "Wiretap Report 2016," Administrative Office of the United States Courts, Dec. 31, 2016. http://www.uscourts.gov/statistics-reports/wiretap-report-2016.

37. "Smartphone Encryption and Public Safety," pp. 8–9. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and Rosenstein. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval. However, some have questioned the accuracy of these numbers. See, e.g., Marcy Wheeler, "Is FBI Still Fluffing Its Encryption Numbers?", *Emptywheel*, Nov. 11, 2016. https://www.emptywheel.net/2016/11/11/fbi-still-fluffing-encryption-numbers.

38. "Smartphone Encryption and Public Safety," pp. 10–11. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

39. Ibid., pp. 6–7.

40. "Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search," *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS3000*, No. 5:16-cm-10 (C.D. Cal. Feb. 16, 2016), p. 3. https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.pdf.

41. "Government's Ex Parte Application for a Continuance," *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS3000*, No. 5:16-cm-10 (Mar. 21, 2016). https://epic.org/amicus/crypto/apple/191-FBI-Motion-to-Vacate-Hearing.pdf.

42. Certainly, the vulnerability exploitation avenue was less efficient, but it is hard to imagine that efficiency concerns alone could justify an encryption backdoor.

43. "We Need Examples of Cases Hindered By 'Going Dark,'" *Prosecutors' Center for Excellence*, April 4, 2017. http://pceinc.org/need-examples-cases-hindered-going-dark; "Smartphone Encryption and Public Safety," pp. 10–11. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

44. 47 U.S.C. § 1002(b)(3). https://www.law.cornell.edu/uscode/text/47/1002.

45. Carrie Cordero, "Weighing in on the Encryption and 'Going Dark' Debate," *Lawfare*, Dec. 4, 2014. https://lawfareblog.com/weighing-encryption-and-going-dark-debate.

46. Ibid.

government and states from conducting "unreasonable searches and seizures,"[47] and courts have interpreted that provision to strongly protect a citizen's "reasonable expectation of privacy," especially in private communications and information in private possession.[48] Furthermore, the Fourth Amendment's requirement that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized"[49] prohibits "general warrants" that would authorize "searches in any place, for any thing,"[50] and thus likely limits the government's power to conduct mass surveillance in the first place.[51]

Even information not protected under the Fourth Amendment, such as a financial transaction voluntarily disclosed to a third party,[52] is not open to all government inspection because federal statutes impose further limits. When gathering foreign intelligence, for example, the Foreign Intelligence Surveillance Act (FISA) of 1978 may require the government "to minimize the acquisition and retention, and prohibit the dissemination" of domestic parties' communications or information in several situations.[53] The USA Freedom Act of 2015 imposes further limits on long-term government collection of "call detail records" and certain mass wiretapping.[54] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits the government from wiretapping any "wire or oral communication" without consent or prior judicial authorization, and requires the government to make a high showing of the need for wiretapping.[55] The Electronic Communications Privacy Act of 1986 later extended Title III and its limitations to wiretapping of electronic communications,[56] and further imposed limits on law enforcement access to emails or other data stored on a "remote computing service" (a cloud service, in today's nomenclature).[57]

Such an intricate tapestry of rules regarding government surveillance is important because it shows many circumstances where an encryption backdoor could not be used, even if one was present.

Efficacy and utility of already available technology

Within the confines of this legal framework, the government has access to a wealth of information through alternate investigative means—even without an encryption backdoor. Indeed, some commentators have called today the "golden age of surveillance."[58] And, in the numerous cases where these other avenues are sufficient for the needs of the justice and intelligence systems, a backdoor would be duplicative and thus unnecessary.[59]

Today, much information is unencrypted and available to law enforcement already. For example, metadata, or the "data about data" that often travels with encrypted information,[60] is largely unencrypted and can reveal location information,[61] unique identities of individuals,[62] telephone numbers dialed,[63] subject lines of emails,[64] identities of confederates

47. U.S. Constitution, Amendment IV; *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).

48. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *United States v. Jones*, 132 S. Ct. 945, 949 (2012).

49. U.S. Constitution, Amendment IV.

50. *Boyd v. United States*, 116 U.S. 616, 641 (1886) (Miller, J., concurring); *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

51. Richard A. Posner, "Privacy, Surveillance, and the Law," The *University of Chicago Law Review* 75:1 (2008), p. 254. https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/11; Robert Bloom and William J. Dunn, "The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment," *William and Mary Bill of Rights Journal* 15 (2006), pp. 191–92. http://lawdigitalcommons.bc.edu/lsfp/163.

52. *United States v. Miller*, 425 U.S. 435, 443 (1976). The Supreme Court is currently considering a case that may limit this so-called third-party doctrine. See *United States v. Carpenter*, 137 S. Ct. 2211 (2017) (mem).

53. Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, § 101(h), 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1885c). https://www.gpo.gov/fdsys/granule/STATUTE-92/STATUTE-92-Pg1783/content-detail.html. See also, Ibid., § 102(a)(1)(C); § 104(a)(5).

54. USA Freedom Act of 2015, Pub. L. No. 114-23, §§ 101(a)(3), 103 & 201, 129 Stat. 268. https://www.gpo.gov/fdsys/pkg/PLAW-114publ23/content-detail.html.

55. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, § 2511(1)(a), (c), 82 Stat. 197. https://www.gpo.gov/fdsys/granule/STATUTE-82/STATUTE-82-Pg197/content-detail.html. See also, Ibid., § 2518(3)(c); § 2516.

56. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, § 101(c), 100 Stat. 1848. https://www.gpo.gov/fdsys/granule/STATUTE-100/STATUTE-100-Pg1848/content-detail.html.

57.Ibid., § 201, § 2703.

58. Peter Swire, "The Golden Age of Surveillance," *Slate*, July 15, 2015. http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

59. See, e.g., "*Don't Panic: Making Progress on the 'Going Dark' Debate,*" pp. 9–10. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

60. See, e.g., Elizabeth W. King, "The Ethics of Mining for Metadata Outside of Formal Discovery," *Penn State Law Review* 113:3 (2009), pp. 805–07. http://www.pennstatelawreview.org/print-issues/articles/the-ethics-of-mining-for-metadata-outside-of-formal-discovery.

61. *See, e.g., United States v. Jones*, 132 S. Ct. 945, 949 (2012).

62. See, e.g., Peter Eckersley, "How Unique Is Your Web Browser?", *Proceedings of the International Conference on Privacy Enhancing Technologies* 10 (2010), p. 1. https://panopticlick.eff.org/static/browser-uniqueness.pdf.

63. *See, e.g., ACLU v. Clapper*, 785 F.3d 787, 793 (2d Cir. 2015).

64. See, e.g., Tim Worstall, "Why Email Can Never Be Truly Secure: It's the Metadata," *Forbes*, Aug. 18, 2013. https://www.forbes.com/sites/timworstall/2013/08/18/why-email-can-never-be-truly-secure-its-the-metadata.

or accomplices[65] and more.[66] "Side channel" information,[67] such as timing and rates of communications, are also observable by law enforcement and can uncover equally important information[68]—potentially enough even to decipher passwords.[69] All of this is so revealing about a person that it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[70]

Furthermore, the government already has several ways to overcome encryption through legal or technological processes.[71] For example, it can use existing security vulnerabilities to hack into devices or communication systems and retrieve information, as it apparently did with the locked iPhone identified after the San Bernardino shooting.[72] The government can almost certainly compel a suspect to unlock a device using biometrics such as a fingerprint scanner,[73] and according to some courts, may be able to compel him or her to enter a decryption password (although most courts would hold that to be a violation of the Fifth Amendment right against self-incrimination).[74]

Most importantly, the government often has access to third-party devices, services and systems that can help to obtain digital evidence. Cloud storage providers generally do not encrypt data in ways they cannot access,[75] so the government can use a variety of legal tools to gain entry.[76] Telecommunications providers, including broadband and voice-over-IP services, already must offer law enforcement assistance in decrypting communications in certain situations.[77] And Internet-of-Things devices, such as in-home cameras and wearable fitness trackers, are notably vulnerable to hacking and thus can be commandeered or otherwise accessed by government, which renders those devices a "potentially bountiful surveillance platform."[78]

Above all, the investigative strategies outlined raise important policy questions of their own as to how their use should be regulated.[79] However, law enforcement is likely not using these strategies to their fullest extent. Making better use of these already available "workarounds" would further reduce the number of cases where a backdoor would be necessary. Indeed, it is telling that multiple intelligence officials have called the need for encryption backdoors "overblown," arguing instead that skilled investigators "will develop technologies and techniques to meet their legitimate mission goals"—with or without backdoors.[80]

Moreover, the sophistication of criminals or terrorists sometimes requires the use of a workaround as opposed to a backdoor. This is because do-it-yourself encryption techniques are readily available on the Internet, and thus are essentially impervious to the latter. For example, the convicted

65. See, e.g., "The Golden Age of Surveillance." http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

66. See, e.g., Jane Mayer, "What's the Matter with Metadata?", *The New Yorker*, June 6, 2013. https://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata.

67. Formally called a "side-channel attack," such a method is a strategy for breaking encryption or otherwise reading a message not by obtaining the message content, but rather by observing external environment variables, such as the timing of message transmissions or electromagnetic radiation emissions from wires. See, e.g., François-Xavier Standaert et al., "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* 28 (2009), p. 446. https://link.springer.com/content/pdf/10.1007/978-3-642-01001-9_26.pdf.

68. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 38 (2001).

69. See, e.g., Dawn Xiaodong Song et al., "Timing Analysis of Keystrokes and Timing Attacks on SSH," *Proceedings of the Conference on USENIX Security Symposium* 10, Aug. 13-17, 2001. https://www.usenix.org/legacy/events/sec01/full_papers/song/song.pdf.

70. *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (citing *People v. Weaver*, 12 N.Y.3d 433, 441–42 [2009]); see also *United States v. Carpenter*, 137 S. Ct. 2211 (2017) (mem).

71. Orin S. Kerr and Bruce Schneier, "Encryption Workarounds," *Georgetown Law Journal* 106 (forthcoming 2018), pp. 5–29. https://dx.doi.org/10.2139/ssrn.2938033.

72. Joseph Cox, "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds," *Vice: Motherboard*, Feb. 24, 2016 https://motherboard.vice.com/en_us/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds.

73. *See, e.g., United States v. Dionisio*, 410 U.S. 1, 5–6 (1973).

74. See, e.g., *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Apple MacPro Computer*, 851 F.3d 238, 247–48 (3d Cir. 2017); and Orin Kerr, "The Fifth Amendment Limits on Forced Decryption and Applying the 'Foregone Conclusion' Doctrine," *The Washington Post*, June 7, 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine.

75. Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," *Journal on Telecommunications and High Technology Law* 8:2 (2010), pp. 392–96. http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF.

76. See, e.g., Fed. R. Crim. P. 17(c)(1); All Writs Act, 28 U.S.C. § 1651, applied in *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977). https://www.law.cornell.edu/uscode/text/28/1651. Obviously, the government must "fully satisfy the statute's threshold requirements" for a legal procedure such as the All Writs Act to apply. See *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016).

77. See Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, § 103(a)(1), 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010). https://www.gpo.gov/fdsys/granule/STATUTE-108/STATUTE-108-Pg4279/content-detail.html; *In re Communications Assistance for Law Enforcement Act & Broadband Access & Services.*, 20 F.C.C. Rcd. 14989, ¶¶ 25, 39 (Sept. 23, 2005). https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf.

78. Stephanie K. Pell, "You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?", *North Carolina Journal of Law and Technology* 17:4 (2016), p. 643. http://ncjolt.org/you-cant-always-get-what-you-want-how-will-law-enforcement-get-what-it-needs-in-a-post-calea-cybersecurity-centric-encryption-era.

79. See, e.g., Eliza Sweren-Becker, "This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone," *American Civil Liberties Union*, March 30, 2016. https://www.aclu.org/blog/privacy-technology/internet-privacy/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone; Soghoian, p. 423. http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF.

80. Mike McConnell et al., "Why the Fear Over Ubiquitous Data Encryption Is Overblown," *The Washington Post*, July 29, 2015. https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; Jose Pagliery, "Ex-NSA Boss Says FBI Director Is Wrong on Encryption," *CNNMoney*, Jan. 13, 2016. http://money.cnn.com/2016/01/13/technology/nsa-michael-hayden-encryption/index.html; Jenna McLaughlin, "NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI," *The Intercept*, Jan. 21, 2016. https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi.

terrorist, Rajib Karim, used a communication encryption scheme that involved first encrypting messages with custom Excel macros, saving the result in a password-protected Word document, compressing the document as an encrypted compressed file and then uploading the compressed, triply-encrypted file on an anonymous website.[81] Indeed, Karim's communications were decrypted only because investigators used a workaround to forensically retrieve the Excel spreadsheet from his computer hard disk.[82] Other, less-skilled wrongdoers likely leave evidentiary traces that are already accessible to law enforcement anyway and thus a backdoor would merely be duplicative.

All of the foregoing suggests that backdoors would be legally restrictive to law enforcement and unnecessary in the first place. Future changes to technology or better data on current law enforcement outcomes could justify a need for them in the future, but the many potential limits on their efficacy place the burden squarely on proponents to produce clear, quantifiable, objective evidence.

ASSOCIATED POLICY RECOMMENDATIONS

Collect quantitative evidence of need

Research should be done to quantify the need for a backdoor. Efforts such as NDCAC's Statistics Collection Tool are an important start, but that data collection could be more comprehensive and systematic. Congress could hold new hearings and consider legislative proposals for data collection, such as reporting requirements on law enforcement's collection of device data. These would be akin to the reporting requirements for wiretapping found in 18 U.S.C. § 2519, for example. Other national security experts argue that information on terrorist investigations should be declassified to provide the factual basis for any claimed need.[83]

Two caveats are appropriate with regard to this collection of statistics. First, to avoid the possibility that the government will engage in cherry-picking to serve its own interests, any data collection ought to be done objectively and subject to peer review. Second, data supporting the potential value of a backdoor will not in itself justify one; rather, that data would feed into the cost–benefit calculus of tradeoffs, which policymakers must evaluate.

As one former prosecutor wrote: "It will take more than a sampling of case anecdotes to make the case" for a backdoor.[84] Statistics on device investigative work would reveal the true extent to which encryption poses a real problem, and perhaps more importantly, they could reveal other soft spots where investigations could be improved with technological training or education. Better empirical evidence of the need is essential to advance the policy debate over encryption.

Increase resources and training for law enforcement

Law enforcement investigators often cannot take advantage of the wealth of information offered by the "golden age of surveillance," because they lack the resources to maximize its potential and in particular, to use that information quickly enough to match the pace of the digital world.[85] Increasing resources and training would help law enforcement do its job more effectively and provide sounder evidence of whether a backdoor is still necessary once law enforcement has exhausted all of its other options.

Government-sponsored hacking or exploitation of vulnerabilities, for example, ought to be brought within a systematic legislative framework, extending and formalizing the executive branch's current Vulnerabilities Equities Process for reviewing security vulnerabilities that the government may want to exploit.[86] Formalization would help streamline the process and make it available to state and local investigators,[87] and it would also allow critical stakeholders to weigh in on the process.[88]

Additionally, government investigators ought to receive training to gain a "deep technical understanding of modern telecommunications technology and also, because all phones are computers, deep expertise in computer science."[89] Important points will likely include retrieval and use of

81. Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel*, June 2016, p. 23. https://ctc.usma.edu/how-terrorists-use-encryption.

82. Ibid.

83. Jaffer and Rosenthal, p. 305. https://scholarship.law.edu/jlt/vol24/iss2/3.

84. Cordero. https://lawfareblog.com/weighing-encryption-and-going-dark-debate.

85. Marshall Erwin, "The FBI's Problem Isn't 'Going Dark.' Its Problem is Going Slowly," *Just Security*, July 16, 2015. https://www.justsecurity.org/24695/fbis-problem-going-dark-slow.

86. "Vulnerabilities Equities Policy and Process for the United States Government," The White House, Nov. 15, 2017, pp. 7–8. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; Lily Hay Newman, "Feds Explain Their Software Bug Stash—But Don't Erase Concerns," *Wired*, Nov. 15, 2017. https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns.

87. Michelle Richardson and Mike Godwin, "It's Time to Pass Legislation Governing a Key Part of the Government's Hacking Policy," *Just Security*, Oct. 5, 2017. https://www.justsecurity.org/45636/time-pass-legislation-governing-key-part-governments-hacking-policy.

88. The recent change to the criminal procedure rules, which expand the government's ability to conduct hacking under warrant garnered much criticism. Fed. R. Crim. P. 41(b)(6). See, e.g., Jadzia Butler, "U.S. Supreme Court Endorses Government Hacking," *Center for Democracy & Technology*, May 6, 2016. https://cdt.org/blog/u-s-supreme-court-endorses-government-hacking; and Jennifer Stisa Granick, "Challenging Government Hacking: What's at Stake," *American Civil Liberties Union*, Nov. 2, 2017. https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake.

89. Testimony of Susan Landau, Professor of Cybersecurity Policy, House Committee on the Judiciary, "The Encryption Tightrope: Balancing Americans' Security and Privacy," 114th Congress (GPO, 2016), p. 105 (spoken error omitted). https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf.

metadata, and also in-the-field knowledge of contemporary devices, such as the 48-hour window for biometric unlocking of some smartphones.[90] Partnerships between federal and local law enforcement, such as NDCAC, will be a key part of this learning.

QUESTION TWO: IS THERE A PASSABLE TECHNICAL SOLUTION?

Even a strong cost–benefit showing in favor of an encryption backdoor will mean little if an actual technical solution that adequately protects public security and individual liberty does not exist.

As noted above, the current encryption debate is often couched in absolutes, with proponents of backdoors claiming that a technical solution would be easy to invent, while opponents argue that a secure backdoor is a technical impossibility. Although neither side has the definitive answer as a matter of absolute correctness, a review of the evidence leans heavily toward a comprehensive technical solution being extremely hard to develop.

Law enforcement and others who advocate for a backdoor appear to believe that developing one would be simple, which is why several current legislative proposals simply mandate technology companies to create one without regard for the necessary technical mechanism.[91] Yet experience with past attempts at backdoors shows that such systems are hardly simple. Backdoors raise numerous concerns about increased cyberattack surface and attractiveness to hackers that have been well-covered by others;[92] two of these concerns are worth mention here.

First, encryption backdoors would limit progress in developing better encryption and in patching vulnerabilities as they are discovered. For example, perfect forward secrecy is a class of encryption technologies being rolled out today, which use frequently rotating encryption keys to ensure that theft of one key does not compromise future communications.[93] A backdoor system that requires messages to be encrypted with a single government-accessible key (sometimes called a "golden key" backdoor[94]) would render moot the development of that technology, thereby leaving individuals' communications more vulnerable to third-party interception. Indeed, perfect forward secrecy means that any backdoor applied to transitory communications will likely be inadequate from a technical perspective.

Second, bad actors may be able to modify and thus commandeer the backdoor system in ways that not only give them access to encrypted communications but also keep the government out. The Dual EC algorithm previously discussed was supposed to have contained a backdoor in the form of a numeric parameter called Q. That parameter had properties known only to the NSA that enabled it to guess encryption keys quickly.[95] The Q value thus acted as a sort of "golden key." However, in 2015 it was discovered that someone had used a software update to change the Q value in one program using the algorithm, which suggested that someone other than the NSA had gained the power to decrypt messages encrypted by that program.[96] In other words, encryption backdoors can be broken into not just by obtaining the government's keys, but by changing the backdoor's locks.

At the same time, some of the stronger views as to the impossibility of a technically secure backdoor may be overly simplistic. As one scholar points out, if a method of breaking a backdoor "takes 1000 years to develop, then it doesn't matter" that the backdoor is theoretically vulnerable to such a time-consuming method of breaking.[97] Furthermore, there may exist more limited-domain backdoors that overcome at least some of the technical challenges identified for all-purpose ones. For example, one criticism of "key escrow" backdoors, in which the government is given a copy of encryption keys, is that it would be difficult "to safely transport the key to the key escrow location" and "to securely store that key alongside millions—or potentially billions—of other keys."[98] However, others have proposed "device-specific" backdoors for smartphones, in which case the encryption key can be

90. Because the FBI apparently did not know of this window, it missed the opportunity to unlock the phone of a recent mass shooting attacker. See Nick Statt, "Apple Says It Immediately Contacted FBI About Unlocking Texas Shooter's iPhone," *The Verge*, Nov. 8, 2017. https://www.theverge.com/2017/11/8/16626452/apple-fbi-texas-shooter-iphone-unlock-encryption-debate.

91. See, e.g., Richard Burr and Dianne Feinstein, "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill," U.S. Senate, Apr. 13, 2016. https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation; "Smartphone Encryption and Public Safety," p. 32. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and Cyrus Farivar, "Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones," *Ars Technica*, Jan. 21, 2016. https://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones.

92. See Neumann et al., pp. 2–3. http://www.csl.sri.com/users/neumann/cacm237.pdf; and "*The Ground Truth About Encryption,*" pp. 11–12. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

93. Whitfield Diffie et al., "Authentication and Authenticated Key Exchanges," *Designs, Codes, and Cryptography* 2:2 (1992), p. 107. http://people.scs.carleton.ca/~paulv/papers/sts-final.pdf; Adam Langley, "Protecting Data for the Long Term with Forward Secrecy," *Google Online Security Blog*, Nov. 22, 2011. https://security.googleblog.com/2011/11/protecting-data-for-long-term-with.html.

94. "*The Ground Truth About Encryption,*" p. 5. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

95. Stephen Checkoway et al., "A Systematic Analysis of the Juniper Dual EC Incident," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, p. 468. https://eprint.iacr.org/2016/376.pdf.

96. Matthew Green, "On the Juniper Backdoor," *A Few Thoughts on Cryptographic Engineering*, Dec. 22, 2015. https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor.

97. Herb Lin, "Making Progress on the Encryption Debate," *Lawfare*, Feb. 4, 2015. https://www.lawfareblog.com/making-progress-encryption-debate.

98. "*The Ground Truth About Encryption,*" p. 6. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

escrowed on the physical phone itself, thus avoiding the transport and storage issues entirely.[99] This does not mean that a device-stored key escrow backdoor is a technically sound solution (among other things, the backdoor should not be usable by phone thieves), but it is to suggest that it may be too early to say that backdoors are a technical impossibility.

As with the initial cost-benefit question, in the end, arguments against the existence of a technical backdoor solution are likely correct, but they are not necessarily conclusive in view of new ideas for backdoors of more limited scope.

ASSOCIATED POLICY RECOMMENDATIONS

Conduct adversarial testing

To answer the question of whether a technical solution exists, our recommended approach is actual research and experimentation. In particular, we propose an "adversarial testing" process, in which one or more technical backdoor solutions are proposed and opened up to other researchers to show flaws, gaps or insecurities in those solutions.

Several experts have proposed experimentation and testing to prove one way or another whether there is a workable technical backdoor solution. One believes that the proponents of a backdoor should "propose a specific NOBUS mechanism" (using an acronym for "nobody but us" that refers to a backdoor) and put it up for technical scrutiny.[100] Another proposes a stress test. Or put more simply, the idea that a backdoor should be used only if "the methodology for that technology has been published publicly for more than 12 months and no efforts to subvert or defeat it have been successful."[101]

An excellent model for adversarial testing may be found in the development of the Advanced Encryption Standard, an encryption algorithm that is standardized and in use today. In the process of its creation, The National Institute of Standards and Technology sought proposals for encryption technologies from the technology community, opened up those proposals for peer review and finally selected a winning technology based upon the results.[102]

The alternatives to an open-testing process include development of the backdoor by a government commission,[103] or tasking industry to create one on its own initiative.[104] Neither is preferable. Both the creation of a backdoor and stress-testing to find flaws are processes that require creativity and ingenuity. It is unlikely that the best ideas will come either from a government-sponsored commission or from the business industry. Widespread input from academics, technologists and thinkers is the best way to ensure that all facets of the encryption backdoor question are addressed.

QUESTION THREE: IS THERE A WORKABLE POLICY IMPLEMENTATION?

Even if a technical solution to "going dark" is found to be adequately secure and protective of important interests, the task still remains for lawmakers to turn that technical solution into national and global policy. And, the subsequent problems to be addressed are numerous, difficult and likely intractable. For purposes of illustration, this section will discuss a hypothetical backdoor applied to smartphones, but the policy problems identified here could also apply to backdoors for different technologies such as cloud data storage or communications.

For starters, policymakers will have to assess the complex and costly tradeoffs required to place the backdoor in service in a way that would guarantee its almost-universal adoption. Consumer incentives to buy devices with backdoors likely will not work,[105] so the government may have to mandate inclusion of the backdoor on smartphones. But devices already in use would not be equipped with one, which means that widespread adoption could take years. A more rapid method would be for the government to pay for new phones for everyone (akin to the digital television transition) or to render the cell phone networks incompatible with older devices. Either way, the monetary costs would be enormous,[106] and there is a real question as to whether the value of the backdoor would outweigh such costs.

Policymakers would also have to lay out the rules for when and how the backdoor could be used, in ways akin to CALEA or ECPA. Numerous recent and historical events have shown that law enforcement is wont to use surveillance capabilities

99. Jamil N. Jaffer and Daniel J. Rosenthal, "Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge," *Catholic University Journal of Law and Technology* 24:2 (2016), p. 309. https://scholarship.law.edu/jlt/vol24/iss2/3; "Decrypting the Encryption Debate," pp. 50–51. https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers.

100. Lin. https://www.lawfareblog.com/making-progress-encryption-debate.

101. Paul Rosenzweig, "Testing Encryption Insecurity: A Modest Proposal," *Lawfare*, July 7, 2015. https://lawfareblog.com/testing-encryption-insecurity-modest-proposal.

102. James Nechvatal et al., "Report on the Development of the Advanced Encryption Standard (AES)," *Journal of Research of the National Institute of Standards and Technology* 106:3 (2001), p. 511. http://nvlpubs.nist.gov/nistpubs/jres/106/3/j63nec.pdf.

103. H.R. 4561, 114th Congress (2016); S. 2604, 114th Congress (2016); Jaffer and Rosenthal, pp. 305–06. https://scholarship.law.edu/jlt/vol24/iss2/3.

104. Burr and Feinstein. https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation.

105. One can imagine offering the backdoor as a consumer feature, for example, to recover data from the phone if it is damaged or the password is forgotten. But advertising a backdoor as a feature is unlikely to persuade, and frequent consumer use of backdoors would introduce significantly greater complexity to the development of technical and policy solutions.

106. See Eliot Van Buskirk, "How We Bungled the Digital Television Transition," *Wired*, Feb. 20, 2009. https://www.wired.com/2009/02/how-the-governm.

for personal or political gain.[107] Detailed procedural requirements, akin to the Woods Procedures that the FBI uses prior to conducting surveillance under FISA,[108] would be especially important to prevent abuses of a backdoor that could potentially reveal highly private and personal information. Transparency interests would also require consideration: Smartphone users will want to be sure that no one is secretly using the backdoor to snoop on them, but law enforcement will likely want to be able to conduct investigations in secret.

If keys or other components of the backdoor are maintained on third-party or government computer systems, then cybersecurity and data breach notification laws would be necessary. The government has proven on several occasions that it cannot maintain security of sensitive data from hackers.[109] Indeed, the Transportation Security Administration once accidentally allowed its backdoor keys for luggage locks to be published in a photo in the Washington Post.[110] Lawmakers have struggled with data breach and cybersecurity questions in the comparatively simpler field of personal data collection,[111] and they are likely to face greater difficulties with regard to a backdoor.

The government would almost certainly want a program for ongoing white-hat testing of the backdoor to discover unexpected flaws or vulnerabilities. Numerous recent events remind us that even systems designed to be as secure as possible can fall victim to software bugs or mistakes,[112] making continuous review necessary. But that poses a dilemma: Opening up the backdoor to researchers raises the possibility that a malicious actor could pose as a researcher to gain unauthorized access to confidential aspects of the backdoor. Developing satisfactory testing policy may thus prove to be an unusually hairy problem of security clearances and background checking.

Use of a backdoor as a tool for mass surveillance is a concerning problem that must be addressed. People often leave their smartphones unattended in a variety of circumstances, such as when crossing the national border[113] or when at school.[114] For this reason, it would be economically and socially detrimental if people were faced with the possibility that their phones could be decrypted on a regular basis. Technological solutions, such as making the backdoor time-consuming or difficult to use, can help but may not be sufficient.

Issues of federalism also come into play. Several states have attempted to introduce encryption backdoor legislation already.[115] These would likely be unduly burdensome on national- or global-scale companies, so federal preemption would be appropriate and warranted.[116] But state and local law enforcement will probably be the more frequent users of any encryption backdoor and thus federal legislation will need to develop rules for information-sharing between federal and state authorities. In the past, local law enforcement's failure to understand the legal ramifications of surveillance technology have already caused otherwise airtight cases to be thrown out, rendering the technology moot.[117]

Most importantly, there would have to be a contingency plan in case the backdoor is widely breached by a third party, a risk that can be minimized but almost certainly never eliminated. National security interests would be at stake, especially in the likely case that government and military personnel use the same devices as civilians. Likely the only secure solution is to replace all smartphones with the backdoor, a costly proposition for which the government must prepare.

Globalization presents even greater policy difficulties. If backdoor keys are stored externally on third-party servers, then every nation will vie to have copies and will likely impose pressures on device manufacturers or one another to

107. Andrea Peterson, "LOVEINT: When NSA Officers Use Their Spying Power on Love Interests," *The Washington Post*, Aug. 24, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests; Ellen Nakashima, "Justice Dept. Told Court of Source's Political Influence in Request to Wiretap Ex-Trump Campaign Aide, Officials Say," *The Washington Post*, Feb. 3, 2018. https://www.washingtonpost.com/world/national-security/justice-dept-told-court-of-sources-political-bias-in-request-to-wiretap-ex-trump-campaign-aide-officials-say/2018/02/02/caecfa86-0852-11e8-8777-2a059f168dd2_story.html.

108. See, e.g., Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Senate Committee on the Judiciary, "Oversight Hearing on Counterterrorism," 107th Congress (GPO, 2002), pp. 14–15 and 260-73. https://www.gpo.gov/fdsys/pkg/CHRG-107shrg86517/pdf/CHRG-107shrg86517.pdf.

109. Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," *Wired*, Oct. 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government; David Perera, "Researcher: Voter Registration Data of 191 Million Exposed Online," *Politico*, Dec. 28, 2015. https://www.politico.com/story/2015/12/voter-registration-data-exposed-217172.

110. Nicholas Weaver, "A Tale of Three Backdoors," *Lawfare*, Aug. 27, 2015. https://www.lawfareblog.com/tale-three-backdoors.

111. Rachel German, What Are the Chances for a Federal Breach Notification Law?", *Center for Identity, University of Texas at Austin*, April 14, 2015. https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law.

112. See, e.g., Thomas Fox-Brewster, "The Feds Can Now (Probably) Unlock Every iPhone Model in Existence," Forbes, Feb. 26, 2018. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite.

113. Morgan Chalfant, "Homeland Security Sued over Warrantless Phone, Laptop Searches at Border," *The Hill*, Sept. 13, 2017. http://thehill.com/policy/cybersecurity/350449-dhs-sued-over-warrantless-electronic-device-searches-at-border.

114. Amy E. Feldman, "When Does a Public School Have the Right to Search Its Students?", *National Constitution Center*, May 31, 2013. https://constitutioncenter.org/blog/when-does-a-public-school-have-the-right-to-search-its-students.

115. Farivar. https://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones.

116. H.R. 4528, Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016, 114th Congress (2016).

117. Robert Patrick, "Controversial Secret Phone Tracker Figured in Dropped St. Louis Case," *St. Louis Post-Dispatch*, April 19, 2015. http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html.

gain access.[118] And at the time law enforcement seeks to use a backdoor with the keys held in another country, mutual legal assistance treaties would come into play.[119] Requests under these treaties can be slow and complicated,[120] which could frustrate the value of any backdoor. Finally, the presence of one within the United States could have economic repercussions for global trade, as foreign businesses that want to avoid communicating with backdoor-vulnerable systems might stop manufacturing for the U.S. market or doing business with U.S. companies altogether.[121]

If any backdoor system is adopted, it must not only be secure as a technological matter. It must also be implemented with policy that solves the many problems discussed above, as well as others that will likely arise. This is a serious challenge that unfortunately does not appear to be addressed sufficiently in the current debate thus far. When it comes to putting a backdoor into practice, the policy difficulties will almost certainly exceed even the technical ones.

ASSOCIATED POLICY RECOMMENDATIONS

Conduct scenario planning

To address the question of what laws and policies must be in place to implement a technical backdoor, we recommend systematic thinking, and in particular, scenario planning as to ways that the backdoor could fail or otherwise be misused in practice. Scenario planning is a common practice that largely originates in the field of military strategy and came into common use after World War II.[122] Now extended to business settings as well, the practice involves statistical modeling or other analysis to develop reasonably detailed scenarios that can be planned for in advance.[123]

Done correctly and comprehensively, scenario planning could highlight the many potentially difficult situations that an encryption backdoor could face, including a government data breach, law enforcement misuse of the backdoor or malicious hacking efforts. Detailing these possible scenarios could help to put into focus the many policy tradeoffs that lawmakers would have to make in order to implement even a theoretically secure backdoor. This would move the debate beyond its current single hypothetical proposition.

CONCLUSION

As with many things, when it comes to encryption, reality is complicated. And when reality is complicated, there is a tendency to fall back on easy hypotheticals: the terrorist's cell phone with all the secrets encrypted or the government's golden decryption key too easily stolen by hackers. However, policymakers should avoid that trap, embrace the complexity of reality, and tackle *real* questions about how to deal with "going dark" in practice and what implementation of an encryption backdoor would look like in reality.

The time to answer these questions is now. The worst-case scenario for the encryption debate is a terrorist attack or other emergency threat that pushes Congress to enact an ill-conceived encryption backdoor mandate that is not justified either by actual law enforcement needs or by technological study. To avoid such a scenario requires laying the groundwork for research into the relative costs and benefits, workable technical solutions and policy implementation. Doing so requires a deliberate attempt to move past the current thought-experiment debates that have so far stymied pragmatic progress.

ABOUT THE AUTHORS

Charles Duan is a senior fellow and associate director of tech and innovation policy at the R Street Institute, where he focuses his research on intellectual property issues. Before joining R Street in January 2018, Charles was the director of the patent reform project at Public Knowledge, where he handled all aspects of patent policy ranging from outreach on the Hill to writing white papers and filing amicus briefs. Prior to this, he was a research associate to Professor Paul Ohm on an NSF-funded project that investigated the policy implications of newly proposed Internet architectures. He also worked as a patent attorney at Knobbe Martens.

Zach Graves is director of technology and innovation policy for the R Street Institute, where he manages development efforts for the tech program, oversees its scholars and coordinates work across a variety of issue areas. Zach joined R Street in April 2013, having previously worked at the Cato Institute and the America's Future Foundation. He is also a fellow at the Internet Law and Policy Foundry and a visiting fellow at the National Security Institute at George Mason University's Antonin Scalia Law School.

Arthur Rizer is director of justice and national security policy for the R Street Institute, where he heads institute programs dealing with a variety of issues related to intelligence, national security, crime and policing. In this capacity, he produces original research,

118. Already China has pressured Apple into making encryption keys more easily available to the government. See, e.g., Thuy Ong, "Apple Will Store Some iCloud Encryption Keys in China, Raising Security Concerns," *The Verge*, Feb. 26, 2018. https://www.theverge.com/2018/2/26/17052802/apple-icloud-encryption-keys-storage-china.

119. Arthur Rizer and Anne Hobson, "Cross-Border Data Requests: Evaluating Reforms to Improve Law Enforcement Access," *R Street Policy Study* No. 120, November 2017. http://www.rstreet.org/policy-study/cross-border-data-requests-evaluating-reforms-to-improve-law-enforcement-access.

120. Ibid., p. 4.

121.For comparison, national security concerns about malicious computer systems led Congress to ban use of Russian software on government computers and led AT&T to drop a plan to sell certain Chinese phone handsets. See Dustin Volz, "Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software," *Reuters*, Dec. 12, 2017. https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4; and Paul Mozur, "AT&T Drops Huawei's New Smartphone Amid Security Worries," *The New York Times*, Jan. 10, 2018. https://www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html.

122. Ron Bradfield et al., "The Origins and Evolution of Scenario Techniques in Long Range Business Planning," Futures 37:8 (2005), pp. 797–98. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.322.703&rep=rep1&type=pdf.

123. Paul J.H. Schoemaker, "Scenario Planning: A Tool for Strategic Thinking," Sloan Management Review 36:2 (1995), pp. 27–30. http://www.ftms.edu.my/images/Document/MOD001074%20-%20Strategic%20Management%20Analysis/WK4_SR_MOD001074_Schoemaker_1995.pdf.

writes for the popular press and educates policymakers on national security and criminal justice issues. Arthur joined R Street in August 2016, having previously served as associate professor of law at West Virginia University's College of Law and visiting professor of law at Georgetown University Law Center.

Mike Godwin is a distinguished senior fellow at the R Street Institute, where he focuses on the areas of patent and copyright reform, surveillance reform, technology policy, freedom of expression and global internet policy. Before joining the R Street Institute in 2015, he served as a senior policy advisor at Internews, advising the organization's public-policy partners in developing and transitional democracies, as part of the Global Internet Policy Project. Prior to his return to Washington, he served as general counsel for the California-based Wikimedia Foundation, which operates Wikipedia and other collaborative projects. At the foundation, he created and directed anti-censorship, privacy, trademark and copyright strategies, and policies including Wikimedia's responses to the SOPA and PIPA initiatives. Godwin received his undergraduate and law degrees at the University of Texas at Austin where, while a law student, he served as a reporter and later editor-in-chief of *The Daily Texan*. Upon graduation, Godwin began his legal career as the first staff counsel for the Electronic Frontier Foundation, which he advised on a range of legal issues centered on freedom of expression and privacy rights during the accelerated growth of Internet access in the United States. His continuing career as an Internet-law thought leader has included a policy fellowship at the Center for Democracy and Technology and a research fellowship at Yale Law School. He has been a contributing editor at *Reason* magazine since 1994 and is the originator of the widely cited "Godwin's Law of Nazi Analogies," which in 2012 was added to the *Oxford English Dictionary*.