ENCRYPTION WORKAROUNDS

Orin S. Kerr* & Bruce Schneier**

Abstract

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 an unencrypted version of a target's data that has been concealed by encryption. This essay provides an overview of encryption workarounds. It begins with 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. For each approach, we consider the practical, technological, and legal hurdles raised by its use.

The remainder of the essay develops lessons about encryption workarounds and the broader public debate about the role of 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 by only a few. Third, the scope of legal authority to compel third-party assistance will be a continuing difficult 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 many legal questions that currently remain unanswered.

---

* Fred C. Stevenson Research Professor, George Washington University Law School.

** Lecturer and Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School. Fellow, Berkman-Klein Center for Internet and Society, Harvard University. Special advisor to IBM Security and CTO, IBM Resilient.

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 poses 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 information known as ciphertext, which is useless unless the ciphertext can be decrypted into the unencrypted 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 paper, we will call such efforts "encryption workarounds." We use the term broadly to refer to any effort to reveal an unencrypted version of a target's data that has been concealed by encryption. Encryption workarounds as a lawful government investigative technique are not conceptually new. In 1807, during the treason trial of Aaron Burr, the prosecution attempted to decipher Burr's encrypted messages by

---

[1] According to a 2015 study, 68% of adults in the United States own a smartphone. See Monica Anderson, *Technology Device Ownership: 2015*, Pew Research Center, available at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/. That percentage is up from 35% in 2011, *see id*., suggesting that the percentage today may be substantially higher than 68%.

[2] *See End-to-End Encryption*, available at https://www.whatsapp.com/faq/en/general/28030015.

[3] *See generally* Sang Ah Kim, *HTTPS: Staying Protected On the Internet*, 1 GEO. L. TECH. REV. 119 (2016)

[4] *See generally* BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD Ch. 6 (2009).

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

forcing Burr's 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 for the first time. Even just twenty years ago, encryption was typically cumbersome and its use 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 focused law enforcement attention on how to bypass encryption that criminal suspects use.

This essay 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, which we label as follows: 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.[8] 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 it implicates. None of the methods is unique to law enforcement. Anyone, criminals and law enforcement alike, can employ any of 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 the law should be that governs 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 essay develops lessons about encryption workarounds and the broader public debate about the role of encryption in government investigations.[9] First, encryption workarounds are inherently

---

[6] *United States v. Burr*, 25 F. Cas. 38 (C.C. Va. 1807) (Marshall, C.J.).

[7] *See* SIMON SINGH, THE CODE BOOK 32–44 (1999).

[8] *See* Part II, *infra*.

[9] *See* Part III, *infra*.

probabilistic. None works 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 by only a few. Third, the scope of legal authority to compel third-party assistance will be a continuing difficult 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. FBI Director James Comey has expressed fears that the government is "going dark" because encryption blocks access to communications.[10] Critics have argued that these fears are overblown.[11] Which side is right depends in part on the success of workarounds. The law and technological feasibility of many workarounds is unsettled, however, and empirical evidence about their use is largely unknown.

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. But the effect of encryption may prove less dramatic than the government fears or civil liberties activists hope.

The essay contains three parts. Part I introduces the basic technology of encryption. Part II surveys the six kinds of encryption

---

[10] See James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Remarks at the Brookings Institution, Washington, D.C. October 16, 2014, available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[11] *See, e.g.*, Berkman Center for Internet and Society, *Don't Panic: Making Progress on the "Going Dark" Debate* (2016), available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going _Dark_Debate.pdf.

workarounds. Part III suggests lessons for policymakers drawn from the workarounds.

I. INTRODUCTION TO ENCRYPTION

Cryptography—the science of encryption—is as old as writing itself, and its basic principles date back thousands of years. 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 very simple. For example, the algorithm might merely be to change each letter in the alphabet one letter so that *A* becomes *B*, *B* becomes *C*, *C* becomes *D*, and the like. 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 are much more complex and mathematical. Modern encryption algorithms follow Kerckhoff's Principle, first stated by the Dutch cryptographer Auguste Kerckhoff 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. But because every user of BitLocker has his own key, no one can unlock and decrypt a computer belonging to someone else. 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 computer data can be encrypted: 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. For example,

---

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

[13] *See id*.

a 128-bit key might be 01000110011110001101111110001110101000100101011100100101011100001111011010001110011111100010111010010111011001000011010110100011100. Generally, this will be expressed in hexadecimal notation, where every eight bits make up a single two-character "byte": 4678df8ea25c95c3da39f8ba5d90d68c. A 256-bit key would look similar, but twice as long.

Encryption algorithms are designed such that there should be no faster way to break them then to try every possible key. This is known as a "brute-force attack."[14] To thwart a brute-force attack, the key must be long enough to make such an attack impossible. Fortunately, this is easy. 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 twice as long as the previous number. In the arms race between encryption and brute force attacks, the mathematics overwhelmingly favors encryption. Very generally speaking, 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 the algorithm.

Today, 64-bit keys can be brute-forced with a reasonable amount of computing power, and 80-bit keys can be brute-forced by large national-intelligence agencies.[15] But 128-bit keys are beyond the reach of any current or near-future technologies, and 256-bit keys are beyond the reach of any foreseeable computer technologies, including still-theoretical quantum computers. The latter two key lengths are the ones most commonly used today. Brute-force attacks on a typical-length key are effectively impossible.

While some encryption applications accept random hexadecimal 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, for example, the computers that have the messaging system software encrypt and decrypt the messages using keys that the computers themselves generate

14

15

and use.[16] 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 will refer to collectively as passwords).[17] Although it is essentially impossible 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 often allowing access based on a shorter password instead of the full key. They key itself is encrypted, and the encryption for the key is unlocked with the password. Behind the scenes, the process of decryption is broken into two parts: one algorithm pairs with the password to decrypt the key, then 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 but functionally act as encryption keys. Consider the 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 unlock the phone. The two-stage process is invisible to the casual user. 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 in the foreseeable future, every encryption system will have weaknesses. The algorithm must be written in software and run on a computer. The key must be entered into the system somehow. 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.[18] Weaknesses in

---

[16] *See End-to-End Encryption*, available at https://www.whatsapp.com/faq/en/general/28030015.

[17] 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.

[18] Users choose and remember short and non-random passwords. In cryptography, the strength of a password or key is known as "entropy." A random binary string has the maximum possible entropy for its length. Anything shorter or less

encryption systems are common, and they will play a big part in the encryption workarounds described below.

It is important to understand that encryption and encryption workarounds are "dual use" technologies. 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 occurs, as well. The government often uses encryption to maintain the privacy of valuable government data, and criminals or terrorists often use workarounds to defeat it.

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 legal compulsion, that make them unique to law enforcement, the United States government, or governments as a whole. Anyone can use encryption, and anyone with sufficient technical expertise and financial resources can use encryption workarounds.

II. Six Types of Encryption Workarounds

This section 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 then using the key to decrypt the data. The key-based methods differ based on whether the key is found in a place (find the key), obtained from a person (compel the key), or guessed (guess the key). The latter three methods work without the key. They differ primarily based on how the government bypasses the encryption to obtain an unencrypted copy of the information.

---

random—a dictionary word, for example—has less entropy. In general, passwords have much less entropy than the underlying keys they protect.

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 have the option of storing passwords and keys, and a user might use that option to store a copy there. 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.[19]

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 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 the computers to locate them. Keys can themselves be encrypted, such that a second key is needed to decrypt the key needed to decrypt the original messages. 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 the average person has with a single master key. The master key must be used to decrypt the file of 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*,[20] the government knew that the suspect had encrypted a file on his home computer but lacked the password to decrypt it. Agents obtained a warrant, secretly entered into

[19] This step would combine "find the key" with a second workaround, "exploit a flaw in the encryption scheme," discussed below. See notes [] to [], supra.

[20] 180 F. Supp.2d 572 (D.N.J. 2001).

his home, and installed a keylogger on his computer. When the suspect alter used his computer and entered in his password to decrypt the file, the keylogger intercepted the password. Agents later retrieved the keylogger and used the password to decrypt the file.[21] The federal court then had to determine whether installing and using the keylogger was permitted using a traditional search warrant or whether it required a wiretap order under the Federal Wiretap Act.[22] The court ruled that the traditional search warrant was sufficient because of the technical details of how the keylogger was installed.[23]

B) Guess the Key

A second approach is to guess the key. Although random encryption keys are sufficiently long as to make this effectively impossible, the more easily memorizable and typable passwords, passcodes, and passphrases that often protect the keys are generally much shorter. A passcode or password can be relatively easy to guess. And since the password unlocks the encryption key, which in turn decrypts the encrypted volume, such as a hard drive, 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. While the most secure systems allow for an arbitrary length string including any typable characters, many systems have limitations that limit the set of possible keys.

Other factors that affect whether a key can be guessed 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 likely number of guesses. In the simplest case, agents may guess the key

---

[21] *See 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," *New York Times*, Aug. 6, 2001, available at http://www.nytimes.com/2001/08/06/business/compressed-data-password-protection-with-prison-stripes.html

[22] 180 F.Supp.2d at [].

[23] *See id*.

successfully by making educated guesses about what passwords the owner is likely to have used. Passwords generally need to be remembered by their users, which means they are often memorable numbers or phrases.

Consider the recent case of *United States v. Lopez*.[24] The defendant Lopez was arrested at the U.S. border when agents discovered cocaine in her car. Agents also seized the defendant's locked iPhone and iPad tablet. During questioning, the agents asked Lopez her date of birth. After she shared that information with the agents, agents successfully unlocked the iPhone and iPad by correctly guessing that Lopez used her birthday as the code needed to unlock both devices.[25] 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 4-digit code, 6-digit code, or something else. The entry may have been simply been a good first guess: Everyone has memorized their birthdates, and agents may try that intuitive sequence as a likely passcode.[26]

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 15% of the passcodes consisted of only 10 combinations out of the 10,000 possibilities.[27] The most popular passcode was 1-2-3-4, which was used about 4% percent of the time.[28] On computers, the most common passwords are "123456," "qwerty," and "password."[29]

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. Modern computers can try millions of password per second. 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

---

[24] 2016 WL 7370030 (S.D. Cal. 2016).

[25] Id. at *1.

[26] Acccording to a prosecutor who contacted one of the authors, a birthdate is a common law enforcement guess.

[27] http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes

[28] See id.

[29] https://13639-presscdn-0-80-pagely.netdna-ssl.com/wp-content/uploads/2016/01/TeamsID-IG- Worst-Password-V3.pdf

less that are entirely lowercase letters, and so on.[30] And while there are techniques for creating passwords that are both secure and easily remembered, relatively few people use them.[31]

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 remove the encrypted file from the suspect's computer and bring it to a forensic laboratory. This allows the guesser to use parallel-processing systems optimized to guess passwords as quickly as the processing speed permits.

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, requiring up to 10,000 combinations, is almost instantaneous on an offline computer. But the iPhone's processor is comparatively slow. It would take an iPhone 22 hours to run through the 10,000 possible keys under its default four-digit configuration.[32] If a user expands a passcode to 13 digits, it would take only minutes to guess offline but about 25,000 years to run through every possibility on the iPhone itself.[33]

Technical means can be used to slow down or thwart guessing. The current iPhone operating system combines these features with the "Erase

---

[30] A 2013 article tested four password-cracking experts against a list of 16,000 encrypted passwords. The winner successfully guessed 90% of them in 20 hours using a single computer and a commonly available add-on card. Passcodes used 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."

This gives some flavor of how effective password guessing is. Some criminal organizations have much more powerful capabilities to guess passwords than these 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.

[31] https://www.theguardian.com/technology/2008/nov/13/internet-passwords

[32] https://theintercept.com/2016/02/18/passcodes-that-can-defeat-fbi-ios-backdoor/

[33] See id.

Data" feature.[34] The feature is not enabled by default. When 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 wrong entry #6, to fifteen minutes each for entries #7 and #8, to an hour for entry #9. After the tenth wrong entry, the phone's data is permanently erased and cannot be accessed at all.[35] 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 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. Depending on the person's relationship with the law and the law in general, coercion could include threats, bribery, seduction, torture, and so on. The phrase cryptographers use for this attack is "rubber-hose cryptanalysis."[36] In this essay, 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 the key that is provided so long as the Fourth Amendment is otherwise satisfied.[37] The more significant case is where the person refuses to disclose the key voluntarily. The

---

[34] http://ioshacker.com/how-to/enable-erase-data-option-delete-data-10-failed-passcode-attempts

[35] http://abc13.com/news/how-apples-security-features-have-locked-investigators-out/1203960/

[36] This is humorously portrayed in the popular webcomic xkcd. https://xkcd.com/538/

[37] Similarly, it seems likely that he evidence on the decrypted device would nonetheless be admissible if the password were obtained in violation of *Miranda v. Arizona*. See generally https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/12/12/when-miranda-violations-lead-to-passwords/.

Searching a device will often be a Fourth Amendment search that requires a warrant. If the person who has common authority over 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. On the other hand, the government may 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.

government may be able to order the computer's owner to enter in the password or to disclose the password to the government. In the case of storage devices where the key is protected by a biometric access mechanism, such as a fingerprint reader, the government could order the owner to unlock the device using the biometric access.

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 could compel it from her even if she was not a regular user of the data the key can unlock.[38] 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 out of reach.[39]

The second problem is that the available person who knows or controls the key may not wish to disclose it, which raises the legal question of how much pressure the government can exert to encourage disclosure. This depends largely on the limits of the Fourth Amendment and Fifth Amendment. 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 Fourth Amendment limits on compelling the key are fairly modest, in part because of the limited or nonexistent Fourth Amendment limits on governmental compelling of testimony and documents.[40] On the

---

[38]

[39] The San Bernardino terrorism case is an example: The user of the phone was dead before the government wished to unlock the phone. *See generally* notes [] to [], *infra*.

[40] See *United States v. Dionisio*, 410 U.S. 1 (1973) (no Fourth Amendment limits on forcing a person to testify before the grand jury); *United States v. Horowitz*, 482

other hand, significant Fourth Amendment issues may arise when biometric authentication can be used to decrypt data. Typically, the suspect will be "seized" in order to have his fingerprints placed on a fingerprint reader until either one opens up access or additional fingerprint reads are no longer permitted. The open legal question is what level of cause and what court order the government might need to compel the act.

Courts have generally held that reasonable suspicion that a particular person committed a crime is sufficient to compel a suspect to provide a fingerprint that can show a match with known evidence. It is possible that courts will similarly require reasonable suspicion of criminality to order a suspect to place fingers on a fingerprint reader to unlock a phone. This is possible but not obvious. When investigators seek a fingerprint to unlock a phone, ordinarily they are not interested in proving a fingerprint match. Instead, they want to unlock the phone to enable searching its contents, which itself will ordinarily require a search warrant. This might conceivably alter the Fourth Amendment standard, as 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.[41] For example, the required type of cause might be reason to think that the person controls a phone rather than cause that the owner committed a crime.[42] The precise standard currently remains unknown.

The more significant legal hurdle to compelling acts that decrypt devices is the Fifth Amendment right against self-incrimination.[43] The Fifth Amendment ordinarily does not impose limits on forcing a person to use a biometric means of access.[44] Because biometric access ordinarily

---

F.2d 72 (2d Cir. 1973) (only fourth Amendment limits on compelling documents are reasonableness, which looks to the burden of complying with the disclosure).

[41] 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.

[42]

[43]

[44] This is the case because placing a body part on a scanner does not imply any testimony required under the Fifth Amendment. However, such access may be testimonial if government tells the person to decrypt the device and leaves up to them to select the specific body part that the biometric reader recognizes. *See generally* Orin Kerr, *The Fifth Amendment and Touch ID*, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id/.

does not require testimony, the government can force a phone's owner to press their finger onto a fingerprint reader without triggering the Fifth Amendment.[45] The government also can compel a person to speak a known password, as voice examplars are not testimonial under the Fifth Amendment.[46]

On the other hand, a person who is forced by threat of law to enter in an unknown password is being compelled to testify.[47] Successfully entering in the passcode implicitly testifies that the person knows the passcode: Without that knowledge, the act of unlocking the device could not have occurred. Knowing the password to the device may be incriminating: it may provide a "link in the chain" that can help to show awareness of the contents of the device and involvement in its creation or possession.[48] As a result, being compelled to decrypt an encrypted device raises potential Fifth Amendment issues. If the government seeks to have the person disclose the password to the government, rather than merely use it, the password itself might also be independently incriminating.

If an individual asserts his Fifth Amendment rights not to comply with such an order, a court must determine if the government can legally compel the act of decryption.[49] The answer hinges largely on fact-specific applications of the "foregone conclusion" doctrine.[50] The foregone conclusion doctrine teaches that if the testimonial aspect of production is already known to the government, and is not to be proven by the testimonial act, then the testimony is a foregone conclusion and the Fifth Amendment privilege does not apply.[51]

How the "foregone conclusion" doctrine applies to compelled decryption is presently uncertain. The open question is what facts must be established as known by the government to make the testimony implicit in decryption a foregone conclusion. On one view, the government must establish that it already knows the specific files expected to be found on

---

[45] *See* State v. Diamond, ___ N.W.2d __, 2017 WL 163710 (Minn. Ct. App. 2017).

[46] United States v. Dionisio, 410 U.S. 1 (1973).

[47]

[48]

[49] *Salinas v. Texas*.

[50] See *Fisher v. United States*.

[51] *Fisher v. United States*; Hubbell.

the decrypted device.[52] From this perspective, decrypting the device amounts to testimony about their 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.[53] On another view, the government must only establish that it knows that the person knows the password. From this perspective, decrypting the device only amounts to testimony that the person knows the password. This standard would be vastly easier for the government to meet in practice, as evidence that the person uses the phone regularly is likely sufficient to establish that the person knows the password.[54] Which standard is correct is not yet clear in the case law.[55]

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, physically placing his finger on the reader. But the government has no way to actually force a suspect to disclose a key or decrypt a device even if a court rules no Fifth Amendment privilege applies. The government must instead rely on the possibility that the punishment of noncompliance, including jail time for contempt or failure to follow an officer's unlawful order, appears greater than the possible punishment that might follow from decryption and government access to plaintext. If the evidence on the device is particularly damning, a rational suspect may decide to suffer the punishment for noncompliance rather than suffer the greater punishment of the underlying crime.

Enforcing compliance with orders to decrypt typically requires legal proceedings for contempt (if a court order is obtained)[56] or failure to

---

[52] In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

[53] *See id*. at [].

[54] State v. Stahl, Case No 2D14-4283 (Fl. Ct. App. 2D 2016), available at https://consumermediallc.files.wordpress.com/2016/12/iphonepasscode.pdf.

[55] For a detailed look at the arguments, see Orin Kerr, *The Fifth Amendment limits on forced decryption and applying the 'foregone conclusion' doctrine*, The Volokh Conspiracy, June 7, 2016, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/.

[56] See, e.g., Fed. R. Crim Pro. 41.

follow an officer's lawful order (if no such order is obtained). The government must show that the defendant is willfully refusing to comply with a lawful order, either by outright refusal or by falsely claiming to be unable to comply.[57] 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 determine accurately if the defendant is unable to comply. A defendant may truthfully claim to have forgotten the password or to never have 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—means of obtaining and then using the designated key. 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 breaking a window instead of picking the lock. Access is gained without requiring 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 and on a computer. The weakness could be the result of new advances in the science of cryptanalysis, or a mistake made by a system designer or programmer. The flaw could also be deliberately inserted.

Flaws are not uncommon. All software contains bugs, and commercial software can contain thousands. Some of these bugs result in

[57] In re Weiss, 703 F.2d 653, 662–663 (2d Cir. 1983).

security vulnerabilities, and some of those vulnerabilities can be exploited to defeat the encryption scheme. Hackers, criminals, foreign governments, and others all take advantage of these flaws in encryption systems. Additionally, some flaws are deliberately inserted, either by the software vendors themselves or by individuals wanting to subvert the security of the software.[58] These are commonly called "backdoors." In both the 1990s and over the past few years, the FBI has endorsed a requirement that vendors create these backdoors for their agents to use.[59]

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. When exploits become known, companies and software writers will try to quickly correct the flaw. Exploiting a flaw therefore often requires knowledge of a flaw that is not otherwise widely known or has not yet been corrected for that particular device.

A dramatic example of such a flaw was discovered by security researcher John Gordon about the Android smartphone operating system called "Lollipop" released in 2015.[60] Gordon discovered that a phone running that operating system would unlock after several minutes if a user entered any extremely long string of characters—roughly 50 pages of text -— at the password prompt.[61] The exceedingly long data entry overwhelmed the phone, causing it to crash and bypass the lock. Gordon notified Google of the flaw, and Google then created and distributed a patch to correct the error.[62]

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. Farook's phone was known to have used 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. Apple objected to the assistance order, and the FBI was able to gain access to the phone a

---

[58] https://www.schneier.com/essays/archives/2013/10/how_to_design_and_de.html.

[59] https://na-production.s3.amazonaws.com/documents/Doomed_To_Repeat_History.pdf

[60] http://money.cnn.com/2015/09/16/technology/android-hack/index.html

[61] See id.

[62] See id.

different way. Although details remain murky, it appears that a private company had found an exploit that disabled the auto-erase function.[63] The FBI reportedly paid the company $1M for the use of the exploit, allowing the FBI to access the phone by guessing the passcodes. This approach relied on two workarounds in tandem: First, exploit the flaw; second, guess the key.

E) Access Plaintext When the Device Is In Use

The fifth type of encryption workaround is to access plaintext when the device is in use. Data must be decrypted to be read by intended users. Encrypted data must be available in unencrypted form where intended users access it. This necessarily creates a security vulnerability: the government may work around the encryption by gaining access to the information when it is in decrypted form for the user. This technique is limited in scope because it usually works only in real time" For the most part, the information it seeks will be available only when the government has ongoing real-time access to the device where the information rests at the moment it is available in plaintext.

Consider an encrypted text message that is end-to-end encrypted from the sender's device to the recipient's device. Although the message will be encrypted from device to device, it will be readable in unencrypted form both on sender's keyboard and on the recipient's screen. Access to either device, perhaps from a hidden camera or an investigator surreptitiously looking over the suspect's shoulder, will enable access to an unencrypted copy of the information.

The same dynamic can exist when investigators target a suspect's encrypted hard drive. That hard drive might be encrypted when the computer is turned off, so that turning on the computer requires a key to decrypt it. When the computer is turned on and being used, however, the encryption key is available and constantly being used to access the hard drive. Someone who has control of the computer can access the hard drive and view the decrypted information. An investigator could insert a keylogger into a computer to collect keystrokes or install a hidden camera

[63] 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

in the room where the computer is that can record both what the suspect is typing and what he is reading.

The technological sophistication required to access plaintext when the device is in use varies widely. In some cases, it is as simple as physically grabbing the device from the suspect. In the investigation into the Silk Road website, for example, the FBI carefully planned the arrest of suspect Ross Ulbricht to bypass the whole-disk encryption on his laptop.[64] Ulbricht was known to be using his laptop at a public library. The laptop was encrypted when shut down, but decrypted when in use. To capitalize on this, the FBI sent two plainclothes agents into the library posing as a couple. While standing next to Ulbricht, the two agents began a loud fight.[65] The fight distracted Ulbricht, allowing one of the agents to grab the laptop while it was open.[66] That agent turned it over to a third officer who immediately began to search the device while Ulbricht was placed under arrest. The ruse enabled the FBI to bypass Ulbricht's whole-disk encryption by taking it from his hands.

If investigators cannot gain physical control of a device, accessing it 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.[67] This is much more complicated than physically seizing the machine. First, hacking will require the government to have figured out a technical means to gain 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. Playpen was a child pornography website available only using Tor. The government took over the website in an effort to trace back the identities of the site's visitors. Because Tor masked the true IP addresses of its

---

[64] See Natasha Bertrand, "The FBI staged a lovers' fight to catch the kingpin of the web's biggest illegal drug marketplace," *Business Insider*, January 22, 2015, available at http://www.businessinsider.com/the-arrest-of-silk-road-mastermind-ross-ulbricht-2015-1

[65] See id.

[66] See id.

[67] Landau's "lawful hacking" paper: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip

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 and visit Playpen. To reveal the true IP addresses of users, the government obtained a warrant authorizing the installation of a "network investigative technique"—in other words, malware—on the computers of Playpen visitors.

The NIT was a workaround response 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 identity information about the user's machine, including its real IP address. It would then send that information to the government. After the warrant was signed, the Playpen NIT was successfully placed on over 1,000 machines around the world. The information revealed by the NIT led to the arrest and prosecution of over 200 defendants in the United States.[68]

This complex technical means of access to data raises many legal questions that are currently before the federal courts in challenges to the Playpen investigation. The legal questions include: Was accessing the suspect's machines to obtain their IP addresses a Fourth Amendment search? Did accessing computers that ended up being located outside the district where the warrant was obtained violate the territoriality rules of the search warrant statute? Did the single warrant used to commit hundreds or thousands of searches satisfy the Fourth Amendment's probable cause and particularity requirements? Finally, does the government need to disclose to the defense how the NIT worked? 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 investigations, requiring a complex technical workaround with novel legal implications to obtain the same information.

F) Locate a Plaintext Copy

The sixth and final kind of encryption workaround is to obtain a separate and unencrypted copy of the information. The target may have

---

[68] https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/?utm_term=.4ab79b62d717

multiple copies of the sought-after records, and the government may be able to access an unencrypted version. Unlike the workarounds discussed above, this approach does not involve decryption of a known encrypted file or device. Instead, it instead looks for another copy of the sought-after information.

This strategy may be used as a second-best alternative 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 had automatically created.[69] 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 prominent example. The government attempted to decrypt the iPhone used by suspect Syed Farook pursuant to a search warrant served on Apple.[70] When that proved initially unsuccessful, the government obtained what was available from an iCloud backup copy. The cloud-stored copy was somewhat out of date because the phone had last been backed up six weeks before the shooting.[71] Nonetheless, the backup gave the government access to at least some the contents of Farook's phone without needing to decrypt it.

The success of locating another copy depends on three questions. First, does an additional unencrypted copy of the sought-after information exist? Second, is the government able to locate the unencrypted copy of the data? Third, is the unencrypted copy sufficiently similar to the encrypted copy to be an adequate substitute? The last question is often difficult to answer because investigators ordinarily will not know what has been encrypted. This means that investigators may not know if the additional copy of the data is accurate and complete.

---

[69] Cf. *Commonwealth v. Copenhefer*, 587 A.2d 1353 (Pa. 1991) (recovering draft copies of ransom note automatically saved by word processing software on suspect's computer)

[70] http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernardino-shooter-s-icloud-backup-likely-disabled-doj-says-n536171

[71] http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernardino-shooter-s-icloud-backup-likely-disabled-doj-says-n536171

III. Four Observations about Encryption Workarounds

With a taxonomy of encryption workarounds in place, we next offer insights that the taxonomy suggests about law enforcement responses to the widespread use of encryption. We identify four lessons.

The first lesson is that there is no 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; 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 practical matter, this likely means that state and local investigators will be forced to rely heavily on low-resource approaches such as compelling keys. The federal government, with its greater technical resources, is likely to choose from a wider range of workarounds. This may lead to the federal government taking over certain kinds of state and local investigations.

A 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.

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, the fact that a target has used encryption does not mean the investigation is over. It only means 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 likely 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 provide successful.

Proposals to mandate government access to a key do not alter this basic dynamic. In theory, key mandates sound as if they can work every time. But any legal regime that requires mandating access to a key can be circumvented, essentially providing a reverse encryption workaround against the encryption workaround. This means that mandates at most can regulate default uses of encryption products. Defaults are important, certainly: many or most users use products in the default way, even if changes are simple to make. But even at their hypothetical best, legislation can only facilitate particular workarounds. They cannot ensure their success.[72]

The fact that encryption will stymie some government investigations does not make encryption unique. FBI Director James Comey has said that encryption "takes us to a place—absolute privacy—

[72] For example, 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 [X years] to guess.

that we have never seen before."[73] 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 no one did. When the police interrogate a suspect, the suspect might confess or he might refuse to talk. When the police search a house for drugs, the drugs might be there or they could have been moved or destroyed. When the police investigate a conspiracy, a conspirator might flip and cooperate with the government or none might. 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 wish to obtain a confession, the law gives the police a set of tools they may use in an effort to persuade the suspect to confess. Some techniques are outlawed, such as excessive force or pressure.[74] And some techniques are regulated in detail, such as custodial interrogations regulated by the *Miranda* rules.[75] But within legal bounds, the police are free to try to persuade a suspect to confess by using various strategies for interrogations. None of the methods work every time. In some cases, no matter what the government does, suspects will confess. In other cases, no matter what the government does, suspects will assert their rights and refuse to say a word. The government must work with the inherently probabilistic nature of obtaining confessions.

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 government agency and others are likely to be used rarely and only by a few. As a practical matter,

---

[73] http://www.dailydot.com/layer8/encryption-privacy-security-fbi-director-james-comey-kenyon-conference/

[74] See voluntariness/due process cases.

[75] *Miranda v. Arizona*. See generally….

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, the least resources are required to compel the key. If a person is available who knows the key, the government needs only to assert legal pressure on that person to try to persuade them to disclose it. So long as the Fifth Amendment does not block the government's order, the government can exert that pressure and the suspect must make a choice whether to comply. The strategy of compelling the key makes encryption a relatively traditional question of contempt law: whether the pressure of jail time is too much for the subject of the order to refuse to comply. This approach certainly can raise complex practical questions, such as how best to know when the subject of an order genuinely cannot comply with a disclosure order. 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. 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.[76] Cyberweapons arms manufacturers like Hacking Team and Gamma International sell espionage systems to Third World countries for millions of dollars to circumvent encryption. Such expensive exploits are not likely to be broadly available within law enforcement.

The range of resources required for different workarounds is important because available resources vary considerably inside the government. Government resources in national security cases will generally exceed resources in criminal cases. 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.

---

[76] http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032

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 fairly modest resources. But other kinds of investigations are likely to need federal resources and expertise.

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.[77] 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 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.[78] Even today, any

[77] The limit to "criminal investigators" is important because the expertise may exist elsewhere inside government. In particular, intelligence agencies and particularly the NSA has 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. Details may have to be disclosed to the defense in a criminal case.

[78] Statute of Winchester of 1285, 13 Edw. I cc. 1 and 4. See also *Babington v. Yellow Taxi Corp.*, 250 N.Y. 14, 17, 164 N.E. 726, 727 (1928) (Cardozo, C.J.) ("Still, as

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.[79]

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 try to conduct the surveillance themselves.[80] For that reason, network surveillance laws generally include assistance provisions requiring providers to provide necessary assistance to effectuate surveillance pursuant to court orders.[81] 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.[82]

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

---

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"); In re Quarles and Butler, 158 U. S. 532, 158 U. S. 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")

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

[80] 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).

[81] Cite Wiretap Act and Pen Register assistance provisions.

[82] NY Telephone.

providing the most secure product possible, assistance with workarounds may appear less a nuisance than a threat.

This dynamic became clear in the recent litigation over whether Apple was legally required to assist efforts to decrypt the iPhone used by San Bernardino attacker Syed Farook. Farook was already dead, making the compel-the-key strategy unavailable. The government knew that Farook's phone had enabled the auto-erase feature to thwart guessing the passcode, complicating the guess-the-password strategy. The government had pursued the locate-another-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.[83] Apple objected to the order.[84] 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.[85]

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 our customers—including tens of millions of American citizens—from sophisticated hackers and cybercriminals." According to Apple, 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."[86] 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.[87]

---

[83]

[84]

[85] See earlier discussion.

[86] http://www.apple.com/customer-letter/

[87] The briefs are available at http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html. 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

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 an "unreasonable burden"[88] or be too obtrusive.[89] The difficult question is, how much assistance is too much?

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, 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 today, 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,[90] 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 and/or designers of software to weaken security practices and make an additional key available before the crime occurred. In effect, it is a meta-strategy designed regulate products directly

---

U.S. government surveillance following the 2013 disclosures by Edward Snowden has made distancing themselves from U.S. surveillance practices a business necessity.

[88] *New York Telephone*, 434 U.S. at 172.

[89] 18 U.S.C. 2518(4).

[90] *See generally* Hal Abelson, et al., The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption (1997), available at https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf

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 guarantee weaker security.

D. The Law of Encryption Workarounds Is Still Developing

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

Several examples have been covered in Section II. For example, 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. 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.

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 often will 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 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 yet 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.[91] 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 a net negative.

This paper 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. Empirical evidence about their use is largely unavailable. 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. But 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.

[91] See, e.g., Feinstein-Burr bill.