The Going Dark Problem and Forced Assistance

Scott Neugroschl[1]

"Everybody goes dark" – Cassie Steele[2]

1 INTRODUCTION

On December 6, 2019, a terrorist attack occurred at Naval Air Station Pensacola, which killed three people and injured eight others. Al-Qaeda claimed responsibility. The FBI wished to unlock the shooter's iPhone. If this sounds familiar, that is because it is. The fact set (with the exception of the al-Qaeda connection) is similar to the well-known San Bernardino shooting.

In both cases the FBI asked Apple for assistance in decrypting the shooter's iPhone. In both cases Apple refused to create a "backdoor" to unlock the phone to defeat the encryption. In both cases, the FBI successfully used third-party software to access the phones.

Even though the FBI was able to access the phones, it illustrates the issue, namely the concept of "going dark". In the law enforcement context, the term "going dark" refers to the use of encryption to conceal evidence from law enforcement. This includes both "data in motion", making it difficult – if not impossible – to intercept communications, such as phone calls, email, and live chat sessions; as well as "data at rest", referring to stored data, such as email, text messages, photos, and videos.[3] See section 3.4 below for a discussion of data at rest vs. data in motion.

The question arises, how should the government deal with data that has gone dark? Specifically, data that the government has legal access to via a warrant or other means, but is unable to access due to encryption. The lack of access is the crux of the going dark issue.

Various government agencies have argued in public fora[4] and in the courts that technology companies should assist them in providing such access, such as they did in the two above cases. They have even called upon Congress to restrict encryption for Americans by forcing the use of encryption that is compromised so that the FBI – and only the FBI (in theory) – can access it [5] Further, in possible violation of the Fifth Amendment, the courts have agreed with law enforcement that in certain cases, it is legal to compel someone to decrypt his own data; data which may contain incriminating information.

---

[1] MLS Candidate 2022, LMU Loyola Law School

[2] Cassie Steele, AZ Lyrics – Go Dark Lyrics, https://www.azlyrics.com/lyrics/cassiesteele/godark.html (last visited Dec 3, 2021).

[3] Comey, James B., Going dark: Are technology, privacy, and public safety on a collision course? (2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last visited Oct 11, 2021).

[4] Barr, William P., Attorney general William P. Barr delivers keynote address at the International Conference on Cyber Security, The United States Department of Justice (2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber (last visited Dec 7, 2021).

[5] C. Mitchell Shaw, FBI director calls on Congress to restrict encryption for Americans, The New American (2021), https://thenewamerican.com/fbi-director-calls-on-congress-to-restrict-encryption-for-americans/ (last visited Dec 7, 2021).

This paper shall argue that both of these positions are untenable in the real world, as it intrudes upon Americans' constitutional freedoms, and will not work under the laws of mathematics, as well. Specifically discussed will be the issues surrounding compelled decryption – both by the encryptor and by third parties, as regards the First Amendment right to free speech, and the Fifth Amendment right against self-incrimination. In addition, an explanation of encryption concepts is provided, which explains why mathematics prohibits an FBI-only universal decryption key. Further, this paper shall examine whether – if such a key were possible – such a requirement would be legal, again under the First Amendment, or even useful at all. Finally, a proposed path for law enforcement will be provided.

2 "GOING DARK"

In both the Pensacola and San Bernardino cases, the FBI was seeking legal, court-ordered access to the data stored on the devices (i.e., data at rest, see section 3.4 below).

Due to the nature of the iPhone (see 3.5 below), law enforcement was unable to access the contents of the device. The FBI requested Apple's assistance under the All Writs Act (28 U.S.C §1651). Apple refused and filed suit.

Both former FBI Director James Comey[6] and former Attorney General William Barr[7] have addressed this issue by calling upon technology companies to assist law enforcement. The most common interpretation of their requests is for encryption with a "master key". Privacy advocates have called this a request for a "back door". Comey denies this and calls it a front door, or alternatively requests key escrow. Key escrow is where a trusted third party (in Directory Comey's case, most likely the federal government) maintains a copy of an encryption key.[8] Another possible alternative is specialized decryption software, as the FBI requested Apple to provide in the San Bernardino case. All three of these raise practical and legal concerns, discussed in section 4 below.

Going Dark predates the use of computers for communications. Some of the Zodiac Killer's messages to the press and police were not deciphered until 51 years after the fact[9]. And yes, the Zodiac was never caught. However, we as a society need to decide whether we should – to paraphrase Sir William Blackstone[10] – sacrifice the rights of the many in order to catch the few. Do we force third parties to write decryption code? Should we force everyone to hand over their encryption keys?

---

[6] Comey, James B., *Supra*

[7] Barr, William P., *Supra*

[8] Techopedia, What is Key Escrow? - Definition from Techopedia Techopedia.com (2011), https://www.techopedia.com/definition/3997/key-escrow (last visited Dec 12, 2021).

[9] Kevin Fagan, Zodiac '340 Cipher' cracked by code experts 51 years after it was sent to the S.F. Chronicle San Francisco Chronicle (2021), https://www.sfchronicle.com/crime/article/Zodiac-340-cypher-cracked-by-code-expert-51-years-15794943.php (last visited Dec 12, 2021).

[10] 10 Guilty Men, Criminal Justice, http://mrsmucciolaw.weebly.com/criminal-justice-7-blog/10-guilty-men (last visited Dec 12, 2021). "It is better that Ten Guilty Persons Escape than One Innocent Suffer."

3 ENCRYPTION AND TECHNOLOGY

The issue in both these cases is that the data on the devices was encrypted. What does that mean? Encrypting data means that the data is scrambled, so that only those with a key to access it can read it. Anyone else will just find a jumble. The meaning of the term "key" is discussed in the next section.

Simply put, encryption is the process of transforming data so that only a person with certain knowledge can make use of it. Historical examples of encryption schemes familiar to the layman include the German Enigma device and the Navajo code talkers. In the case of Enigma, only those who knew the rotor settings for the day would be able to use it. For the code talkers, only people fluent in the Navajo language could understand the messages.

3.1 USES OF ENCRYPTION

In our interconnected modern world, we use encryption to protect our privacy and our personal information. For example, in the United States, we are free to read whatever we want. We use encryption in our Internet services to ensure the privacy of whatever people choose to read on the Internet, to protect our purchase history, or our library searches and records. We also use it to protect eavesdroppers from obtaining our passwords or our credit card information. Banks and other institutions use it to protect financial information from would-be thieves. In fact, it would not be an exaggeration to say that our modern economy depends upon encryption. In 2013, over 3.3 TRILLION dollars in purchases depended upon the security that encryption provides.[11] By 2020, that had grown to 4.28 trillion dollars in retail commerce, by over 2 billion people – a 21.8% share of total global retail sales.[12] And, even more, these numbers are purely retail, they do not include any business to business (B2B) transactions or funds transfers. Financial institutions made roughly 800,000 transfers per day via the Federal Reserve's Fedwire service in 2021 (through October), with an average daily total value of 3.8 trillion dollars.[13] Without the security that encryption provides, that amount of electronic financial activity would be impossible.

To be fair, Barr and Comey were not discussing encryption in the financial world; rather, they were discussing encryption as regards personal communications. There are two forms of encrypted communications: server-side encryption and end to end encryption (E2EE). With server-side encryption, there are no issues for law enforcement, as the server owner has the encryption keys[14] (see sections 3.2 and 3.3 below), and can provide access to the contents of encrypted message under the third-party doctrine, assuming the proper court order or warrants apply. Therefore, the use of server-side encryption does not contribute to the going dark problem.

---

[11] National Journal Kaveh Waddell, How much is encryption worth to the economy? The Atlantic (2015), https://www.theatlantic.com/politics/archive/2015/11/how-much-is-encryption-worth-to-the-economy/458466/ (last visited Dec 10, 2021).

[12] E-commerce worldwide, Statista (2021), https://www.statista.com/topics/871/online-shopping/#dossierKeyfigures (last visited Dec 11, 2021).

[13] Fedwire® Funds Service - Monthly Statistics, The Federal Reserve, https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html (last visited Dec 11, 2021).

[14] Jos Poortvliet, What is end-to-end encryption and why does it matter?, https://nextcloud.com/blog/what-is-end-to-end-encryption-and-why-does-it-matter/ (last visited Dec 14, 2021).

E2EE, on the other hand, takes into account users' concerns that a middleman may have access to their messages, including the fact that the middleman can provide the contents of their communications to law enforcement. In E2EE, the encryption is negotiated between the two endpoints of the communication, so that nobody else knows the encryption key, even if the message is stored on a server until the recipient retrieves it. This means that even if a law enforcement officer obtains a warrant for a message stored on the server, he cannot retrieve the contents of the communication. Once again, we have the scenario from Pensacola and San Bernardino. For law enforcement agencies, this is a nightmare scenario, and why they want some form of access. What happens if there is reason to believe that there is an imminent terrorist attack, and the particulars are protected by E2EE?

So why not mandate some kind of law enforcement access? E2EE is often used by journalists and human rights activists under repressive regimes, preventing the law enforcement of such regimes from arresting such people. What prevents an such a regime from using the law enforcement access to determine the identities of its critics? Even if such an access mechanism was created for the exclusive use of the US government, there is nothing to stop a foreign government from demanding law enforcement access as a condition of market access.

Let us assume that Congress mandates and the courts uphold some form of mandated law enforcement access. In this case, who maintains the mechanism for this access, and how do they keep it secure? Such a mechanism would instantly become the number one target of hackers all over the world, both state-sponsored and criminal. Furthermore, consider that even the NSA – one of the most secretive agencies in the world – was unable to prevent its secrets from leaking.[15] Should the mechanism be leaked or stolen, there would be no recourse, the genie would be out of the bottle.

We can see that any such mandate would be a two-edged sword, allowing law enforcement to access such E2EE, but at the cost of potentially endangering those under repressive foreign governments, as well as exposing US and foreign citizens to the potential of blackmail and theft.

3.2 TERMINOLOGY

Cryptography, the study of encryption, has its own terminology, just as with any other field of study. The following terms will be used:

a. Algorithm — The method used to encrypt or decrypt data. An algorithm may be as simple as "replace each letter with the third letter following in the alphabet"[16], or as complicated as the Advanced Encryption Standard (AES)[17]. The algorithm may be known to an attacker without violating security. The same algorithm may be used with different keys.

[15] Edward Snowden: Leaks that exposed US spy programme, BBC News (2014), https://www.bbc.com/news/world-us-canada-23123964 (last visited Dec 14, 2021).
[16] Also known as the "Caesar Cipher", as Julius Caesar is alleged to have used it.
[17] *FIPS 197, Advanced Encryption Standard (AES) - NIST*. (n.d.). Retrieved October 12, 2021, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

b. Attacker — A person not in possession of the key, who is attempting to decrypt the ciphertext. Note that an attacker may not be a criminal, but an authorized law enforcement agent.

c. Brute Force — An attempt to decrypt data by repeatedly guessing the key.

d. Ciphertext — The result of the encryption process. The encrypted data. The plaintext, key, and algorithm determine what the ciphertext will be.

e. Decryption — The process of unscrambling a ciphertext to a plaintext. The ciphertext, key, and algorithm determine what the decrypted plaintext will be.

f. Encryption — The process of scrambling a plaintext into a ciphertext. The plaintext, key, and algorithm determine what the encrypted ciphertext will be.

g. Key — A unique value that, in combination with the algorithm, will determine how the data will be encrypted or decrypted. The key is the only part of the encryption process (outside of the plaintext) that needs to be kept secret.

h. Plaintext — The original text that is to be encrypted.

3.3 A SIMPLE EXAMPLE

Given its importance, we must understand the basics of encryption before creating any attempt to regulate it. How, then, does encryption work? As stated earlier, the idea is that only a person with the encryption key – whether authorized or not – can decrypt the data. Without the key, the encrypted data will look like so much random junk.

Historically, before the 1970s, encryption was only used on alphanumeric data – that is, letters and numbers. With the advent of digital computers, encryption was extended to encompass digital data as well as text data.

For our example, we will look at a simple scheme for encrypting text only data. The concepts for digital data are similar, even if the implementation is more complex.

A simple example might be the “Cryptoquote” that can be found on the puzzle page of the daily newspaper. The letters are scrambled up (e.g., the puzzle writer might use the letter “Q” as a substitution for the letter “A” in the real quote), and unless you can determine the substitution pattern, all you can see is jumbled letters. As an example, one might try to solve the notional cryptoquote “NQZZP APDZI”.

It might be difficult to determine that the original message was “HELLO WORLD” without the information in Table 1:

Original Letter	Substituted Letter
D	I
E	Q
H	N
L	Z
O	P
R	D
W	A

Table 1 – A notional substitution scheme.

A more complete example would use a substitution table that would contain the entire alphabet on each side, and an original text that uses the entire alphabet (such as “the quick brown fox jumped over the lazy dogs”).

The act of creating the cryptoquote by following the substitution pattern is called “encryption”. The technical term for the original text is “plaintext”, and the technical term for the scrambled text (the cryptoquote) is “ciphertext”. The act of obtaining the original text from the ciphertext is called “decryption”. The substitution pattern is known as the “key”. Much as a physical key unlocks a lock, using the encryption key “unlocks” a ciphertext to plaintext.

When encrypting a plaintext, there is one more item necessary. This is known as the algorithm. The algorithm describes how to use the key and the plaintext to create the ciphertext. In the example given, the algorithm is “replace the original letter with the substituted letter from the table.” Similarly, the reverse algorithm allows us to recreate the plaintext from the ciphertext, using the algorithm “replace the substituted letter with the original letter from the table.”

This is clearly a highly simplified example, simply used to demonstrate the concept and introduce the terminology.

When dealing with digital data such as that stored on computer systems, the encryption algorithm and keys are much more complex than the simple substitution above. The current standard algorithm is known as the Advanced Encryption Standard (AES).

Regardless of the algorithm and key used, the important thing to know about encryption is that, properly implemented, given a specific algorithm, a specific plaintext, and a specific key, the ciphertext is unique. For example, in the contrived example above, if any substitution specified in the key changes, the ciphertext will be different. Similarly, if the key changes, one cannot obtain the original plaintext from the ciphertext – the result of decryption will be different. This means that unlike a physical lock and key, there is no such thing as a “master key”. For example, if the plaintext was “the quick brown fox jumped over the lazy dogs”, as above, and the substitution table (key) had every letter of the alphabet, and instead of substituting “E” for “Q” (as in Table 1 – A notional substitution scheme.Table 1, you had “N” for “Q” and “E” for “L”, you would have an incorrect decryption of the ciphertext. All portions of the key must be correct.

As mentioned above, current encryption standards are more complicated and have vastly more potential keys than the example above. Contrary to what Hollywood would have us believe, a brute force attack against an AES encrypted device would take trillions of times longer than the current age of

the universe.[18] Now, most encryption does not require the user to remember the full key (a sequence of 256 1s and 0s), but rather a passcode or passphrase. This reduces the time to brute force, but even assuming that a password contains just 20 upper or lower case letters, there are 52 raised to the power of 20 potential passwords to search. That is over 200,000,000,000,000,000,000,000,000,000,000 nonillion passwords. Even assuming that one could test a million passwords per second, that would still take over 600,000,000,000,000,000,000 – six hundred quadrillion – years[19]. Remember that the universe is roughly thirteen billion years old.

3.4 DATA AT REST VS. DATA IN MOTION

As mentioned above, there are two kinds of data to consider: data at rest and data in motion. While they might seem quite similar, they are handled differently. And yet, they can easily be transformed into each other. Let us consider Alice and Bob.[20] Alice has a picture on her iPhone. This is data at rest, as it is stored on her phone. She wishes to send it to Bob. She uses the "send" function on her phone to transmit the picture to Bob's phone. While the picture is in transit to Bob's phone, it is data in motion. Once Bob's phone receives the picture and stores it, it once again becomes data at rest.

Since data at rest and data in motion can be converted into each other, why are they considered differently?

First of all, data at rest may have different keys, depending upon where it is stored. Alice may not want Bob to have access to everything on her phone, so she sends him a plaintext copy of the photo, not her ciphertext of the photo. Once Bob receives it, he (or his phone, to be more precise) will encrypt it using his key for storage.

Let us assume that Alice and Bob do not want anyone else to see this picture (perhaps they are lovers, and it is a highly intimate picture), so they do not show it to other people. However, there is a time when it may be intercepted, namely while it is being transmitted from Alice's iPhone to Bob's phone. Unfortunately, Eve – who is Bob's ex-girlfriend – wants to snoop on his messages. How do they keep Eve from listening in and obtaining the picture? This is the problem of data in motion.

The solution is that Alice's iPhone and Bob's phone negotiate a transmission key, and the data is encrypted upon transmission. The actual details of such negotiation are irrelevant to the discussion. Now that the transmitted data is encrypted, Eve will only see ciphertext when she intercepts the transmission. However, Bob's phone, being in possession of the transmission key, can decrypt the transmission and store the picture. The important thing here is that the key is ephemeral, and once Alice sends the picture to Bob, the key is discarded. Further, since the key was negotiated between the phones without any intervention by Alice or Bob, neither of them knows the key, and they cannot reveal it, even under penalty of law. There are secure ways to negotiate the key, so that Eve cannot discover it.

---

[18] How long would it take to brute force AES-256?, ScramBox, https://scrambox.com/article/brute-force-aes/ (last visited Dec 12, 2021).

[19] The math is as follows: 52^{20} passwords/(365 days/year * 24 hours/day * 3,600 seconds/hour *1,000,000 passwords/second).

[20] Cryptographers (people who study encryption) often refer to Alice and Bob, who wish to hold a secure conversation. Should they wish to discuss a notional eavesdropper, said eavesdropper is referred to as Eve.

In the 1990s, the federal government was so concerned about the inability to wiretap digital communications that they proposed something called the Clipper Chip. The use of Clipper would be voluntary, and every Clipper chip had its own internal key, and the government would have its own escrowed copy of that key, along with information to identify which chip had that internal key. The clipper chip would encrypt communications using the ephemeral negotiated key as above, but would then encrypt the ephemeral key with its own internal key. It would then attach the encrypted ephemeral key and its own identification to the communication, allowing law enforcement to retrieve the ephemeral key and listen to the conversation, either in real time or after the fact. Needless to say, entities outside of the United States were not particularly thrilled with such a scheme, nor were most commercial businesses within the United States, along with civil liberties organizations. In the end, the only significant buyer of Clipper enabled devices was the U.S. Department of Justice.[21]

Note that data at rest cannot use an ephemeral key like data in motion – if it is ephemeral, when the user later tries to retrieve the data, he will not be able to access it, as he no longer possesses the key. The lack of access to the key leads us to the iPhone cases.

3.5 THE IPHONE AND ENCRYPTION

In the San Bernardino and Pensacola cases, the data in question is stored on the iPhone, so it is considered data at rest. The iPhone is designed to store the key in a secure part of the phone[22], and if and incorrect password is given ten times in a row, the key is wiped out.[23] Without the key, there is no way to decrypt the data stored on the iPhone. This is a deliberate design decision, to protect the phone. Without the password, an attacker – remember, an authorized person may be considered an "attacker" if he does not possess the encryption key – will not be able to access the iPhone's encryption key, and he will not be able to access any information stored on that device.

This is what the San Bernardino and Pensacola Apple suits were about. The FBI wished for Apple to create a custom version of iOS which would remove the ten failure limitation, allowing for the FBI to attempt to brute force the phones' passwords. Apple refused.

Let us assume that Apple did comply with the FBI's request, would not the excessive amount of time required to brute force AES or a long password make it useless? No, because the iPhone generally uses a 4 digit passcode (it is possible to use something longer or more complex by specifying an alphanumeric passcode[24], but most people do not do so), there are only 10,000 potential passcodes to search. Such a brute force attempt could be completed in a few days, even assuming it was performed by human beings, rather than a computer.

---

[21] Ira Flatow, Dorothy Denning, & Marc Rotenberg, From Clipper Chip to Smartphones: Unlocking the Encryption Debate Science Friday (2016), https://www.sciencefriday.com/segments/from-clipper-chip-to-smartphones-unlocking-the-encryption-debate/#segment-transcript (last visited Dec 12, 2021). Audio Transcript.

[22] Secure enclave, Apple Support (2021), https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web (last visited Dec 11, 2021).

[23] Avery Hartmans, There's a scary iPhone feature that erases all your data after too many password attempts - here's why you should turn it on anyway Business Insider (2018), https://www.businessinsider.com/iphone-security-failed-passcode-attempts-2018-6 (last visited Dec 11, 2021).

[24] Set a passcode on iPhone, Apple Support, https://support.apple.com/guide/iphone/set-a-passcode-iph14a867ae/15.0/ios/15.0 (last visited Dec 12, 2021).

4 LEGAL LANDSCAPE

Due to the built-in encryption on iPhone devices, and the limited number of attempts allowed to access the data before completely losing the encryption key, the FBI was stymied in its attempt to access this data. In the case of the San Bernardino shooter, the FBI invoked the All Writs Act to require Apple to provide assistance, and received a court order to do so.[25]

4.1 ALL WRITS ACT

The All Writs Act (AWA) states that

> "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law. (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction."

This allows the Court to order any party to render assistance in enforcing an order. The AWA is commonly used to force the government to comply with a previous order, with a writ of mandamus. It has been used, though, to compel private companies to assist the government.

In *U.S. v. New York Tel. Co.*[26], a court order had been issued requiring the phone company to assist law enforcement with setting up a pen register. The Supreme Court stated that the power conferred by the AWA "extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice".[27] The court further noted that that New York Telephone regularly employed such devices as part of the normal course of business, and that the order was in no way burdensome to New York Telephone. The court also took notice of congressional intent to allow the use of pen registers.

Apple was not in the business of thwarting the encryption it had developed for its own devices, and as a moderately large development effort, including design, coding, and testing, was burdensome to Apple. Further, as discussed below regarding the Communications Assistance for Law Enforcement Act (CALEA), Congress had decided not to pursue a law requesting such assistance when asked to do so by the Obama Administration, making it clear that there was no congressional intent here. In fact, in a concurrent case, *IN RE Order Requiring APPLE, INC. to Assist in the Execution of a Search Warrant Issued by this Court*[28], in the Eastern District of New York, decided the AWA's requirement that a writ be "agreeable to the usages and principles of law" was not fulfilled, because CALEA explicitly absolves a company of the responsibility to provide the assistance sought, and that CALEA is part of a legislative scheme that is so comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe.[29] Indeed, *Pennsylvania Bureau*

---

[25] *In the MATTER OF the SEARCH OF AN APPLE IPHONE SEIZED DURING the EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203*, 2016 WL 618401
[26] 434 U.S. 159 (1977)
[27] *Id.* at 174.
[28] 149 F.Supp.3d 341
[29] *Id.* at 354.

of Correction v. U.S. Marshals Service[30] explicitly states that where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act that is controlling.

Nevertheless, the FBI obtained a court order under the AWA to require Apple to assist in the decrypting of the iPhone in the San Bernardino case, requiring Apple to create a new version of the iPhone Operating System (iOS) that would disable certain security features. Apple declined to do so, leading to a court case. This case was rendered moot when the FBI decrypted the phone using third-party software.

In the resulting fallout, Apple received a large amount of criticism from the government, and in the press for refusing to assist the FBI. Though Apple declined to provide the requested tool, it did provide assistance to the FBI in the case[31]. In fact, the government's use of the AWA to compel Apple to write a customized iOS was due to the government's own errors in handling the evidence.[32] It is hard to believe that the Founders' intent when they wrote the AWA was to compel third parties to clean up after the government's mistakes.

Even though the case was rendered moot, there are still several issues to consider with this approach

Under CALEA[33], a company has no obligation to assist the government with decryption when it does not retain a copy of the key[34]. Congress had considered expanding CALEA to include data stored on phones, but chose not to[35]. This is clear evidence of legislative intent, so there were no "gaps" in the law for the AWA to fill[36]. Since Apple had no copy of the key, there was no statutory authority for the government to obtain a writ compelling assistance under the AWA.

Internet pioneer Phil Karn once said, "'National Security' is the root password to the Constitution".[37] Within the politically aware technology community, it has been adapted to "'X' is the root password to the Constitution.", where "X" is most commonly "terrorism", "child porn", or whatever the threat *du jour* is.. The term "root password" refers to the system administrator credentials, where the system administrator can do whatever he wants on the system. The implication is that the referenced crime is so horrible, the government can ignore constitutional safeguards. Whether or not the canard is true, using the AWA to force assistance in decryption raises constitutional issues, relating to the First and Fifth Amendments.

4.2 FIRST AMENDMENT ISSUES

4.2.1 Forced speech

[30] 474 U.S. 34 at 43
[31] *IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203*, 2016 WL 767457
[32] *Id*.
[33] 47 U.S.C. 1001-1010.
[34] 47 U.S.C. 1002(b)(3)
[35] 2016 WL 767457, *Supra.*
[36] Dmitri D. Portnoi, RESORTING TO EXTRAORDINARY WRITS: HOW THE ALL WRITS ACT RISES TO FILL THE GAPS IN THE RIGHTS OF ENEMY COMBATANTS, 83 NYULR 293 at 298.
[37] Phil Karn, "National security": the root password to the Constitution. Twitter (2013), https://twitter.com/ka9q/status/365961235809832960 (last visited Nov 17, 2021).

Can the government compel someone to speak, assuming that the Fifth Amendment right against self-incrimination is not involved? In particular, in dealing with going dark in general, and in the San Bernardino case specifically, can the government compel a third party to write software to enable decryption of a device? Note that in the case of an iPhone, the third party cannot decrypt the device directly, but can remove the restrictions on attempts to unlock the phone. To answer this, we must answer the following two questions. First, is software speech? And second, assuming that software is speech, can the government compel this speech?

Examining the first issue, it is appropriate to begin with *Junger v. Daley*,[38] a case from the early days of the Internet regarding encryption. Junger wished to publish encryption source code on his website, and was prohibited from doing so under the Export Administration Regulations 15 C.F.R. § 730-774. Junger filed suit against the government. The regulations were upheld at the district level, but Junger appealed to the Sixth Circuit. The Court struggled with this, as computer source code has both functional and expressive features.[39] In *Roth v. United States*[40], the Supreme Court noted that "All ideas having even the slightest redeeming social importance—unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion—have the full protection of the guaranties…" of the First Amendment. Using this as their guide, the Sixth Circuit noted that symbolic conduct, which also has functional and expressive features, has First Amendment protection.[41] The court also noted that computer source code, while perhaps unintelligible to the layman, is often the preferred method of communication among computer programmers. Following this chain of logic, the court ruled that computer source code is protected speech under the First Amendment.

In 2001, the Second Circuit took up the same question.[42] This was a case involving the Digital Millennium Copyright Act (DMCA) and the publishing of code to defeat the copy protection on DVDs. In this case, the court likened computer source code with musical notation, agreed with the arguments in *Junger v. Daley*, ruling that software is protected by the First Amendment.

Given these rulings that software is protected speech, we now consider the issue of compelled speech. Let us begin with *West Virginia State Board of Education v. Barnette*.[43] The Supreme Court ruled that requiring the recital of the Pledge of Allegiance consisted of compelled speech, and was as such, a violation of the First Amendment. *Wooley v. Maynard*[44] continued this ruling noting that "the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all."[45]

---

[38] Junger v. Daley, 209 F.3d 481 (2000)
[39] *Id.* at 484
[40] Roth v. United States, 354 U.S. 476, at 484
[41] United States v. O'Brien, 391 U.S. 367 (1968)
[42] Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2001)
[43] West Virginia State Board of Education v. Barnette 63 S.Ct. 1178 (1943)
[44] Wooley v. Maynard, 430 US 705 (1977)
[45] *Id.* at 714

Comprehensive Health of Planned Parenthood of Kansas and Mid-Missouri vs. Templeton et al, followed suit, noting that "just as the First Amendment may prevent the government from prohibiting speech, it may prevent the government from compelling expression of certain views".[46]

Granted, all three of these cases were discussing viewpoint-based compulsion, and the texts in *Barnette*[47] and *Planned Parenthood* were explicit about discussing restrictions or compulsions on viewpoint-based speech, the text in *Wooley* is more straightforward. The government may not compel speech – the First Amendment includes the right to refrain from speaking.

The Supreme court went even further in *Riley v. National Federation of the Blind of North Carolina, Inc.,*[48] stating 'There is certainly some difference between compelled speech and compelled silence, but in the context of protected speech, ***the difference is without constitutional significance***, for the First Amendment guarantees "freedom of speech," a term necessarily comprising the decision of both what to say and what not to say' (emphasis by the author, not the Court). The Court is explicit here. The government may not compel speech.

From this, we may conclude that forcing a person or persons to write decryption software or code to defeat password lockouts (hereafter referred to as encryption defeating software; the author's term, not a common term) is a violation of the First Amendment rights of those persons, be they natural or corporate[49].

4.2.2 Chilling effect

Even if it were the case that the government could compel a company to provide encryption defeating software, it would be undesirable to do so. If companies offering E2EE or secure encryption find themselves in a position where their business model is in danger due to the government forcing then to design and provide decryption mechanisms, then there may be a chilling effect, causing such vendors to cease providing such products.

This causes harm to innocent third parties, such as consumers, due to the fewer available purchase options, as well as the reduction of personal security and privacy.

There is little existing jurisprudence on any chilling effect of compelled speech – most chilling effects cases deal with prohibited speech; and the precedents on compelled speech are mostly about forced political speech, as in *Barnette*. But given *Riley v. National Federation*, we may speculate that the courts would take a dim view of any chilling effects caused by compelled speech.

4.3 Fifth Amendment Issues

The Fifth Amendment states that "No person shall be … deprived of life, liberty, or property, without due process of law". Having determined that production of code is speech, does the government's attempt to compel a third party to write code violate that portion of the Fifth Amendment?

---

[46] Comprehensive Health of Planned Parenthood of Kansas and Mid-Missouri vs. Templeton et al 954 F.Supp.2d 1205 (2013) at 1216

[47] West Virginia State Board of Education v. Barnette, *Supra.* at 639.

[48] Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781 at 796

[49] Santa Clara County v. Southern Pac. R. Co., 118 U.S. 394 (1886)

For example, in San Bernardino, Apple had nothing to do with the crimes committed, other than the fact that the perpetrators had purchased their product. Yet the government attempted to compel Apple to provide encryption defeating software. Is that not a violation of their liberty under *Riley v. National Federation* to decide "what not to say"? The government claims it was under due process of law, as they obtained a court order to do so. Yet, except for the AWA, there is no legal standing for such compulsion. As discussed above, even under CALEA, there was no statutory authority for such a demand.

In addition, the order to compel was filed *ex parte*[50], and Apple had no chance to argue against this order prior to its issuance. Given the First Amendment issues with the order, this violates Apple's right to due process.

Let us also consider the case where the alleged perpetrator of a crime is in custody, and the government wishes to investigate the contents of his phone, under warrant. Can he then be compelled to unlock his phone?

In *State v. Diamond*[51], the Supreme Court of Minnesota ruled that requiring a defendant to unlock his phone with his fingerprint was nontestimonial and more akin to that of providing fingerprints upon arrest. However, such an act is also equivalent to forcing a defendant to provide documents, which is considered testimonial. This conflict is currently unresolved, but most courts have followed *Diamond*.

What if the suspect does not use his fingerprint to unlock his phone? In general, it is assumed that a password or passcode may not be forced, as it is not a physical characteristic, but is instead testimonial in nature, see *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*[52], *Commonwealth v. Baust*[53], *and Seo v. State*[54]. However, jurisdictions vary. In particular, in *State v. Andrews*[55], the Supreme Court of New Jersey ruled that a person could be forced to disclose his passcode, ruling that it was nontestimonial. Andrews appealed to the U.S. Supreme Court, but was denied certiorari. However, most courts still believe that such disclosure is testimonial, as such an act "demand[s]the use of the contents of the mind".[56] Because there are now conflicts in the courts, this is an area that should be followed as the established law may change.

4.4 OTHER LEGAL ISSUES

4.4.1 Digital Media Searches

Searches of computer storage devices (such as a phone), is not as straightforward as a search of a place. Due to the sheer volume of material stored on a computer storage device, there is a two-step process

[50] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 2016 WL 680288.
[51] 905 N.W.2d 870
[52] 670 F.3d 1335 (2012)
[53] 89 Va. Cir. 267 (2014)
[54] 109 N.E.3d 418 (2018)
[55] 243 N.J. 447
[56] Michael A Foster, Catch Me If You Scan: Constitutionality of Compelled Decryption Divides the Courts (2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10416 (last visited Dec 15, 2021).

for search warrant execution, wherein the computer storage device is first seized, and then searched[57]. The issue here is that once the search begins, everything on the device is searched, whether or not it appears to be responsive. Compare this to a traditional search and seizure. Consider the hypothetical case of an accountant who eschews the use of computers, and keeps all his records on paper. Execution of a search warrant for his business records will not look at the videotapes labelled "Vacation", even if those tapes contain child pornography, as such videotapes would not be responsive to the search for financial records. However, if his brother, who uses his computer for his accounting business is subject to a similar warrant, the child pornography found on his computer will certainly be used against him under the plain sight doctrine.

Given that most people now "keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate"[58], compelling a suspect to unlock his phone provides a huge intrusion into the life of the suspect, especially given how digital search and seizure is handled. Such an intrusion could even be equivalent of the general warrants[59] that are specifically prohibited under the Fourth Amendment.

4.4.2 Key Escrow and the Right to Privacy.

Also, regarding the possibility of key escrow, we need to consider the right to privacy.

In *Katz v. U.S.*[60], for example, the Supreme Court commented on how the Third Amendment protects a person's privacy from the government. In *Griswold v. Connecticut*,[61] the court observed that "the First Amendment has a penumbra where privacy is protected from governmental intrusion".[62] And, of course, *Roe v. Wade* finds the right to privacy through the First, Fourth, Fifth, Ninth, and Fourteenth Amendments.[63]

In the physical world, would it be acceptable for the government to require everyone to provide the keys to their house and the combinations to their safe to the FBI, just in case they later commit a crime? Any court would laugh at such a requirement and immediately strike it down as unconstitutional. Why should it then be acceptable for the government to propose the digital equivalent?

4.5 Other Considerations

The government claimed that the San Bernardino case was about "just this once" and "just this phone", but even at the time the case was filed, the government had multiple applications for similar orders in other courts.[64]

---

[57] FRCRP Rule 41
[58] Riley v. California 573 U.S. 373 at 395.
[59] IN the MATTER OF the SEARCH OF INFORMATION ASSOCIATED WITH the FACEBOOK ACCOUNT IDENTIFIED BY the USERNAME AARON.ALEXIS THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC. 21 F.Supp.3d 1 (2013)
[60] 389 U.S. 347 at 350, Footnote 5.
[61] 381 U.S. 479
[62] *Id.* at 483
[63] 410 U.S. 113 at 152
[64] 2016 WL 767457, *Supra.*

In addition, there is always what is commonly called "mission creep". Even assuming that the government assures such software would be used for terrorism related purposes only, there is nothing preventing the use of it for other purposes. The government has expanded the use of terrorism laws in other instances. Indeed, the ACLU found that between 2003 and 2005, the FBI issued 143,074 National Security Letters under the USA PATRIOT Act, which led to 53 reported criminal referrals to prosecutors. Of these 53 referrals, 17 were for money laundering, 17 were immigration related, and 19 were related to fraud. Not a single criminal referral was made regarding a terrorism related investigation. [65]

Similarly, the USA PATRIOT Act created "sneak and peek" warrants, where law enforcement may execute a search warrant without informing the occupant. This was also allegedly intended to be used in terrorism investigations. However, again out of 3,970 sneak and peek warrants issued in 2010, less than one percent were used for terrorism investigations. The vast majority (76%) were issued in drug investigations.[66]

Given the history of mission creep, it would be almost certain that this capability would be used for other phones, in other types of investigations.

5 HOW SHOULD LAW ADAPT?

People use encryption for a variety of reasons, including for financial security, to keep their private information private, and – yes, unfortunately – to confound law enforcement should they come under investigation. However, Blackstone's maxim should still apply, we should not punish the innocent multitude due to the actions of the criminal minority.

Any attempt to provide voluntary governmental access to private encrypted information, be it at rest or in motion is doomed to fail, as we saw in the 1990s with the Clipper chip.

Given that compelled decryption by a third party is most likely a First Amendment violation, how should law adapt?

5.1 SHOULD THE GOVERNMENT FORCE COMPANIES TO PROVIDE DECRYPTION CODE?

Should the government force companies to provide encryption defeating software? We have discussed the First and Fifth Amendment implications above, and it is most likely unconstitutional to do so, as it is compelled speech. Even if such compulsion is found to be constitutional (as we noted above, "National Security is the root password to the Constitution"), other issues remain; namely economic impact, security, and human rights.

If developers within the United States are compelled to provide encryption defeating software to the US government, such products will most likely suffer in the international marketplace. Remember the Clipper chip. Instead, foreign purchasers of smartphones and encryption products will purchase from companies not subject to such restrictions. As of 2021, Samsung – not Apple – is the largest smartphone

[65] *Surveillance under the Patriot Act. American Civil Liberties Union*. (n.d.). Retrieved October 11, 2021, from https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act.
[66] *Id.*

vendor.[67] Similarly, encryption expertise is not restricted to the United States. In fact, AES was developed by Belgian cryptographers[68], and implementations are freely available from multiple sites around the world.[69] There will definitely be an economic impact, though the size thereof is open to question.

Second, we must consider the security of such encryption defeating software. As mentioned above, the repository of such software would instantly become the target of every hacker in the world. Even the NSA, as previously noted, was unable to keep its secrets from leaking. What evidence does the US government have that this time it would be different? Given that the mantra in computer security is "it's not if you are hacked, but when",[70] and the fact that the FBI has been recently hacked,[71] the confidence level in the security of any repository can not be high.

Third, there are human rights considerations. If a vendor is compelled to provide encryption defeating software by the US government, what is to prevent another government, such as China, from requesting the same access? This kind of access could put dissidents in risk of life or limb,[72] as well as human rights activists. This also opens up US companies to the danger of industrial espionage by the Chinese government, as the Chinese government hacks the phones of visitors.[73]

5.2 PROPOSED SOLUTIONS

What is the government to do? There are several options, all bad from one point of view or the other.

First, there is the option of forcing companies and developers to assist with decryption. This appears to be non-viable based on constitutional analysis, as well as other practical reasons such as security, economic issues, and the widespread available of options outside of the reach of US law enforcement.

Second, the US government could, in theory, ban E2EE. Again, this is not a viable option. First of all, this would be prior restraint, which would be presumptively unconstitutional.[74] Even were this not the case, problems remain with such a ban. What is to be done with all the devices and programs currently supporting E2EE? It is not possible to force everyone within the US to upgrade their phones or software;

---

[67] Global Smartphone Market Share: By Quarter, Counterpoint Research (2021), https://www.counterpointresearch.com/global-smartphone-share/ (last visited Dec 17, 2021).
[68] AES, Encyclopædia Britannica, https://www.britannica.com/topic/AES (last visited Dec 14, 2021).
[69] For example, the Cryptlib toolkit is developed in New Zealand. Cryptlib Encryption Toolkit, https://www.cs.auckland.ac.nz/~pgut001/cryptlib/index.html (last visited Dec 17, 2021).
[70] Michael Paluska, Expert: Getting hacked a matter of when, not if WFTS (2016), https://www.abcactionnews.com/news/security-expert-getting-hacked-a-matter-of-when-not-if (last visited Dec 17, 2021).
[71] Rachel Pannett, FBI email system compromised by hackers who sent fake cyberattack alert The Washington Post (2021), https://www.washingtonpost.com/nation/2021/11/14/fbi-hack-email-cyberattack/ (last visited Dec 13, 2021).
[72] Paul Mozur & Nicole Perlroth, China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn The New York Times (2020), https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html (last visited Dec 13, 2021).
[73] Octavio Mares, Be careful if you visit China; the government hacks phones of tourists Information Security Newspaper | Hacking News (2019), https://www.securitynewspaper.com/2019/07/03/be-careful-if-you-visit-china-the-government-hacks-phones-of-tourists/ (last visited Dec 13, 2021).
[74] James Grimmelmann, Internet Law: Cases and Problems (2019), pg 119.

some may not be able to afford it, and some may choose not to do so. What happens if two people decide to write or implement their own E2EE from publicly available sources? Will mere possession of such software become a crime with strict liability? Using the way that the Digital Millennium Copyright Act regulates circumvention devices[75] as an analogy, the publication or sale of E2EE could conceivably criminalized. But such software is freely available in source form from foreign websites. In addition, the US government publishes descriptions of algorithms that could be used to implement E2EE.[76] Further, since criminals are not known for their adherence to laws, this ban would punish law abiding citizens, while having almost no effect upon criminals. Given all these issues, even if the Constitution were amended to allow it, such a course is almost certainly doomed to fail.

Third, the government could mandate key escrow, where some branch of the government would maintain a database of all device keys, much as in the Clipper chip fiasco. However, this would be a mandate, rather than a voluntary submission. Once again, we have the issue of security, ensuring that the database of keys is not hacked or stolen. The size of the database is not an issue, there are approximately 300 million smartphones in the US as of 2021.[77] Commercial databases can easily handle datasets that size. However, what prevents someone from purchasing a phone outside of the US, where a key escrow mandate is not in order? Just as with the Clipper chip, foreign entities would not desire to provide their information to US law enforcement. And even with a key database, there is nothing stopping anyone from using their own encryption to protect their secrets, as opposed to the intrinsic encryption on the devices; unless the US government decides to ban encryption. We have already discussed this possibility and it is a horrible option.

The final option is the status quo, bad though it may be for law enforcement. Government can continue to use metadata and other forms of surveillance to investigate crimes. Remember that it is difficult to get a wiretap[78], and that law enforcement often relies on pen registers instead. Using communications metadata is similar to using a pen register. Yes, having to do the investigation without having access to certain information is more difficult, but that is what law enforcement is being paid to do. And further, consider the opinion of former Vice Chairman of the Joint Chiefs of Staff, "But I think we would all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only is the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done."[79]

---

[75] 17 U.S.C 1201(a)(2)
[76] FIPS 197, *Supra.*
[77] Number of smartphone users in the U.S. 2025, Statista (2021), https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ (last visited Dec 14, 2021).
[78] 18 U.S.C 2511
[79] Harold Abelson et al., Keys under doormats: mandating insecurity by requiring government access to all data and communications, Journal of Cybersecurity 73 (2015), page 73.

6 CONCLUSION

Benjamin Franklin said, “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.”[80] Every time a new invention or restriction has risen, law enforcement has claimed it would be the figurative end of the world. The Miranda Rule means that you can’t force someone to talk in an interrogation? Criminals will go free! Can’t do random stop and frisk?[81] Criminals will terrorize New York City! Yet each time somehow law enforcement manages to adapt and do its job.

Remembering that hard cases make bad law, the best solution is, unfortunately for law enforcement, the status quo. Yes, that means that sometimes criminals may go free. Yes it makes investigation more difficult for law enforcement. Sure, law enforcement would think it was wonderful it they didn’t have to comply with those pesky constitutional restrictions, but in the long run, regardless of the short term, we are all a bit safer and more secure when our constitutional freedoms and rights are respected.

[80] Historical Review of Pennsylvania (1759)
[81] Floyd v. City of New York, 959 F.Supp.2d 540 (2013)