Encryption Workarounds

ORIN S. KERR* & BRUCE SCHNEIER**

The widespread use of encryption has triggered a new step in many criminal investigations: The encryption workaround. We define an encryption workaround as any lawful government effort to reveal unencrypted plaintext of a target's data that has been concealed by encryption. This Article provides an overview of encryption workarounds. It begins with a taxonomy of the different ways investigators might try to bypass encryption schemes. We classify six kinds of workarounds: find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy. For each approach, we consider the practical, technological, and legal hurdles raised by its use.

The remainder of this Article develops lessons about encryption workarounds and the broader public debate about encryption in criminal investigations. First, encryption workarounds are inherently probabilistic. None work every time, and none can be categorically ruled out every time. Second, the different resources required for different workarounds will have significant distributional effects on law enforcement. Some techniques are inexpensive and can be used often by many law enforcement agencies; some are sophisticated or expensive and likely to be used rarely and only by a few. Third, the scope of legal authority to compel third-party assistance will be a continuing challenge. And fourth, the law governing encryption workarounds remains uncertain and underdeveloped. Whether encryption will be a game changer or a speed bump depends on both technological change and the resolution of important legal questions that currently remain unanswered.

TABLE OF CONTENTS

* Frances R. and John J. Duggan Distinguished Professor, University of Southern California Gould School of Law.

** Fellow, Berkman Klein Center for Internet & Society at Harvard University; Chief Technology Officer, IBM Resilient. The authors thank Dan Richman, Catherine Crump, Andrea Roth, Holly Doremus, Mark Rumold, Steven Bellovin, the University of California at Berkeley Law School Public Law and Policy Colloquium, and the Privacy Law Scholars Conference for comments on an earlier draft.

INTRODUCTION

In the last decade, encryption technologies have come into widespread use. Most Americans now use smartphones that encrypt when not in use and require the user's passcode to unlock it.[1] Free messaging services, such as WhatsApp, now encrypt communications from end to end.[2] Millions of websites now routinely encrypt traffic in transit.[3] This increased use of encryption has been largely imperceptible to users, but it amounts to a profound shift in the accessibility of computer-stored information.

Encryption raises a challenge for criminal investigators. When a criminal suspect has used encryption, the suspect's data is protected from access by third parties. Lawful government access to the data typically reveals only scrambled

1. According to a 2015 study, 68% of adults in the United States own a smartphone. Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CTR.: INTERNET & TECH. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/ [https://perma.cc/R774-6MXD]. That percentage is up from 35% in 2011, *id.*, suggesting that the percentage today may be substantially higher than 68%.

2. *See End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/general/28030015 [https://perma.cc/MR8X-USCM].

3. *See* Sang Ah Kim, Note, *HTTPS: Staying Protected on the Internet*, 1 GEO. L. TECH. REV. 119, 120–23 (2016).

information known as ciphertext, which is useless unless it can be decrypted into the original readable form known as plaintext.[4] For government investigators, encryption adds an extra step: They must figure out a way to access the plaintext form of a suspect's encrypted data.[5]

In this Article, we refer to such efforts as "encryption workarounds." We use the term broadly to refer to any effort to reveal a plaintext version of a target's data that has been concealed by encryption. Encryption workarounds are not conceptually new as a lawful government investigative technique. In 1807, during the treason trial of Aaron Burr, the prosecution attempted to decipher Burr's encrypted messages by forcing his private secretary to testify about their plaintext meaning.[6] Even further back, in 1587, Mary Queen of Scots was convicted of treason and then beheaded when her role in an assassination plot against Queen Elizabeth was revealed by the decryption of private letters among the conspirators.[7]

Despite their historical antecedents, encryption workarounds have recently assumed widespread importance. In the past, encryption was typically cumbersome and its use was rare. That has changed. Today it is both easy and ubiquitous. As encryption has been embraced by most users, and therefore most criminal suspects, investigators have come to encounter it in routine cases. That change has forced law enforcement to focus its attention on how to bypass the encryption methods used by criminal suspects. Although empirical evidence is spotty, recent government disclosures suggest that law enforcement currently finds successful workarounds for encrypted devices about half the time.[8]

This Article provides an overview of encryption workarounds. It presents a taxonomy of the different ways investigators might try to work around encryption schemes. We classify six kinds of workarounds: find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy. The first three are strategies to obtain an existing key to unlock encrypted data. The latter three are ways of accessing the data in plaintext form without obtaining the key.

For each approach, we consider the practical, technological, and legal hurdles that they implicate. None of the methods are unique to law enforcement. Anyone,

4. *See* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 91–92 (2004).

5. We use the term "data" to refer broadly to a suspect's information and communications, whether at rest or in transit.

6. *See* United States v. Burr, 25 F. Cas. 38, 39–40 (C.C.D. Va. 1807) (No. 14,692E).

7. *See* DAVID KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING 119–24 (1996).

8. According to former FBI Director James Comey, the FBI received 2,800 devices in the last three months of 2016; the FBI was unable to access 1,200 of them. *See* Tom Winter, Tracy Connor & Pete Williams, *Comey: FBI Couldn't Access Hundreds of Devices Because of Encryption*, NBC NEWS (Mar. 8, 2017, 6:17 PM), www.nbcnews.com/news/us-news/comey-fbi-couldn-t-access-hundreds-devices-because-encryption-n730646 [https://perma.cc/JS33-WD9B]. Assuming that all of those devices were initially encrypted, which is suggested but not obvious from Comey's remarks, that implies an FBI workaround success rate of about 57%.

criminals and law enforcement alike, can employ these methods to access encrypted data. But in this Article, we consider how each workaround might arise in the course of a lawful domestic criminal investigation. We take no view on which workaround is best, or what law should govern any particular one. Instead, we hope to explain the range of options investigators have, and the promise and challenges of each.

The remainder of the Article suggests implications for the public debate about the role of encryption in government investigations. Understanding the taxonomy of encryption workarounds puts them into context, revealing the tradeoffs among them and the new investigatory dynamic they create. Four lessons emerge. First, encryption workarounds are inherently probabilistic. None work every time, and none can be categorically ruled out. Second, the different resources required for different workarounds will have significant distributional effects on law enforcement. Some agencies will focus their efforts on a narrow set of workarounds and others will have broader options. Third, the scope of legal authority to compel third-party assistance will be a continuing challenge. And fourth, the law regarding encryption workarounds remains uncertain and underdeveloped.

These observations, in turn, suggest two broad conclusions about the new criminal investigative environment caused by widespread use of encryption. First, it is too early to tell how much the widespread use of encryption will impact the government's ability to solve criminal cases. Former FBI Director James Comey has expressed fears that criminal investigations are "going dark" because encryption blocks government access to communications.[9] Critics respond that the government has access to more data than ever, in part because there are investigative techniques the government can use that don't involve breaking encryption.[10] Which side is right depends in part on the success of workarounds. The law and technological feasibility of many workarounds is presently unsettled, and little empirical evidence about their use is known.

The second conclusion is a corollary of the first: The existence of workarounds may mean that encryption does not cause a dramatic shift in the government's investigative powers. When targets use encryption, the government does not give up. The government turns to encryption workarounds that attempt to erase the barrier that encryption tries to erect. The success rates of different workarounds remain unclear. However, the effect of encryption may prove less dramatic than the government fears or civil liberties activists hope.

---

9. *See* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks at the Brookings Institute: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/45X9-AG2M].

10. *See, e.g.*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/JYG2-8D3V].

This Article contains three parts. Part I introduces the technology of encryption. Part II surveys the six kinds of encryption workarounds. Part III suggests lessons for policymakers.

I. THE BASIC PRINCIPLES OF ENCRYPTION

Cryptography—the science of encryption—is as old as writing itself. Its basic principles date back thousands of years.[11] At its core is an encryption algorithm, which is a series of operations performed on information that encodes the information to make it unreadable. The operations might be simple. For example, the algorithm might merely change each letter in the alphabet one letter so that A becomes B, B becomes C, C becomes D, and so on. The plaintext phrase "law review" would become the ciphertext "mbx sfwjfx." Performing the same operation in reverse would restore the ciphertext back to plaintext.

Modern encryption algorithms use the same principle but rely on complex mathematics. They follow Kerckhoffs's Principle, first stated by the Dutch cryptographer Auguste Kerckhoffs in the 1800s: An encryption algorithm should be secure if everything is known about it except the key.[12] Under this principle, modern cryptographers assume that the inner workings of their encryption algorithms are known.[13] These algorithms are widely known and common across systems. For example, every Windows computer with the disk-encryption software Microsoft BitLocker uses the same algorithm.[14] Because every user of BitLocker has her own key, no one can unlock and decrypt a computer belonging to someone else.[15] The only thing that is secret is the key.

The key to an encryption algorithm is the special code that pairs with the known algorithm to encrypt or decrypt data. Any data can be encrypted, including text, images, video, or programs. In the context of modern computer encryption methods, a key is a long string of information known as "bits," consisting of zeros and ones. Modern computer encryption keys are typically 128 or 256 bits long.[16] For example, a 128-bit key might be 01000110011110001101111110001110101000100101011100100101011 10000111101101000111001111110001011101001011101100100001101011010001100.[17] A 256-bit key would be similar, but twice as long.

---

11. *See* KAHN, *supra* note 7, at 71–106.

12. *See* Auguste Kerckhoffs, *La Cryptographie Militaire*, 9 J. SCI. MILITAIRES 5, 10–13 (1883) (Fr.), http://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf [https://perma.cc/MK34-64E9].

13. *See* NIELS FERGUSON, BRUCE SCHNEIER & TADAYOSHI KOHNO, CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 24–25 (2010).

14. *See BitLocker Overview*, MICROSOFT: DOCS (Aug. 31, 2016), https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831713(v=ws.11) [https://perma.cc/ZRS8-Z39X].

15. *See id*.

16. *See* FERGUSON, SCHNEIER & KOHNO, *supra* note 13, at 43.

17. The keys are often expressed in hexadecimal notation, a numerical system in which every eight bits make up a single two-character "byte." The key above would be expressed as 4678df8ea25c95c3da39f8ba5d90d68c.

Encryption algorithms are designed such that there should be no faster way to break them than to try every possible key. This is known as a brute-force attack.[18] To thwart an attempted brute-force attack, the key must be long enough to make such an attack impossible. Fortunately, this is easy. Adding a single bit to the encryption key only slightly increases the amount of work necessary to encrypt, but doubles the amount of work necessary to brute-force attack the algorithm.[19] A 128-bit key has 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible keys. A 256-bit key has 2^{256} possible keys, a number with twice the number of digits as the previous number. These are unimaginably large numbers. In the arms race between encryption and brute force attacks, the mathematics overwhelmingly favors encryption.

Today, 64-bit keys can be brute-forced with a reasonable amount of computing power, and many believe that 80-bit keys can be brute-forced by large national-intelligence agencies.[20] However, 128-bit keys are beyond the reach of any current or near-future technologies.[21] Key lengths of 128 bits and 256 bits are the ones most commonly used today.[22] As a result, brute-force attacks on a typical-length key are effectively impossible.

Although some encryption applications accept random, full-length keys, most do not. Instead, they generate random keys in one of two ways. First, in some encryption applications, the keys are generated and exchanged among computers without a need for users to input them. If you use an encrypted messaging system, such as WhatsApp, the software on your computer—and that on the computers of people you communicate with—will encrypt and decrypt the messages using keys generated by the software.[23] The process of encryption and decryption is essentially invisible to the user.

Second, most modern systems that use encryption rely on the additional step of using passwords, passcodes, or passphrases (which we refer to collectively as passwords).[24] Although it is generally infeasible to memorize a 256-bit key, it is relatively easy to memorize a shorter string of numbers, letters, or words. Modern computer encryption systems generally submit to that reality by allowing access based on a shorter password instead of the full key. The key itself is encrypted, and the encryption for the key is unlocked with the password.[25] Behind the scenes, the process of decryption is broken into two parts: one algorithm pairs

18. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, SECOND EDITION: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 151 (2d ed. 2015).

19. The doubling occurs because the computer must check twice as many combinations: All of the combinations with the added "0" at the end plus all of the combinations with the added "1" at the end.

20. *See* SCHNEIER, *supra* note 18, at 151–54.

21. *See* Mohit Arora, *How Secure Is AES Against Brute Force Attacks?*, EE TIMES (May 5, 2012, 5:29 PM), https://www.eetimes.com/document.asp?doc_id=1279619.

22. *See* FERGUSON, SCHNEIER, & KOHNO, *supra* note 13, at 43.

23. *See End-to-End Encryption*, *supra* note 2.

24. Technically, there are differences. Passcodes ordinarily only contain numbers, passwords ordinarily contain letters, and passphrases are often passwords with added spaces and may amount to sentences or sentence-fragments.

25. *See* SCHNEIER, *supra* note 18, at 176.

with the password to decrypt the key, and a second algorithm is paired with the plaintext key to decrypt the data.

For users, this means that the passcodes and passwords they use to encrypt or decrypt their files are technically not encryption keys even though they function as encryption keys. Consider a four-digit code that may be needed to unlock a smartphone. The code is not the key. Instead, entering the passcode decrypts the key, enabling the key to be processed and unlocking the phone. This two-stage process is invisible to the casual user.[26] To most users, passcodes and passwords serve the function of keys.

Although modern means of encryption may sound impregnable in theory, in practice that is not the case. Today, and for the foreseeable future, every encryption system will have weaknesses. The algorithm must be written in software and run on a computer. The key must somehow be entered into the system. If it is to be used at different points in time, it must be stored in computer or human memory or written down somewhere. The algorithm may have flaws. Users can choose easy-to-guess keys, and the use of passwords or passcodes can dramatically shorten the number of possible keys that must be tested.[27] Weaknesses in encryption systems are common, and they play a big role in the encryption workarounds described below.

Encryption and encryption workarounds are "dual use" technologies.[28] They have both positive and negative uses. Anyone who wants to keep private information away from third parties can use encryption, and any third party who wants to expose a person's encrypted information can try an encryption workaround. This is an essential point because it shows that the context of lawful criminal investigations is only one part of a broader picture. In this Article, we assume that a criminal has used encryption to conceal evidence and that the police are conducting a good-faith investigation to defeat it. But the reverse dynamic also occurs. The government often uses encryption to maintain the privacy of valuable government data,[29] and criminals or terrorists often use workarounds to defeat it.[30]

---

26. For an overview of how encryption programs operate in Apple products, see iOS SECURITY: iOS 9.3 OR LATER, APPLE 10–17 (2016), https://images.apple.com/ca/business/docs/iOS_Security_Guide.pdf [https://perma.cc/8D2W-SXLE].

27. Users choose and remember short, nonrandom passwords. In cryptography, the strength of a password or key is known as "entropy." *See generally* WHITEWOOD ENCRYPTION SYS. INC., UNDERSTANDING AND MANAGING ENTROPY 1 (2015), https://www.blackhat.com/docs/us-15/materials/us-15-Potter-Understanding-And-Managing-Entropy-Usage-wp.pdf [https://perma.cc/M4XQ-VESU] (discussing the concept of entropy in encryption, defined roughly as the degree to which information is "truly random data"). The more random a string of characters becomes, the higher its entropy and the harder it is to predict. *Id.* at 2. Thus, a random binary string has the maximum possible entropy for its length. Anything shorter or less random—a dictionary word, for example—has less entropy. In general, passwords have much less entropy than the underlying keys they protect. *Id.* at 1.

28. We use the phrase "dual use" to mean that encryption and encryption workarounds can be used by any actor to pursue any purpose.

29. *See* Ryan Hagemann, *Which Government Agencies Encrypt Data? The Answer May Surprise You*, THE HILL (Aug. 28, 2015, 9:00 AM), thehill.com/blogs/congress-blog/homeland-security/251500-which-government-agencies-encrypt-data-the-answer-may [https://perma.cc/Z7QN-6CVX].

30. *See, e.g.*, Brett Williams, *Android Pattern Lock Might Be Vulnerable to (Very Determined) Thieves*, MASHABLE (Jan. 23, 2017), https://mashable.com/2017/01/23/android-pattern-lock-hack-report/#hTiR97Etzmqr [https://perma.cc/NRM4-X6XY].

From this perspective, it is wrong to think of using encryption as inherently bad or to think of efforts to bypass encryption as inherently good—or vice versa. The techniques we describe are general. There is nothing about encryption workarounds, aside from the framework of legal compulsion, that make them unique to law enforcement, the United States government, or governments in general. Anyone can use encryption, and anyone with sufficient technical expertise and financial resources can use encryption workarounds.

II. SIX TYPES OF ENCRYPTION WORKAROUNDS

This Part identifies six categories of encryption workarounds. We label them as follows: find the key, guess the key, compel the key, exploit a flaw in the encryption scheme, access plaintext when the device is in use, and locate a plaintext copy. The first three methods are key-based. They work by obtaining and using the key to decrypt data. The key-based methods differ based on whether the key is found somewhere (find the key), guessed (guess the key), or obtained from a person (compel the key).

The latter three methods work without the key. They differ primarily based on how the government bypasses the encryption to obtain the plaintext. The government can break in without the key as a result of an accidental weakness (exploit a flaw), break in without a key when data must be available to the user (access plaintext when the device is in use), or obtain a different copy without breaking in at all (locate a plaintext copy).

A. FIND THE KEY

The first way for the government to decrypt the data is to find an existing copy of the key. For purposes of this section, we can treat all passwords, passcodes, and passphrases as keys. The target might have written down the key somewhere. Perhaps it was entered into a file of passwords stored on the target's computer or phone. Perhaps it was written down on a scrap of paper hidden in a diary. If investigators can locate a copy of the key, they can enter it to decrypt the ciphertext into plaintext.

Whether this approach will work depends on three hurdles. First, the key must be available somewhere. A suspect might have written down a key on a Post-it note left next to the computer. Modern browsers also have the option of storing passwords and keys, and a user might use that option to store a copy there.[31] Alternatively, the encryption program may have a flaw that accidentally leaves a copy of the key in memory or on the computer's hard drive after use.[32]

Second, the government must find the key and be able to read it. Keys can be hidden. A key might be written down on a particular page in a particular notebook

31. *See, e.g.*, *Google Chrome Help: Manage Saved Passwords*, GOOGLE, https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=en [https://perma.cc/W36R-R9H3] (discussing how to save passwords in the popular Google Chrome browser).

32. This step would combine "find the key" with a second workaround, "exploit a flaw in the encryption scheme," discussed *infra* Section II.D.

in the suspect's library, requiring officers to find it. Keys might be stored in a computer somewhere, which would require investigators to perform forensic analysis on that computer to locate them. Keys can themselves be encrypted in another application, such that a second key is needed to decrypt the desired key. For example, the target could record his keys in a single text file and encrypt that file. Alternatively, readily available computer programs known as "password managers" can encrypt the hundreds of passwords and keys of the average person with a single master key.[33] The master key can be used to decrypt the files encrypted by individual passwords.

The third hurdle to finding the key is that the government must have the lawful authority to access it. Depending on the circumstances, this may require a search warrant or even greater legal authority. For example, in a 2001 case, *United States v. Scarfo*, the government suspected that the defendant had encrypted an important file stored on his home computer.[34] Agents obtained a warrant, secretly entered his home, and installed a key logger—an eavesdropping device that records every keystroke typed on the keyboard—on his computer.[35] When the suspect used his computer and entered his password to decrypt the file, the key logger intercepted the password. Agents later retrieved the key logger and used the password to decrypt the file.[36] The court then had to determine whether installing and using the key logger was permitted by a traditional search warrant or whether it required a wiretap order under the Federal Wiretap Act.[37] The court held that the traditional search warrant was sufficient because of the technical details of how the key logger was installed.[38] For our purposes, the particular holding of *Scarfo* is less important than the broader lesson: The strategy of finding the key often requires the legal authority to search for and seize it.

B. GUESS THE KEY

A second encryption workaround is to guess the key. Although random encryption keys are sufficiently long that guessing is effectively impossible, passwords, passcodes, and passphrases that often protect the keys are much shorter. A passcode or password that is relatively easy for the user to memorize can also be relatively easy for an outsider to guess. Because the password unlocks the encryption

33. *See generally* Neil J. Rubenking, *The Best Password Managers of 2018*, PC MAG. (Dec. 7, 2017, 10:00 AM), http://www.pcmag.com/article2/0,2817,2407168,00.asp [https://perma.cc/6F35-6WUQ] (discussing how password managers save login credentials for multiple websites and enable users to log in to each site automatically).

34. 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

35. *Id.* A key logger can be either hardware or software. Some key loggers store keystrokes in memory and must be manually retrieved. Others automatically transmit typed keystrokes to a remote device.

36. *Id.* The password was "NDS09813-050," which happened to be the prison ID number of Scarfo's father. *See* John Schwartz, *Compressed Data; Password Protection with Prison Stripes*, N.Y. TIMES (Aug. 6, 2001), http://www.nytimes.com/2001/08/06/business/compressed-data-password-protection-with-prison-stripes.html [https://nyti.ms/2hKu59Z].

37. *See Scarfo*, 180 F. Supp. 2d at 575.

38. *See id.* at 581–83.

key which, in turn, decrypts the encrypted volume—a hard drive, for example—guessing the password has the same effect as guessing the encryption key.

Whether the government can correctly guess the password or key depends on many variables. The most important is the number of possible keys. Some systems have limitations on what sorts of passwords can be used. A system might use only a four-digit PIN or a password with up to eight alphanumeric characters.[39] Whereas the most secure systems allow a password to be an arbitrary length, including any typeable characters, many systems have restrictions that limit the set of possible passwords.[40]

Other factors that affect the likelihood of successful guessing include: whether investigators have reason to suspect the owner used a particular key, whether technical means exist to make many guesses quickly, and whether weaknesses exist in the encryption algorithm that limit the number of guesses. In the simplest case, agents may guess the key successfully by making educated guesses about what passwords the owner is likely to have used. Users often use memorable numbers or phrases to help them remember their passwords.

Consider the recent case of *United States v. Lopez*.[41] Michelle Lopez was arrested at the United States border after agents discovered cocaine in her car.[42] Agents also seized her locked iPhone and iPad. During questioning, the agents asked Lopez her date of birth. After she shared that information with the agents, the agents successfully unlocked the iPhone and iPad by correctly guessing that Lopez used her birthdate as the code to unlock both devices. The record in *Lopez* does not explain why the agents guessed her birthdate as the code, or whether the phone was configured to accept a four-digit code, six-digit code, or something else. The entry may have simply been a good first guess: Everyone has memorized their birthdates, after all, and agents may try that intuitive sequence as a likely passcode.

In some cases, agents might be able to guess widely used passwords without knowing anything specific about the owner. A 2011 study of four-digit numerical passcodes selected by smartphone users found that fifteen percent of the passcodes consisted of only ten combinations out of the 10,000 possibilities.[43] The most popular passcode was "1234," which was used about four percent of the time.[44] On computers, the most common passwords are "123456," "password,"

39. *See* Brent Jensen, *5 Myths of Password Security*, STORMPATH BLOG (May 3, 2013), https://stormpath.com/blog/5-myths-password-security [https://perma.cc/7J4Y-BJ5K].

40. *See, e.g.*, *A Few Reason* [sic] *for Maximum Password Length*, MALWARETECH (May 27, 2014), https://www.malwaretech.com/2014/05/the-reason-for-maximum-password-lengths.html [https://perma.cc/YZY8-4CDF].

41. No. 13CR2092 WQH, 2016 WL 7370030 (S.D. Cal. Dec. 20, 2016).

42. *Id.* at *1.

43. *See* Daniel Amitay, *Most Common iPhone Passcodes*, DANIEL AMITAY BLOG (June 14, 2011, 5:30 PM), http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes [https://perma.cc/4MDH-RMJT].

44. *See id.*

"12345678," and "qwerty."[45] Although there are techniques for creating passwords that are both secure and easily remembered, relatively few people use them.[46]

The general technique of guessing human-memorizable passwords and keys in some sort of commonness order is known as password-guessing and is a common tactic of both law enforcement and criminals.[47] Modern computers can try millions of passwords per second.[48] They can easily try sets of possible passwords, such as: all dictionary words, all dictionary words with "@" substituted for "O," all pairs of dictionary words with a single digit between them, all strings of eight characters or less that are entirely lowercase letters, and so on.[49]

The ease of password guessing depends on whether potential passwords can be tried offline using dedicated computer systems. Consider the case of an encrypted file. The guesser can copy the encrypted file from the suspect's computer and bring it to a forensic laboratory. This allows the guesser to use incredibly powerful networked computers that are optimized to guess passwords as quickly as processing speeds permit.[50]

If the keys must be guessed on the seized hardware device itself, however, the time required can be considerably greater. Consider Apple's iPhone. Trying every possible four-digit PIN—up to 10,000 combinations—is almost

45. *See Worst Passwords of 2015*, TEAMSID, https://www.teamsid.com/wp-content/uploads/2016/01/TeamsID-IG-Worst-Password-V3.pdf [https://perma.cc/MMB4-CREY].

46. *See* Bruce Schneier, *Passwords Are Not Broken, But How We Choose Them Sure Is*, GUARDIAN (Nov. 12, 2008, 7:01 PM), https://www.theguardian.com/technology/2008/nov/13/internet-passwords [https://perma.cc/5XBS-C95Y].

47. *See id.*

48. *See* Hackers Writer, *Bruteforce Password Cracking Software Tries 8 Million Times Per Second*, HACKERSNEWSBULLETIN (Sept. 4, 2013), http://www.hackersnewsbulletin.com/2013/09/new-password-cracking-software-tries-8-million-times-per-second-crack-password.html [https://perma.cc/B69S-PS8K].

49. *See* Dan Goodin, *Anatomy of a Hack: How Crackers Ransack Passwords Like "qeadzcwrsfxv1331,"* ARS TECHNICA (May 27, 2013, 9:00 PM), https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/3 [https://perma.cc/FMB6-K38K]. A 2013 article tested three password-cracking experts against a list of 16,000 encrypted passcodes. *See id.* The winners successfully guessed 90% of them. *Id.* Passcodes guessed included:

> "k1araj0hns0n," "Sh1a-labe0uf," "Apr!l221973," "Qbesancon321," "DG091101%," "@Yourmom69," "ilovetofunot," "windermere2313," "tmdmmj17," and "BandGeek2014." Also included in the list: "all of the lights" (yes, spaces are allowed on many sites), "i hate hackers," "allineedislove," "ilovemySister31," "iloveyousomuch," "Philippians4:13," "Philippians4:6-7," and "qeadzcwrsfxv1331." "gonefishing1125" was another password Steube saw appear on his computer screen.

Id. This gives some flavor of the effectiveness of password guessing. Some criminal organizations have much more powerful capabilities to guess passwords than, for example, lone hackers and their single computers. The world's national intelligence agencies have even more extensive capabilities. Companies like AccessData sell password-guessing hardware and software to law enforcement that is more powerful than this example indicates. *See, e.g.*, *Uncover the Story Lurking in Your Digital Data*, ACCESSDATA, http://marketing.accessdata.com/uncoverthestory [https://perma.cc/F3G8-Y75Y].

50. *See* Bruce Schneier, *Secure Passwords Keep You Safer*, SCHNEIER ON SECURITY (Jan. 15, 2007), https://www.schneier.com/essays/archives/2007/01/secure_passwords_kee.html [https://perma.cc/8UL3-9FZ7].

instantaneous on an offline computer.[51] But the iPhone's processor is comparatively slow. It would take an iPhone twenty-two hours to run through the one million possible keys under its default six-digit configuration.[52] If a user expands a passcode to thirteen digits, it would take only minutes to guess offline but about 25,000 years to run through every possibility on the iPhone itself.[53]

Technical means can be used to slow down or thwart guessing. The current iPhone operating system combines these features with the "erase data" feature.[54] The feature is not enabled by default. If users turn it on, however, it disables the phone for one minute after five wrong passcode entries. The delay period grows for the next four successive wrong entries, from five minutes for the sixth wrong entry, to fifteen minutes each for the seventh and eighth wrong entries, to an hour for the ninth wrong entry. After the tenth wrong entry, the phone's data is permanently erased and cannot be accessed.[55] This obviously limits the opportunity investigators have to access the phone's contents by guessing.

C. COMPEL THE KEY

A third approach is for the government to compel the key from someone who has it or knows it. In most cases, the relevant key will be a password or passcode. In a broad sense, compelling a key could refer to any use of coercion. In an authoritarian regime, or among criminals, the idea of coercion may include threats, bribery, seduction, and torture. The general phrase cryptographers use for this attack is "rubber-hose cryptanalysis," which emphasizes the physical nature of this coercion.[56] In this Article, we restrict ourselves to legal compulsion techniques.

Of course, if investigators ask for the key and such a person provides it voluntarily, officers may use that key so long as the Fourth Amendment is otherwise satisfied.[57] The more complex case occurs when the person refuses to disclose the

---

51. *See* Micah Lee, *Upgrade Your iPhone Passcode to Defeat the FBI's Backdoor Strategy*, INTERCEPT (Feb. 18, 2016, 4:05 PM), https://theintercept.com/2016/02/18/passcodes-that-can-defeat-fbi-ios-backdoor [https://perma.cc/QDQ5-4D4D].

52. *See id.*

53. *See id.*

54. *See* Zaib Ali, *Enable Erase Data Option to Delete Data After 10 Failed Passcode Attempts*, iOSHACKER (Mar. 28, 2017), http://ioshacker.com/how-to/enable-erase-data-option-delete-data-10-failed-passcode-attempts [https://perma.cc/D477-KFJ4].

55. *See* Jack Date, *The FBI and the iPhone: How Apple's Security Features Have Locked Investigators Out*, ABC NEWS (Feb. 17, 2016, 8:20 AM), http://abcnews.go.com/US/fbi-iphone-apples-security-features-locked-investigators/story?id=36995221 [https://perma.cc/5NG7-3674].

56. This concept is humorously depicted in the popular webcomic xkcd. *See Security*, XKCD (Feb. 2, 2009), https://xkcd.com/538 [https://perma.cc/252P-ZTHS].

57. *See* Recommendation on Defendant's Motions to Suppress Custodial Statements and Fruits of Illegal Search at 1–3, United States v. Felders, No. 16-CR-117 (E.D. Wis. Mar. 15, 2017). Similarly, it seems likely that the evidence on the decrypted device would nonetheless be admissible if the password were obtained with a *Miranda* violation. *See* Orin Kerr, *When 'Miranda' Violations Lead to Passwords*, WASH. POST: VOLOKH CONSPIRACY (Dec. 12, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/12/12/when-miranda-violations-lead-to-passwords [https://perma.cc/L4QP-74BU].

Searching a device will often be a Fourth Amendment search that requires a warrant. *See* United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007). If the person who has common authority over the

key voluntarily. This approach is not limited to targets. Anyone who knows the password is a potential subject for disclosure. If a wife knows her husband's key, for example, the government can compel it from her even if she is not a regular user of the data the key can unlock.[58] Compelling the key can be understood as a close cousin of finding the key. The government effectively "finds" the key by identifying someone who has or knows it and then compelling them to disclose or use it.

Compelling the key raises two practical challenges. First, a person who knows or has the key must be known and available to the government. The government may not know who knows or has possession of the key. For example, imagine officers seize a collection of cell phones from a closet inside a drug-stash house. They will possess the phones, but they may not know who used any particular phone. Alternatively, the government might know who knows the password, but that person may be dead, missing, or in another jurisdiction and therefore out of reach.[59]

The second problem is that the available person who knows or controls the key may not wish to disclose it. This raises the legal question of how much pressure the government can exert to encourage disclosure. The answer depends largely on the limits of the Fourth and Fifth Amendments.[60] These constitutional limits are not yet well-developed and considerable ambiguity remains about how much of a burden they impose. Nonetheless, a basic overview of the range of options is helpful to understand this encryption workaround. The constitutional framework that applies when the government seeks to compel a key depends on which of the three basic ways the government chooses to compel the key: disclosing the key, entering in the key, or using biometric access.

First, the government might seek an order requiring a person to disclose the key to the government. The primary barrier to this method is the Fifth Amendment privilege against self-incrimination.[61] When the government uses the threat of legal punishment to compel an individual to divulge a key, the

---

device and knows the key consents to both disclosing the key and the officer's search, the device can be searched without a warrant. *See* United States v. Buckner, 473 F. 3d 551, 554 (4th Cir. 2007). On the other hand, the government might voluntarily obtain the key from a person who lacks common authority over the device but happens to know the key. In that case, the key will be obtained voluntarily, but the person's consent does not provide a ground for searching the device.

58. The spousal testimonial privilege would only apply to testimony that the husband told her the password in confidence; it would not otherwise protect against disclosure of the password. *See, e.g.*, Humphrey v. State, 979 So. 2d 283, 285 (Fla. Dist. Ct. App. 2008).

59. The San Bernardino terrorism case is an example: the user of the phone was dead before the government sought to unlock the phone. *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.941f798e089e [https://perma.cc/JH4Q-MVAM].

60. *See* U.S. CONST. amends. IV, V.

61. The Fourth Amendment does not impose a barrier. *See* United States v. Dionisio, 410 U.S. 1, 9 (1973) (holding that there are no Fourth Amendment limits on forcing a person to testify before a grand jury).

government is seeking to compel testimony.[62] The person is being forced to go into his memory and divulge his recollection of the key. Some authority supports the view that the key is itself incriminating if its disclosure leads causally to the discovery of incriminating evidence; however, this matter is not free from doubt.[63] In some circumstances, a disclosed key may be incriminating based on its content alone, such as if the password contains a message.[64]

Second, the government might instead order individuals to produce a decrypted device. Investigators typically provide the person with a locked device, and the person can comply with the order by entering the key without disclosing it to the government. The Fifth Amendment once again provides the legal framework,[65] although the standard for compelled acts of decryption may be different than the standard for disclosing a key. Courts have analyzed compelled acts of decryption under the act of production doctrine introduced in *Fisher v. United States*.[66] Under this framework, an act is testimonial for what it implicitly communicates about a person's state of mind.[67] An act of decryption by entering a password is testimonial because it amounts to testimony that the person knows the password.[68]

The primary uncertainty with compelling acts of decryption is how to apply the foregone conclusion doctrine.[69] The foregone conclusion doctrine teaches that, if the testimonial aspect of an act of production is already known to the government and is not to be proven by the testimonial act, the testimony is a foregone conclusion and the Fifth Amendment privilege does not apply.[70] Courts are

62. United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing a subpoena for computer passwords, reasoning that the subpoena would have required the suspect "to divulge through his mental processes his password").

63. *Compare id.* (quashing subpoena on basis that "[c]ompelled testimony that communicates information that 'may lead to incriminating evidence' is privileged" (quoting United States v. Hubbell, 530 U.S. 27 (2000))), *with* Orin Kerr, *A Revised Approach to the Fifth Amendment and Obtaining Passcodes*, WASH. POST: VOLOKH CONSPIRACY (Sept. 25, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes [https://perma.cc/DEQ9-3NJC] (questioning whether testimony that "is solely of value for its casual connection to evidence" is incriminating).

64. In a gang case, for example, disclosing the password "IliveforMS13" might be incriminating.

65. The Fourth Amendment provides almost no protection in this context because the burden of entering a passcode will not be onerous. *See In re* Horowitz, 482 F.2d 72, 75, 78–79 (2d Cir. 1973) (holding that the only Fourth Amendment limit upon compelling documents is reasonableness, which looks to the defendant's burden of complying with disclosure).

66. 425 U.S. 391, 409–12 (1976).

67. *Id.* at 411.

68. *See* United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017).

69. The authors of this Article disagree on whether courts have uniformly held that the act of production doctrine and the foregone conclusion framework is applicable to acts of producing decrypted data. In Schneier's view, some courts have held that the foregone conclusion doctrine is per se inapplicable in such cases. *See* United States v. Mitchell II, 76 M.J. 413, 424–25 & n.5 (C.A.A.F. 2017) (Ryan, J., dissenting). In Kerr's view, however, this understanding is incorrect. Although courts disagree on what standard the foregone conclusion doctrine requires, no court has held that it is per se inapplicable to acts of decryption. *Cf. id.* at 419–20 (considering whether the foregone conclusion doctrine is satisfied on the facts).

70. *See* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 8.13(a) (5th ed. 2009).

uncertain about what facts must be established as known by the government to make the testimony implicit in decrypting a foregone conclusion.

On one view, the government must establish that it already knows the specific files it expects to find on the decrypted device.[71] From this perspective, decrypting the device amounts to testimony about its contents; that testimony is a foregone conclusion only if the government already has relatively detailed awareness of the contents of the device when in decrypted form.[72] On another view, the government must establish only that it knows that the person knows the password. From this perspective, decrypting the device amounts only to testimony that the person knows the password; that testimony is a foregone conclusion if the government already knows that the person knows the password. This standard would be vastly easier for the government to meet in practice because evidence that the person uses the phone regularly is likely sufficient to establish that the person knows the password.[73] Case law is not clear on which standard is correct.[74]

A third way of compelling the key is by compelling a person to use a biometric means to unlock the device, such as a fingerprint reader, if such an access mechanism has been set up. This ordinarily will not raise Fifth Amendment issues because providing fingerprints or other body parts is not testimonial.[75] On the other hand, this process can raise significant Fourth Amendment issues. Typically, the suspect must be "seized" for his fingerprints to be placed on a fingerprint reader.

The open legal question is what level of cause and what court order the government might need to seize the suspect to enable the biometric access. Some courts have held that reasonable suspicion that a particular person committed a crime is

---

71. *See id.*; *see also In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1349 n.8 (11th Cir. 2012) (finding the foregone conclusion doctrine applicable where the government shows "with some reasonable particularity that it seeks a certain file and is aware . . . the file exists in some specified location").

72. *See* In re *Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1344.

73. State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016). As the Third Circuit recently stated in dicta:

> [A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password for these devices."

Apple MacPro Comput., 851 F.3d at 248 n.7.

74. For a detailed look at the arguments, see Orin Kerr, *The Fifth Amendment Limits on Forced Decryption and Applying the 'Foregone Conclusion' Doctrine*, WASH. POST: VOLOKH CONSPIRACY (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 [https://perma.cc/YJ3M-9KC5].

75. *See* State v. Diamond, 890 N.W.2d 143, 151 (Minn. Ct. App. 2017). Forced use of a biometric reader to unlock a device can raise potential Fifth Amendment issues if the government leaves the question of how to comply up to the subject of the order, who may, for example, program her biometric reader to respond only to a specific body part. *See* Orin Kerr, *The Fifth Amendment and Touch ID*, WASH. POST: VOLOKH CONSPIRACY (Oct. 21, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id [https://perma.cc/YGR2-YBLB].

sufficient to compel a suspect to provide a fingerprint that can show a match with known evidence.[76] A similar standard might apply to compelled biometric assistance. When investigators seek a fingerprint to unlock a phone, however, ordinarily they are not interested in proving a fingerprint match. Instead, they want to unlock the phone to enable searching its contents, which ordinarily requires a search warrant. This might conceivably alter the Fourth Amendment standard because the question of whether the phone's owner committed a crime can be quite different from that of whether there is evidence in the phone.[77] The precise standard currently remains unknown.

Another uncertainty is whether the Fourth Amendment permits judges to issue warrants that compel people present at the scene of a search to submit to forced fingerprinting or other compelled biometric access. News reports suggest that some federal agents have requested such provisions and that at least one judge has issued a warrant that includes them.[78] On the other hand, a federal magistrate judge in Chicago rejected a request to include such a provision in a warrant.[79] According to the magistrate judge, the provision was improper because the government had not established sufficient cause justifying the seizure of every person present at the scene of the search.[80]

Notably, compelling a key raises practical and legal hurdles rather than technical ones. Sophisticated technological resources are not required, but a person who knows the key may refuse to hand it over or use it. The government can force a target to use a biometric indicator, for example, by physically placing her finger on the reader.[81] But the government has no way to actually force a suspect to disclose a key or decrypt a device even if a court rules that no Fifth Amendment privilege applies. The government must instead hope that the punishment of noncompliance is greater than the expected punishment for the original crime. If the evidence on the device is particularly damning, a rational suspect may choose to suffer the punishment for noncompliance rather than suffer the greater punishment of the underlying crime.

---

76. *See, e.g.*, United States v. Sechrist, 640 F.2d 81, 86 (7th Cir. 1981).

77. Imagine a victim of domestic violence took photographs of her injuries on her cell phone. There would be probable cause that evidence is on the phone, but there would be no cause to believe that the phone's owner committed a crime. For this reason, perhaps the type of cause required to take a fingerprint in touch ID cases is reason to think that the person controls a phone rather than reason to think that the owner committed a crime.

78. *See* Karen Turner, *Feds Use Search Warrants to Get into Fingerprint-Locked Phones*, WASH. POST (Oct. 18, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/18/feds-use-search-warrants-to-get-into-fingerprint-locked-phones/?utm_term=.a326936a20cf [https://perma.cc/7P76-AZVG].

79. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1074 (N.D. Ill. 2017).

80. *Id.* at 1068–69.

81. If a suspect refuses to comply with a lawful order, officers may use force to effectuate the order or, depending on the jurisdiction, may arrest the individual for disobeying a lawful order. *See, e.g.*, Spry v. State, 914 A.2d 1182, 1186–90 (Md. 2007) (discussing the scope of powers to make arrests for disobeying a lawful order).

Enforcing compliance with orders to decrypt typically requires legal proceedings for contempt (if a court order is obtained)[82] or failure to follow an officer's lawful order (if no such order is obtained).[83] The government must show that the defendant is willfully refusing to comply with a lawful order, either by outright refusal or by falsely claiming that he is unable to comply.[84] The defense can assert claims of privilege or argue that he is unable to comply with the order.

One difficulty with enforcing compliance with decryption orders is that a court may be unable to accurately determine if the defendant is unable to comply. A defendant may truthfully claim to have forgotten the password or to have never known it. If the trial judge finds that testimony unpersuasive and wrongly believes that the defendant is testifying falsely, the judge may wrongly convict the defendant of willful refusal to comply with the order. In that case, using strong encryption may actually work against the suspect's interests: an innocent suspect who forgets his password presumably would rather have the government search his device and clear him of suspicion than face the possibility of jail time for contempt if the judge believes he is only pretending to be unable to comply with a decryption order.

The encryption workarounds discussed so far have all been key-based. They involve means of obtaining and then using a key to decrypt encrypted data. We next turn to workarounds that do not require the key.

D. EXPLOIT A FLAW IN THE ENCRYPTION SCHEME

The first non-key-based encryption workaround is to exploit a flaw in the encryption scheme to gain access without the key. This is analogous to breaking into a locked car by inserting a Slim Jim under the window seal instead of picking the lock. Access is gained without the key by exploiting a weakness in the system designed to keep people out.

This weakness can take several forms. It can be a mathematical weakness in the encryption algorithm, a weakness in the random-number generator used to provide inputs to that encryption algorithm, or a weakness resulting from the implementation of that algorithm in software on a computer.[85] The weakness could be the result of new advances in the science of cryptanalysis or a mistake made by a system designer or programmer.

---

82. *See, e.g.*, FED. R. CRIM. P. 41 (providing procedure for obtaining a federal search warrant).

83. *See* Orin Kerr, *Sandra Bland and the 'Lawful Order' Problem*, WASH. POST: VOLOKH CONSPIRACY (July 23, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/23/sandra-bland-and-the-lawful-order-problem/?utm_term=.e4535316dd13 [https://perma.cc/M23K-VQUP] (discussing the law concerning failures to comply with lawful orders).

84. *See In re* Weiss, 703 F.2d 653, 662–63 (2d Cir. 1983).

85. *See, e.g.*, Derek Kortepeter, *Modern Cryptographic Methods: Their Flaws, Their Subsequent Solutions, and Their Outside Threats*, TECHGENIX (June 27, 2016), http://techgenix.com/modern-cryptography-methods/ [https://perma.cc/5E44-H6EN] (discussing various types of weaknesses in encryption systems).

Flaws are not uncommon. All software contains bugs, and commercial software can contain thousands of them.[86] Some of these bugs result in security vulnerabilities, and some of those vulnerabilities can be exploited to defeat the encryption scheme. Hackers, criminals, foreign governments, and others can take advantage of these flaws in encryption systems.[87] Additionally, some flaws are deliberately inserted, either by the software vendors themselves or by individuals wanting to subvert the security of the software.[88] These are commonly called "backdoors."[89] In the 1990s, the FBI endorsed a requirement that vendors create these backdoors for their agents to use.[90] The FBI has more recently expressed an interest in that same position, although with less certainty than in the past.[91]

The success of exploiting a flaw is contingent on finding or knowing an exploit that will work with a particular device and software combination. Flaws may be specific to a particular version of a device or operating system. Flaws only work for a limited time because when exploits become known, many companies and software writers will try to quickly correct the flaw and issue a patch.[92] This is not guaranteed, however, and known flaws can persist in some systems for years after discovery. Furthermore, issuing a patch is no guarantee that users will apply the patch and secure their systems. Many systems remain unpatched for months or even years.[93]

Nonetheless, exploiting a flaw against a smart user and a well-maintained system often requires knowledge of a flaw that is not otherwise widely known or has not yet been corrected for that particular device. For this reason, exploiting a flaw

86. *See* BEN CHELF, MEASURING SOFTWARE QUALITY: A STUDY OF OPEN SOURCE SOFTWARE 2–4 (2006) https://www.itworldcanada.com/archive/WhitePaperLibrary/PdfDownloads/Coverity.ProtectedEntry.pdf [https://perma.cc/2UNP-WMHK].

87. *See, e.g.*, Mike Peterson, *UK Police Have Resorted to 'Mugging' Criminals Using an iPhone to Bypass Encryption*, IDROP NEWS (Dec. 5, 2016, 1:12 PM), https://www.idropnews.com/news/uk-police-have-resorted-to-mugging-criminals-using-an-iphone-to-bypass-encryption/27387 [https://perma.cc/MR47-Z54R].

88. *See* Bruce Schneier, *How to Design—and Defend Against—the Perfect Security Backdoor*, WIRED (Oct. 16, 2013, 9:25 AM), https://www.wired.com/2013/10/how-to-design-and-defend-against-the-perfect-backdoor [https://perma.cc/V4CM-J8DJ].

89. *See, e.g.*, *id.*; United States v. Budziak, No. CR-08-00284, 2011 WL 175505, at *2 (N.D. Cal. Jan. 18, 2011).

90. *See* DANIELLE KEHL, ANDI WILSON, & KEVIN BANKSTON, NEW AM., DOOMED TO REPEAT HISTORY? LESSONS FROM THE CRYPTO WARS OF THE 1990S 5–11 (June 2015) https://na-production.s3.amazonaws.com/documents/Doomed_To_Repeat_History.pdf [https://perma.cc/C9WQ-EAN6] (describing historical effect by U.S. law enforcement and intelligence agencies to ensure backdoor access to encrypted contents through "Clipper Chips").

91. *See id.* at 1.

92. Many companies offer "bug bounties" that will pay individuals for reporting flaws so the companies can fix the flaws more quickly. *See Bug Bounty List*, BUGCROWD, https://bugcrowd.com/list-of-bug-bounty-programs [https://perma.cc/Y4BY-N7Y8] (listing companies that participate in such programs).

93. *See, e.g.*, Roger A. Grimes, *Zero-Days Aren't The Problem—Patches Are*, CSO (June 1, 2016, 3:00 AM), https://www.csoonline.com/article/3075830/data-protection/zero-days-arent-the-problem-patches-are.html [https://perma.cc/3K2U-K9QB] (noting that "[m]ost exploits involve vulnerabilities that were patched more than a year ago," but that "the vast majority organizations that suffer exploits are those that don't patch in the first year or ever patch at all").

ordinarily requires technological expertise or the resources to buy access from someone who has that expertise, raising a technological challenge rather than a legal challenge.

A dramatic example of such a flaw was discovered by security researcher John Gordon in 2015.[94] Gordon discovered a flaw in the then-new Android smartphone operating system called "Lollipop."[95] A phone running Lollipop would unlock after several minutes if a user entered any extremely long string of characters—roughly fifty pages of text—at the password prompt.[96] The exceedingly long data entry overwhelmed the phone, causing it to crash and bypass the lock.[97] Gordon notified Google of the flaw, and Google then created and distributed a patch to correct the error.[98]

Exploiting a flaw can work in concert with other encryption workarounds. Consider how the government gained access to the iPhone used by San Bernardino attacker, Syed Farook.[99] Farook's phone was known to have the auto-erase feature that thwarts passcode guessing, and the government had sought Apple's assistance in disabling that feature to allow the FBI to guess the passcode quickly.[100] Apple objected to the assistance order,[101] but the FBI was able to gain access to the phone a different way. Although details remain murky, it appears that a private company found an exploit that disabled the auto-erase function.[102] Some have claimed that the FBI paid the company $1 million or more to use the exploit, which allowed the FBI to guess the passcode and access the phone.[103] This approach relied on two workarounds in tandem: exploit the flaw and guess the key.

E. ACCESS PLAINTEXT WHEN THE DEVICE IS IN USE

The fifth workaround is to access plaintext when the device is in use. Because encrypted data must be decrypted to be read or used, the government can bypass encryption by gaining access to information in its decrypted form. Even the most

94. *See* Jose Pagliery, *To Hack an Android Phone, Just Type in a Really Long Password*, CNN: TECH (Sept. 16, 2015, 10:37 AM), http://money.cnn.com/2015/09/16/technology/android-hack/index.html [https://perma.cc/RK2M-LHB3].

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *See* Sean Hollister & Connie Guglielmo, *How an iPhone Became the FBI's Public Enemy No. 1 (FAQ)*, CNET (Feb. 25, 2016, 4:00 PM), https://www.cnet.com/news/apple-versus-the-fbi-why-the-lowest-priced-iphone-has-the-us-in-a-tizzy-faq [https://perma.cc/8J32-CVVM].

100. *Id.*

101. *Id.*

102. *See* Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 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 [https://perma.cc/DZR6-2SW9].

103. *See id.*; Devlin Barrett, *FBI Paid More Than $1 Million to Hack San Bernardino iPhone*, WALL ST. J. (Apr. 21, 2016, 4:07 PM), https://www.wsj.com/articles/comey-fbi-paid-more-than-1-million-to-hack-san-bernardino-iphone-1461266641 [https://perma.cc/SZB5-E7CA].

securely encrypted e-mail will eventually be displayed on the screen so that the recipient can read it. Although the message may be encrypted from device to device, it will be readable in an unencrypted form on the sender's keyboard and on the recipient's screen. Access to either device will enable access to a plaintext copy of the information. This approach is similar to the exploiting a flaw method discussed above, except that it exploits a necessary property of the computer or phone itself rather than an uncorrected flaw in the encryption algorithm.

This technique usually works only in real time when the government has ongoing access to the device in use. Imagine investigators target a suspect's encrypted hard drive. Disk encryption only protects data on a system that is turned off. When a user turns the system on and enters her key, this key gets stored in memory as long as the computer is on and being used.[104] Taking control of the computer while it is on allows access to that key or the files on the hard drive.[105]

The technological sophistication required to access plaintext when the device is in use varies widely. In some cases, investigators can simply grab the device from the suspect.[106] Consider the investigation into the Silk Road website, which was a massive online black market shut down by the FBI in 2013.[107] The FBI carefully planned the arrest of lead suspect Ross Ulbricht to bypass the whole-disk encryption on his laptop.[108] Ulbricht was known to be using his laptop at a public library.[109] The laptop was encrypted when shut down, but decrypted when in use.[110] To capitalize on this, the FBI sent two plainclothes agents into the library posing as a couple.[111] While standing next to Ulbricht, the two agents began a loud fight, which distracted Ulbricht and allowed one of the agents to grab the laptop while it was open.[112] That agent turned it over to a third officer who immediately began to search the device while Ulbricht was placed under arrest.[113] The ruse enabled the FBI to bypass Ulbricht's whole-disk encryption by taking it from his hands.[114]

---

104. *See* J. Alex Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, 17 USENIX SECURITY SYMPOSIUM 45, 54 (2008) (discussing how encryption keys can be extracted from memory images).

105. *See id.* Alternatively, an investigator could insert a key logger into a computer to collect keystrokes or install a hidden camera in the room with the computer that can record what the suspect is typing and reading.

106. *See* Peterson, *supra* note 87.

107. *See generally* NICK BILTON, AMERICAN KINGPIN: THE EPIC HUNT FOR THE CRIMINAL MASTERMIND BEHIND THE SILK ROAD (2017) (discussing the Silk Road website and investigation).

108. *See* Natasha Bertrand, *The FBI Staged a Lovers' Fight to Catch the Kingpin of the Web's Biggest Illegal Drug Marketplace*, BUS. INSIDER (Jan. 22, 2015, 11:14 AM), http://www.businessinsider.com/the-arrest-of-silk-road-mastermind-ross-ulbricht-2015-1 [https://perma.cc/M42D-NSYR].

109. *Id.*

110. *See id.*

111. *See id.*

112. *Id.*

113. *Id.*

114. *See id.*

If investigators cannot gain physical control of a device, accessing it while it is in use raises more difficult technical and legal questions. The chief alternative is to hack into the device remotely while it is connected to the Internet.[115] The remote Internet connection provides the means to access the computer without immediate physical control. This is much more complicated than physically seizing the machine. First, hacking requires the government to figure out a technical means of gaining remote access to the device. Second, government hacking can raise complex legal questions under the Fourth Amendment and other laws.

Dozens of federal courts are currently considering the legality of one prominent example: the search authorized by the Playpen warrant.[116] Playpen was a child pornography website available only using Tor. [117] The government took over the website in an effort to trace back the identities of the site's visitors.[118] Because Tor masked the true IP addresses of its visitors, however, the government could not trace back visitors in the usual way: visits only logged the IP addresses of Tor nodes, which could not be traced back to the IP addresses visitors themselves used to establish an Internet connection to visit Playpen.[119] To reveal the true IP addresses of users, the government obtained a warrant authorizing the installation of a "network investigative technique (NIT)"—in other words, government malware—on the computers of Playpen visitors.[120]

The NIT was a workaround that responded to Tor's use of encryption and anonymizing software to hide IP addresses. When a user logged into the Playpen site, the NIT would travel from Playpen back to the user's machine, install itself, and, from there, locate identifying information about the user's machine, including its real IP address.[121] It would then send that information to the government.[122] After the warrant was signed, the Playpen NIT was successfully placed on more than 1,000 machines around the world.[123] The information revealed by the NIT led to the arrest and prosecution of over 200 defendants in the United States.[124]

This complex technical means of access to data raises many legal questions that are currently before federal courts in challenges to the Playpen

115. *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 6 (2014) (discussing governmental use of remote hacking). Recent news reports suggest that the CIA has developed significant abilities along these lines. *See* Greg Miller & Ellen Nakashima, *WikiLeaks Says It Has Obtained Trove of CIA Hacking Tools*, WASH. POST (Mar. 7, 2017), https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html [https://perma.cc/H73U-7NSK].

116. *See* Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST: VOLOKH CONSPIRACY (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant [https://perma.cc/7E7J-ZKXP].

117. *Id.*

118. *Id.*

119. *See id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

investigation.[125] The legal questions include: Was accessing the suspects' machines to obtain their IP addresses a Fourth Amendment search?[126] Did accessing computers that were subsequently located outside the district where the warrant was obtained violate the territoriality rules of the search warrant statute?[127] Did the single warrant used to effectuate hundreds or thousands of searches satisfy the Fourth Amendment's probable cause and particularity requirements?[128] Finally, does the government need to disclose to the defense how the NIT worked?[129] For our purposes, the answers to these questions are less important than how and why they arose. The use of Tor blocked the usual means of investigation, requiring a complex technical workaround with novel legal implications to obtain the same information.

F. LOCATE A PLAINTEXT COPY

The sixth and final type of encryption workaround is to obtain a separate, unencrypted copy of the information. The target may have multiple copies of the sought-after records, and the government may be able to access a plaintext version. Unlike the workarounds discussed above, this approach does not involve decryption of a known encrypted file or device. It instead looks for another copy of the sought-after information. In that sense, this approach may be less of a workaround than an alternative strategy. Instead of bypassing encryption, it avoids encryption entirely.

Locating a plaintext copy may provide a second-best substitute when law enforcement cannot successfully decrypt a file or device. Police looking for the final version of the ransom note on the suspect's computer might be blocked from reading it but find unencrypted earlier drafts that the word processing software automatically created.[130] Investigators wishing to read e-mails on a locked phone might instead go to the cloud provider and see if copies of the e-mails are stored in the cloud. Similarly, the user of a locked phone may have stored an unencrypted backup copy using a remote cloud storage service.

Once again, the recent investigation into the terrorist attack in San Bernardino, California, provides a salient example. The government attempted to decrypt Farook's iPhone pursuant to a search warrant served on Apple.[131] When that

125. *See The Playpen Cases: Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions [https://perma.cc/C3F6-TWLW].

126. *See* Orin Kerr, *Remotely Accessing an IP Address Inside a Target Computer Is a Search*, WASH. POST: VOLOKH CONSPIRACY (Oct. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search [https://perma.cc/CR7D-Z5EV].

127. *See, e.g.*, United States v. Allain, 213 F. Supp. 3d 236, 248–51 (D. Mass. 2016).

128. *See id.* at 247–48.

129. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 596–601 (E.D. Va. 2016).

130. *See, e.g.*, Commonwealth v. Copenhefer, 587 A.2d 1353, 1355–56 (Pa. 1991) (explaining officials were able to examine draft copies of a ransom note automatically saved by word processing software on suspect's computer), *abrogated by* Commonwealth v. Rizzuto, 777 A.2d 1069 (Pa. 2001).

131. Ellen Nakashima & Mark Berman, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, WASH. POST (Feb. 20, 2016), https://www.washingtonpost.com/world/

proved initially unsuccessful, the government obtained what was available from an iCloud backup copy.[132] The cloud-stored copy was somewhat outdated because the phone had last been backed up six weeks before the shooting.[133] Nonetheless, the backup gave the government access to at least some of the contents of Farook's phone before the government was able to decrypt it.[134]

Successfully locating a plaintext copy requires four conditions to be met. First, an additional, unencrypted copy of the sought-after information must exist. Second, the government must be able to find it. Third, the government must have the legal authority to search for and seize it. These three requirements should be intuitive: For the government to obtain something, that thing must exist and the government must have the legal and technical ability to obtain it. These requirements therefore mirror the conditions of finding a key.[135]

The fourth requirement is less intuitive: The unencrypted copy must be sufficiently similar to the encrypted copy to be an adequate substitute. The contents of hard drives and individual files can change over time, and data that was copied and left in plaintext form in the past may no longer match a newer version that was encrypted. Whether a plaintext copy is an adequate substitute may be difficult to answer because investigators will not know the data on the encrypted file that they cannot access.

III. THE LESSONS OF ENCRYPTION WORKAROUNDS

The taxonomy of encryption workarounds suggests a series of lessons about law enforcement responses to the widespread use of encryption. A broad perspective illuminates the tradeoffs inherent in each approach, as well as the relationships among them. We hope that this perspective helps identify the contours of this new investigatory environment. To that end, we offer four lessons about the new environment that follow from the taxonomy of workarounds.

The first lesson is that there is no single magic way for the government to get around encryption. The nature of the problem is one of probabilities rather than certainty. Different approaches will work more or less often in different kinds of cases. In that sense, the challenge of bypassing encryption is similar to the challenge of interrogating a suspect: some suspects will waive their rights and confess and others will assert their rights and end the interrogation. There are no certainties about what will work.

Second, the different resources required to pursue different workarounds may have considerable distributional effects on law enforcement. Some workarounds require technical expertise and deep pockets. Others require neither. As a result, low-resource agencies will rely heavily on low-resource approaches whereas

national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html?utm_term=.f5b4d765543c [https://perma.cc/UGB8-JXLE].

132. *Id.*

133. *Id.*

134. *See id.*

135. *See supra* Section II.A.

high-resource agencies will choose from a wider range of workarounds. This may lead to the federal government taking over certain kinds of state and local investigations.

The third lesson is that the degree of third-party assistance that can be legally compelled is likely to be a continuing theme of the law of encryption workarounds. Encryption technology runs on software created outside the government and runs on hardware manufactured by private companies. Expertise relevant to workarounds will be found outside the government. As the recent dispute over the San Bernardino iPhone revealed, how much authority the government has to compel the assistance of third parties is a fundamental question of encryption workarounds.

Finally, fourth, the law of encryption workarounds is still developing. Many workarounds raise complex and novel legal questions that courts are only beginning to confront. Until the law of encryption workarounds becomes more settled, it is too early to know how much the widespread use of encryption will interfere with the successful resolution of criminal investigations.

We expand on each of these lessons below.

A. WORKAROUNDS ARE NEVER GUARANTEED

The first lesson of encryption workarounds is that there are no guarantees. Workarounds are inherently probabilistic. On one hand, no approach will work every time. On the other hand, that a target has used encryption does not mean the investigation is over. The government has to search for a workaround that might succeed.

The uncertainty is inherent. Whether a particular workaround is effective, or whether any of the workarounds will work, will often depend on facts that are unknown or even unknowable when the encryption is discovered. Did the suspect write down the passcode somewhere? If a court orders him to decrypt the device, would he agree to do so? Is there a security weakness that the government can exploit for that particular device running that particular software? Does someone else know the passcode? Is there an unencrypted copy of the relevant files somewhere else? These questions do not have universal answers. They typically require investigative work to find out which of the strategies might prove successful.

Proposals to guarantee government access to a key would not alter this basic dynamic. For example, Senators Richard Burr and Dianne Feinstein recently released a "discussion draft" of a bill that would require hardware manufacturers and designers of software products that enable user encryption to "provide" the government with the data in an "intelligible format" pursuant to a court order.[136] If this bill became law, companies would be required to have a way to decrypt user data. The Burr–Feinstein proposal was widely criticized on its merits, and it

136. *See* Compliance with Court Orders Act of 2016, 114th Cong. §3(a)(A) (discussion draft 2016), http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf [https://perma.cc/QFY3-R9X9].

was never formally introduced.[137] At first blush, however, the Feinstein–Burr approach may create the impression of guaranteeing successful workarounds as a matter of law.

That impression is false. Although Congress can pass a law, there is no way to make that law practically enforceable. Any legal regime that requires decryption by companies can be circumvented by users, essentially providing a reverse encryption workaround against the encryption workaround. Users can change to open source software that companies can't control, employ foreign software that the United States can't regulate, or take other countermeasures. Legal mandates, at most, can regulate default uses of encryption products. Defaults are important, certainly.[138] Many or most users use products in the default way, even if changes are simple to make.[139] But even at its hypothetical best, legislation can only facilitate particular workarounds. It cannot ensure their success.[140]

That encryption will stymie some government investigations does not make it unique. Former FBI Director James Comey has said that encryption "takes us to a place—absolute privacy—that we have not been to before."[141] In a limited sense, Comey is right. Any physical place can be entered somehow, which means that the idea of data that can be held, but not accessed, is new. But in a broader sense, there is nothing new about the dynamics of encryption. The success of investigative tools and methods are always matters of chance. When a crime occurs, an eyewitness might have seen it, or maybe no one did. When the police interrogate a suspect, the suspect might confess or refuse to talk. When the police search a house for drugs, the drugs might be there or they might have been moved or destroyed. When the police investigate a conspiracy, a conspirator might flip and cooperate with the government or perhaps no conspirator will. No law enforcement technique works every time. The challenges of encryption are no exception to that general rule.

Perhaps the best analogy is to interrogations. When the police have a suspect and want a confession, the law gives the police a set of tools they may use to persuade the suspect to confess.[142] No interrogation method works every time. In some cases, no matter what the government does, suspects will confess. In other

---

137. *See* Rainey Reitman, *Security Win: Burr–Feinstein Proposal Declared "Dead" for This Year*, ELECTRONIC FRONTIER FOUND. (May 27, 2016), https://www.eff.org/deeplinks/2016/05/win-one-security-burr-feinstein-proposal-declared-dead-year [https://perma.cc/P47W-M4DK].

138. *See* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 591–95 (2006).

139. *See id.*

140. Imagine that Congress passed a federal law after the San Bernardino case prohibiting the software option to block password guessing. A criminal suspect or terrorist could readily block the usefulness of this law by simply switching from a four-digit numerical default passcode that could be guessed within a day to a longer alphanumeric password that would take months or decades to guess.

141. Eric Geller, *FBI Director Warns Against Unbreakable Encryption And "Absolute Privacy*," DAILY DOT (last updated Apr. 7, 2016, 3:02 PM), http://www.dailydot.com/layer8/encryption-privacy-security-fbi-director-james-comey-kenyon-conference [https://perma.cc/JH3D-N79E].

142. *See* LAFAVE, *supra* note 70, at §§ 6.1–6.10 (discussing the law of police interrogations and confessions).

cases, no matter what the government does, suspects will assert their rights and refuse to speak. The government must work with the inherently probabilistic nature of obtaining confessions. Similarly, the government must work with the inherently probabilistic nature of encryption workarounds.

B. WORKAROUNDS WILL HAVE DISTRIBUTIONAL EFFECTS ON LAW ENFORCEMENT

Another characteristic of encryption workarounds is that different workarounds require different resources, which is likely to have considerable distributional effects on law enforcement. Some workarounds require technical expertise and deep pockets. Others require neither. Because resources vary considerably among and within governments, some workarounds can be used often by any governmental agency and others are likely to be used rarely and only by a few. As a practical matter, this likely means that the federal government, with its greater resources, is likely to have a wider range of workarounds to choose from. This may lead to the federal government taking over certain kinds of state and local investigations.

In general, compelling the key uses the least amount of resources. If a person is available who knows the key, the government need only assert legal pressure on that person to persuade them to disclose it. As long as the Fifth Amendment does not block the government's order, the government can exert that pressure and the suspect must choose whether to comply. The strategy of compelling the key prompts a traditional question of contempt law: Is the pressure of jail time sufficient to force the subject of the order to comply? This approach can certainly raise complex practical questions, such as how to know when the subject of an order genuinely cannot comply with a disclosure order.[143] But no special technology or resources are required.

On the other hand, some encryption workarounds are very costly and require significant technical expertise. For example, the NIT warrant used in the Playpen investigation required developing and using special software.[144] Similarly, accessing the phone in the San Bernardino case reportedly required a payment in the neighborhood of $1 million to purchase use of a software exploit that could disable the feature that thwarted password-guessing.[145] Cyberweapons manufacturers, such as Hacking Team and Gamma International, sell espionage systems to third-world countries for millions of dollars to circumvent encryption.[146] Such expensive exploits are not likely to be broadly available within law enforcement.

---

143. The subject of an order may claim to have forgotten the passcode, requiring the court to determine if the subject is telling the truth and should not be held in contempt, or is lying and effectively is refusing to disclose or use it. *See, e.g.*, United States v. Apple MacPro Comput., 851 F.3d 238, 241–43, 247–49 (3d Cir. 2017) (discussing proceedings before a magistrate judge in which the subject of an order claimed to have forgotten the passcode).

144. *See supra* note 125 and accompanying text.

145. *See* Barrett, *supra* note 103.

146. *See* Aaron Sankin, *Forget Hacking Team—Many Other Companies Sell Surveillance Tech to Repressive Regimes,* DAILY DOT (July 9, 2015, 5:00 AM), https://www.dailydot.com/layer8/hacking-team-competitors [https://perma.cc/7BA9-2PQP].

The range of resources required for different workarounds is important because available resources vary considerably among government agencies. The intelligence agencies have a vast budget that makes them by far the best equipped to crack encryption.[147] Federal government resources will typically exceed the resources available in state cases. Local government resources will generally be the most modest of all. As a result, the toolkit of encryption workarounds varies considerably, depending on which government agency is investigating and how important any particular case happens to be.

The different resources needed for different encryption workarounds may further the federalization of many kinds of criminal investigations. This might happen in several different ways. First, particularly important state and local cases might get passed up to the federal government, either for investigative assistance or to take over the investigation, after the workarounds available to state and local police prove unsuccessful. Second, some kinds of investigations will require federal resources and are likely to succeed only at the federal level. State and local investigators will continue to investigate cases and will use the workarounds that require only modest resources, but other kinds of investigations are likely to need federal resources and expertise.

Similar dynamics are likely to influence the investigation of cases within federal law enforcement. When a case is particularly important and high-profile, investigators will pursue the full range of workarounds. The government will try everything in the big cases. On the other hand, more mundane and routine cases may receive less attention and fewer resources.

C. DEFINING THE LEGAL LIMITS ON ASSISTANCE WILL BE A CONTINUING CHALLENGE

A third lesson is that obtaining assistance from third parties outside the government—and the law determining how much assistance can be obtained—is likely to remain a continuing question raised by encryption workarounds. Encryption software and the hardware that hosts it is almost always designed and manufactured by the private sector. Although criminal investigators can pursue some encryption workarounds on their own, they will tend to have fewer resources and less expertise than some others in the private sector.[148] The prospects of deputizing that expertise can seem highly appealing to investigators. How much authority the government has to force the private sector to assist in investigations, and under what conditions, is therefore likely to be a recurring question.

From one perspective, this is not a new problem. In the common law era, criminal investigations relied heavily on mandates of third-party assistance. The

147. *See, e.g.*, Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html [https://nyti.ms/2kuiAmA].

148. The limit to "criminal investigators" is important because the expertise may exist elsewhere inside government. Intelligence agencies—particularly the NSA—have a great deal of technical expertise. That expertise is generally off-limits to law enforcement, however, because successful encryption workarounds that lead to criminal investigations will ordinarily become public and details may have to be disclosed to the defense in a criminal case.

raising of "hue and cry" required all able-bodied men within earshot to assist in the apprehension of a criminal after a witness announced that the crime had occurred in his presence.[149] Even today, any third-party witness can to be forced by subpoena to appear before the grand jury or in court to testify under penalty of perjury about what they have seen, at least if no special privilege exists.[150]

Reliance on third-party assistance is also an established aspect of surveillance law and practice. The government often needs assistance to conduct surveillance on privately owned networks. It can be less intrusive, more privacy-protective, and more efficient to have network providers conduct surveillance on the government's behalf than to have investigators conduct the surveillance themselves.[151] For that reason, network surveillance laws generally include assistance provisions requiring providers to provide necessary assistance to effectuate surveillance pursuant to court orders.[152] The Supreme Court has interpreted the All Writs Act to grant judges a somewhat analogous authority to mandate some amount of provider assistance in the execution of search warrants.[153]

Despite this tradition, third-party assistance with encryption workarounds raises a new twist. Requiring assistance from manufacturers and designers of encryption products can prompt a direct clash between the government's interest and that of the compelled party. The purpose of encryption is to block third-party access, while the goal of encryption workarounds is to enable it. Workarounds try to undo encryption's protection. As a result, mandating assistance with workarounds may compel manufacturers or designers of encryption products to help weaken the products they manufacture or design. To companies committed to providing the most secure product possible, assistance with workarounds may appear less a nuisance than a threat.

This dynamic emerged in the 2016 litigation over whether Apple was legally required to assist efforts to decrypt the iPhone used by San Bernardino attacker

149. Statute of Winchester, 1285, 13 Edw. I, cc. 1, 4 (Eng.). *See also In re* Quarles, 158 U.S. 532, 535 (1895) ("It is the duty . . . of every citizen, to assist in prosecuting, and in securing the punishment of, any breach of the peace of the United States."); Babington v. Yellow Taxi Corp., 164 N.E. 726, 727 (N. Y. 1928) ("Still, as in the days of Edward I, the citizenry may be called upon to enforce the justice of the state, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand.").

150. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 9 (1973) (noting "the longstanding principle that 'the public . . . has a right to every man's evidence'" (quoting United States v. Bryan, 339 U.S. 323, 331 (1950))).

151. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 621–22 (2003) (noting the tradeoffs between "direct surveillance," in which government agents conduct the surveillance, and "indirect surveillance," in which government agents get a court order requiring a provider to conduct the surveillance on the government's behalf).

152. *See* 18 U.S.C § 2518(4)(e) (2012) ("An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference . . . .").

153. *See* United States v. N.Y. Telephone Co., 434 U.S. 159, 172–73 (1977).

Syed Farook. Farook was already dead,[154] making the compel-the-key strategy unavailable. The government knew that Farook's phone had enabled the auto-erase feature to thwart passcode guessing, complicating the guess-the-password strategy.[155] The government had pursued the locate-another-plaintext-copy strategy and obtained an older iCloud backup of the phone's contents, but wished to obtain a more recent copy of the data. The government obtained an order seeking Apple's assistance in disabling the auto-erase function to enable quick password guessing.[156] Apple objected to the order.[157] The case ended without a legal ruling; the government ended up withdrawing its request because access was obtained by purchasing an exploit from an unnamed third party.[158]

The position of the technology industry toward the government in the Apple case was uniform and harshly negative. In an unusual public statement, Apple CEO Tim Cook condemned the request for the order as "dangerous" and said it would make Apple "hack [its] own users and undermine decades of security advancements that protect [its] customers—including tens of millions of American citizens—from sophisticated hackers and cybercriminals." [159] According to Cook, complying with the order would set a precedent that would weaken security for everyone with a phone: "The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe."[160] Almost every major technology company wrote or joined an amicus brief objecting to the government's request, including Amazon, Facebook, Google, Microsoft, Yahoo, AT&T, and Twitter.[161]

The staunch opposition of the technology industry to assisting government decryption efforts has particular importance for the critical question of how much third-party technical assistance the government can compel. The cases and statutes on technical assistance generally recognize some sort of proportionality requirement: parties can be forced to assist in some ways, but the assistance cannot impose "unreasonable burdens"[162] or be too obtrusive.[163] The difficult question is, how much assistance is too much?

---

154. *See* Nakashima & Berman, *supra* note 131.

155. *See* Nakashima, *supra* note 102.

156. *See* Nakashima & Berman, *supra* note 131.

157. *See id.*

158. *See* Nakashima, *supra* note 102.

159. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/2C2Q-REJ2].

160. *Id.*

161. The amicus briefs filed in the case have been compiled by Apple. *See Amicus Briefs in Support of Apple*, APPLE: NEWSROOM (Mar. 2, 2016), http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html [https://perma.cc/HU3V-SMTB]. This is no doubt part of the uniform reaction reflected the politics of the case. The major U.S.-based Internet companies have a global customer base, and international objections to U.S. government surveillance following the 2013 disclosures by Edward Snowden have made distancing themselves from U.S. surveillance practices a business necessity. *See* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11, 15–17 (2015).

162. United States v. N.Y. Telephone Co., 434 U.S. 159, 172 (1977).

163. *See* 18 U.S.C. § 2518(4)(e) (2012).

The technology industry's opposition to assisting with encryption workarounds makes such standards particularly difficult to apply. Companies control the design of their products. Because technical assistance standards generally use a baseline of the product as it exists at the time of the order,[164] companies wishing to thwart technical assistance orders can design their products now to make technical assistance in any future case as burdensome and obtrusive as possible. There is no natural baseline from which to measure the burden of assistance. The more a company fears a government assistance order in the future, the more it can take steps now to ensure that effective assistance will be unreasonable. Given the position of today's technology industry, we should not be surprised if the technical assistance companies provide will only diminish over time.

Proposals to mandate a key, such as key escrow laws proposed but not enacted in the 1990s,[165] can also be understood as a kind of assistance provision. When the government mandates a key, it enacts some statute or other binding legal rule that mandates access to an additional key that can be used to decrypt communications. This is an assistance requirement, but one that works in advance of any investigation. Instead of requiring companies to assist the government in a particular case, mandates would require manufacturers of hardware, designers of software, or both to weaken security practices and make an additional key available before the crime occurred. In effect, it is a meta-strategy designed to regulate products directly to ensure that there can always be a successful encryption workaround. On the other hand, mandating a key is the scenario technology companies fear most: By trying to guarantee workarounds, key mandates would also lead to weaker security.[166]

D. THE LAW OF ENCRYPTION WORKAROUNDS IS STILL DEVELOPING

A fourth observation about encryption workarounds is that the law surrounding them is still developing. Several workarounds raise novel legal questions. Circumventing encryption often relies on untested theories of government power that courts have only begun to address.

Consider several examples from the taxonomy in Part II. The Fourth and Fifth Amendment standards for compelling decryption remain uncertain. The Playpen warrant used to circumvent Tor's hiding user IP addresses raises difficult questions under the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure.[167] Similarly, the level of permitted technical assistance under statutes such as the All Writs Act is largely unresolved and raises complex questions about the standards for measuring the burden of assistance.

---

164. The government will seek assistance based on the state of the provider's network at the time the order was obtained, and it will then seek "assistance necessary to accomplish the [surveillance] unobtrusively and with a minimum of interference" relative to that state of the network. *Id.*

165. *See generally* HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION (1997), https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf [https://perma.cc/SZB8-PBSJ].

166. *See id.* (discussing how key mandates can lead to weaker security).

167. *See* Kerr, *supra* note 116.

That encryption workarounds raise novel and unresolved legal questions should not be surprising. Encryption blocks government access to information, and investigators will naturally respond by trying to gain access to the information in some other way that investigators did not need to consider before encryption was used. Those new ways often involve new strategies or technologies. Their legality will often be untested.

One consequence of the uncertain law of encryption workarounds is that the degree to which encryption will stymie investigations remains unclear. The tools available to investigators depend on both technology and law. Courts may approve encryption workarounds readily, or they may block them or place high barriers to their use. We don't yet know. As a result, the government's toolkit of encryption workarounds is presently unsettled. We can map out the possibilities, but we can't yet know how easy or difficult any particular workaround may prove to be. Until the law of encryption workarounds becomes clear, it is difficult to assess how much encryption will prove a practical barrier to investigations and in what kinds of cases the barriers will be greater or lesser.

CONCLUSION

The public debate over the impact of encryption on criminal investigations often treats encryption as a game-changer. On one side, the government argues that investigations are "going dark." Its supporters contend that that legislation to help or even mandate encryption workarounds may be required to make criminal cases solvable again. Civil libertarians respond that encryption offers an essential tool to restore necessary limits on government access to communications and to improve security for everyone. It is usually taken for granted, by both sides, that encryption will have a dramatic impact on government power. The disagreement is whether that impact is a net positive or negative.

This Article suggests a different view. How much encryption is a game-changer for criminal investigations depends on the success of encryption workarounds. When targets use encryption, the police do not simply give up. Rather, investigators turn to encryption workarounds that try to erase the barrier that encryption can create. Just as for every action there is an equal and opposite reaction, for every use of encryption to conceal communications there is a set of workarounds that could be employed to try to reveal them.

It is too early to tell how much the widespread use of encryption will impact the government's ability to solve criminal cases because the law and technical feasibility of many encryption workarounds is unsettled. Little empirical evidence about their use is available. The impact of encryption may be modest or great—or perhaps modest in some kinds of cases and great in others. Encryption adds a new step to many investigations. Whether it proves a game-changer or a speed bump remains unclear, and it will depend on both technological change and the resolution of many legal questions that currently remain unanswered.