Smartphone Encryption: A Legal Framework for Law Enforcement to Survive the "Going Dark" Phenomenon

MICAH HILL-SMITH*

Law enforcement agencies have been sounding the alarm for decades about encryption that is causing communications to "go dark". Digital communications have moved from easily tapped phone lines to secure encrypted systems. Law enforcement's access to data stored on smartphones has emerged as a critical component of this issue. Legally valid searches of smartphones have been frustrated by both technical and legal barriers. This article considers the different methods for effecting smartphone search warrants — forced entry, compelling users and compelling manufacturers — focusing particularly on the United States. It concludes by recommending a robust legal framework to govern law enforcement's search of encrypted data on smartphones.

I INTRODUCTION

In iOS 11, Apple introduced a smartphone function that the media came to nickname the "cop button".[1] When an iOS 11 user presses the power button on their device five times, the function, among other things, temporarily disables Touch ID and Face ID (Apple's branded biometric authentication features) until the user enters their passcode. This feature has the effect of preventing United States law enforcement from compelling the device owner to give access to the device, even to execute a lawful search warrant.

This situation represents the exploitation of an oddity of United States constitutional law by one of the most valuable companies in the world. It speaks to a broader question: how can law enforcement validly execute search warrants in an increasingly encrypted world? Law enforcement's concerns about the "going dark" phenomenon are well documented,[2] and the answers to its criticism are not easy.

This article discusses the practical and legal barriers that stand in the way of law enforcement's execution of valid search warrants on smartphones. I argue that the solution is to continue to allow strong encryption but to

* BSc/LLB(Hons), University of Auckland. I would like to thank John Ip for his supervision and encouragement.

1 Tom Warren "iOS 11 has a 'cop button' to temporarily disable Touch ID" (17 August 2017) The Verge <www.theverge.com>.

2 Federal Bureau of Investigation "Going Dark" <www.fbi.gov>.

provide a legal framework that permits compelled decryption. I do not consider questions of when a search warrant should or should not be granted; such questions are a separate issue and the subject of a separate area of research. I argue that even if there are issues with the way warrants are granted, an imperfect legal test is preferable to taking the final decision away from the courts.

Forced entry without the support of the user or manufacturer has largely ceased to be a viable method for law enforcement to execute search warrants, and the number of instances where forced entry is possible will continue to decrease over time. A mandatory back door for law enforcement will also continue to be an impractical and undesirable option. This article concludes that the best way forward is a legal framework compelling users to provide the authentication information necessary to search devices. These rules should be coupled with significant criminal penalties for non-compliance.

This article takes a United States-centric approach and only briefly surveys other jurisdictions. As Apple[3] and Google[4] are both American companies, the United States legal and policy position has far greater extra-jurisdictional impact than any other country involved in this issue. Further, the United States has the greatest experience with issues surrounding smartphone encryption, albeit that its treatment of these issues has arguably been problematic under current law.

I begin by setting out the technical background. This involves a brief discussion of smartphone cryptography. I then consider the range of legal and technical issues involved in law enforcement's three main options for accessing smartphones: forced entry, compelling users and compelling manufacturers. I undertake this analysis having regard particularly to the current United States position. Following this is a survey of New Zealand's and the United Kingdom's position. I conclude by proposing a possible way forward: an ideal legal framework to govern law enforcement's search of encrypted data on smartphones.

II ENCRYPTION

Consumer technology has trended quickly towards encryption at all levels over the last 10 years. The first iPhone launched in 2007 without hardware encryption; users primarily sent unencrypted short message service (SMS)

3 Apple Inc is an incorporated publicly traded technology company in the United States that is at the time of publication the third most valuable company in the world. It makes the iPhone, which runs its proprietary iOS mobile operating system: Yahoo! Finance "Apple Inc (AAPL)" <www.finance.yahoo.com>; and Apple "iPhone" <www.apple.com>.

4 Google LLC is an incorporated publicly traded technology company in the United States that is at the time of publication the fourth most valuable company in the world. It developed the open-source Android mobile operating system and licenses it to other manufacturers, who produce and sell phones based on it: Yahoo! Finance "Alphabet Inc (GOOG)" <www.finance.yahoo.com>; and Android "Google Mobile Services — Android" <www.android.com>.

messages via traditional mobile carriers.[5] Now, every modern iPhone and Android phone comes with full disk encryption by default, and a given user is as likely to use an end-to-end encrypted messaging service as they are to use a traditional mobile carrier's calling service and SMS.[6] Communication and data storage are indeed "going dark".

Encryption Basics

The term "encryption" on its own is largely meaningless. Almost all electronic data stored or communicated in the 21st century undergoes some kind of encryption, so distinction is necessary. There are two types of encryption: *encryption at rest* and *encryption in transit*.

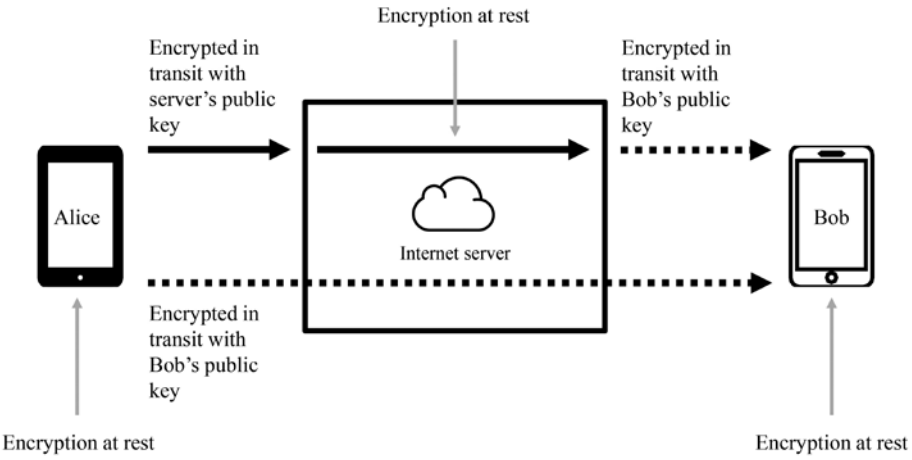

Figure 1[7]

This article is concerned with encryption at rest of data stored on smartphones. Encryption at rest refers to encryption of data in its stored state.[8] It is achieved by applying a mathematical process that uses an encryption key and turns the data on the device into an unreadable form.[9] In a smartphone using full hardware encryption, an encryption key is created by combining the user's passcode with a unique device identifier stored in an inaccessible part of the device's memory.[10] The data must be decrypted before it can be read. Decryption requires the use of the encryption key used to encrypt the data.[11]

5 Apple Inc *iOS Security: iOS 12.3* (May 2019).
6 James Andrew Lewis and William A Carter "Scoping Law Enforcement's Encrypted Messaging Problem" (6 April 2018) Center for Strategic and International Studies <www.csis.org>.
7 For further discussion on the underlying cryptography, see generally William Stallings and Lawrie Brown *Computer Security: Principles and Practice* (4th ed, Pearson Higher Ed, New York, 2018) at ch 21.
8 At 79.
9 At 67.
10 Apple Inc, above n 5, at 8.
11 Stallings and Brown, above n 7, at 54.

Encryption in transit refers to the transmission of data from one location to another and is used to prevent third parties from viewing the data.[12] While this article is not directly concerned with encryption in transit, a brief description is necessary for context. Encryption in transit is generally conducted using public key encryption. Rather than both the sender and receiver of data using the same key, each party has a public key and a private key. The sender encrypts data using the intended receiver's public key. After data is encrypted using a public key, only the corresponding private key can decrypt it.[13]

It is important to recognise the difference between two subtypes of encryption in transit: encryption with a server's public key and end-to-end encryption.[14] Encrypting with a server's public key is how traditional Internet messaging services work. This situation is represented by the three horizontal arrows at the top of Figure 1: the data is encrypted at rest on Alice's phone, encrypted with a server's public key for transit to the server, encrypted at rest on the server, encrypted with Bob's public key for transit to Bob and then encrypted at rest on Bob's phone. Crucially, this set-up allows the server in the middle to decrypt the data being sent — encryption is used here to prevent third parties from seeing into the communication. This situation contrasts with encryption with a user's public key, or end-to-end encryption, as shown by the long horizontal arrow at the bottom of Figure 1. Here, although the data passes through a server, it can only be decrypted once it reaches Bob's phone. This is significant because it means the only way to read the data is by getting access to one of the devices.

End-to-end encryption used to be a complex and rare undertaking. Now, it is increasingly available to the public and is a default function. It is used, for example, in Facebook's secret messages feature in Messenger or its WhatsApp network. Even if legislation were put in place to ban companies like Facebook from deploying commercial encryption, there is now a vast proliferation of encrypted services on the Internet. Anyone concerned about privacy can use end-to-end encryption to ensure messages cannot be read in transit.

Smartphone Encryption

Accessing smartphone data is increasingly challenging. Data on modern smartphones running iOS or Android is now encrypted at rest using full hardware encryption. Without access to an unpatched security flaw, it is impossible to get in without the encryption key. In order that users know their phones are truly secure, Apple and Google have elected to encrypt phones using a key they cannot recreate.[15] As discussed above, this is achieved

12 At 53.
13 At 67.
14 See Margaret Rouse and Madelyn Bacon "end-to-end encryption (E2EE)" Search Security <https://searchsecurity.techtarget.com>.
15 Apple Inc, above n 5, at 15; and Android Open Source Project "File-Based Encryption" <https://source.android.com>.

through a key creation process that combines a user's passcode with a unique device identifier stored in an inaccessible part of the device's memory.[16]

The traditional way of cracking encryption keys is brute force — attempting passwords through trial and error until the correct one is found. If it were possible to brute-force crack a smartphone's encryption key, it would take days to months, and it would be necessary to have a copy of the encrypted password on a separate computer where possible passwords could be attempted at a rate of millions per second.[17] Smartphones are now built such that this is not possible: modern smartphone keys require that the passcode be combined with the device's unique identifier, which is stored in hardware and cannot be extracted, and then tested on the phone itself.[18] Instead of attempting millions of combinations a second, an adversary can only attempt a dozen before the phone locks down or wipes itself. Brute-force cracking of smartphone encryption is therefore effectively impossible.

This means the only way to decrypt a modern smartphone is to get around the encryption, rather than break it. This requires exploiting a security flaw. Security flaws that are unknown to manufacturers are known as "zero day" exploits (reflecting the fact that the manufacturer has had zero days to patch the flaw), and represent a very serious threat.[19] Once zero day exploits are discovered, manufacturers immediately begin working on patches for the flaws, which they distribute in software update packages.

III UNITED STATES

Law enforcement in the United States has three options for accessing an encrypted smartphone: forced entry, compelling the user or compelling the device manufacturer.

16 Apple Inc, above n 5, at 8.
17 Stallings and Brown, above n 7, at 55.
18 Apple Inc, above n 5, at 18.
19 JM Porup "What is a zero day? A powerful but fragile weapon" (30 July 2019) CSO <www.csoonline.com>.

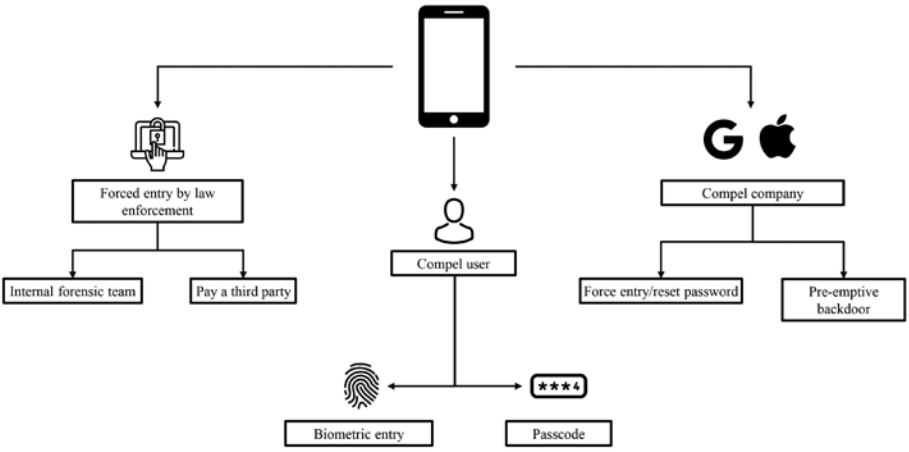

Figure 2

Forced Entry

From a law enforcement perspective, the most desirable option is to open confiscated phones without external help. Ten years ago, this was largely possible because protection was weak and toolkits to access devices were available. Today, zero-day flaws being the only way to crack modern phones, law enforcement does not have the internal tools to decrypt smartphones.

There is, however, a significant private market for services to open locked phones. There are two main companies offering products that can crack modern smartphones: Cellebrite[20] (Israel-based) and Grayshift[21] (United States-based). So far, there have been no legal issues with these companies. There would be no breach of law if these products were used by law enforcement in compliance with search powers; however, if these companies sold their products to anyone other than the government they would breach various laws regarding interference with computer systems. Sale of these products to foreign governments would entail more complex legal issues, but those issues are outside the scope of this article.

In September 2019 Cellebrite announced it had developed a new method of forced entry into smartphones that was effective on all versions of iOS up to iOS 12.4.2, as well as a range of Android devices.[22] This means forced entry is possible on a significant proportion of devices provided law enforcement is prepared to pay Cellebrite's price. However, as at the time of publication, Apple's latest iOS is iOS 13.2,[23] which Cellebrite has not yet

20 Joanna Shemesh "Cellebrite Advanced Services Solves the Toughest Encryption Problems for Apple and Android Devices" (24 September 2019) Cellebrite <www.cellebrite.com>.

21 Thomas Brewster "Mysterious $15,000 'GrayKey' Promises To Unlock iPhone X For The Feds" *Forbes* (online ed, Jersey City (NJ), 5 March 2018).

22 Shemesh, above n 20.

23 Apple Inc "Apple security updates" (5 November 2019) <https://support.apple.com>.

announced its ability to crack. It is also clear that only a minority of law enforcement agencies have access to this technology.[24]

From a technical perspective, it is highly undesirable for security bugs to exist in our devices. If Cellebrite or Grayshift are able to find a bug, it stands to reason any similarly resourced group could do the same. For this reason, Apple and Google tirelessly work to fix security flaws in their products and they will continue to do so in order to protect their customers' privacy, with the end result being law enforcement's inability to force entry without compelling either the user or the manufacturer to open the device.

Exploitable security flaws are undesirable and smartphone manufacturers should be encouraged to win the arms race against private hacking companies. Given this, I will not cover the legal issues involved in private sales of hacking toolkits and will instead focus on methods law enforcement might employ that do not face a technological block. While there are legal pathways to forced entry, the technological trends rule out forced entry as virtually impossible.[25]

Compelling Users

Where a phone has been confiscated, either in a search incident to arrest or as part of the execution of a search warrant, the natural first step is to ask the user to unlock it. A person can be compelled to assist law enforcement in the execution of a valid search warrant unless that person can claim some type of privilege.[26] In the United States, users may assert their Fifth Amendment privilege against self-incrimination[27] to resist an order to give up their device passwords. Given this is possible, it can be assumed users would assert the privilege whenever there is anything potentially incriminating on their phone.

This section discusses the issues that come up in this situation. The most significant legal oddity in this context relates to the United States' treatment of the difference between passwords and biometric authentication.

1 Fifth Amendment and Passwords

The modern understanding of the Fifth Amendment privilege, as set out in *Doe v United States*, is that it requires the following three elements:

(a) the statement was compelled by the government;
(b) the statement is incriminating; and
(c) the statement is testimonial.[28]

24 See Cellebrite *Industry Trend Survey 2019: Law Enforcement* (2019).
25 See Figure 3.
26 *Counselman v Hitchcock* 142 US 547 (1892) at 559.
27 United States Constitution, amend V.
28 *Doe v United States* 487 US 201 (1988) at 207–208. See also Richard M Thompson II and Chris Jaikaran *Encryption: Selected Legal Issues* (Congressional Research Service, R44407, 3 March 2016) at 6.

Depending on the scope of inquiry, it can be unclear why the Fifth Amendment should prevent law enforcement from compelling a user to give up their password. For this discussion, I will work on the basis of three possible scopes of inquiry:

(1) The password itself as the scope of inquiry. Prima facie, the statement will fail to meet the second criterion unless the content of the password is incriminating.
(2) The device as the scope of inquiry. Prima facie, the statement will fail to meet the first criterion unless the government compelled the user to use the device.
(3) The information on the device as the scope of inquiry. Prima facie, the statement will fail to meet the first criterion unless the government compelled the user to create the information.

According to this surface-level analysis, courts could find that the Fifth Amendment fails to protect a user from disclosing their password no matter the scope of inquiry. However, while this outcome is desirable, this legal analysis is unfortunately unsatisfactory. It fails to account for the testimonial significance inherent in giving up a password. At a minimum, giving up the password to a device means surrendering control and possession of the information contained within the device.

(a) Act of Production Doctrine

United States courts have accounted for this dilemma through a doctrine known as the *act of production doctrine*.[29] This doctrine recognises that the act of producing evidence can have "communicative aspects of its own".[30] For example, a suspect may incriminate themselves if the incriminating contents of documents they possess and control are revealed. However, the fact that they possess those documents is itself evidence that can be used against them. This means the first requirement, that the statement be compelled by the government, can be satisfied if production of the documents was compelled, even if creation of the documents was not.

Fisher v United States first set out the act of production doctrine.[31] *Fisher* concerned a request by the Internal Revenue Service for tax documents from the lawyers of two taxpayers. The United States Supreme Court held that the documents themselves were created voluntarily and so could not be "compelled testimonial evidence".[32] This means they could not meet the first limb of the *Doe* test. The act of giving up the documents, however, would have had testimonial implications — namely, that the documents existed and the defendants had possession and control of them.[33]

29 See *Fisher v United States* 425 US 391 (1976).
30 At 410.
31 *Fisher*, above n 29.
32 At 409–410.
33 At 409–410.

The act of production doctrine is qualified by the *foregone conclusion* exception.[34] This exception prevents suspects from relying on the doctrine where their testimony is a foregone conclusion. The exception was accepted in *Fisher* and later expanded on in *United States v Hubbell*.[35] In *Fisher*, the foregone conclusion exception applied because the government knew and could show that the documents existed and were under the defendant's control.[36] In *Hubbell*, the government could not demonstrate knowledge of the existence or location of the documents.[37] This meant the testimony inherent in the act of production would not be a foregone conclusion.

It follows from the focus on the testimonial impact of the act of production that the government need not show the contents of the documents are a foregone conclusion, just that the existence and location of the documents are. This analysis was confirmed by the United States Court of Appeals for the Ninth Circuit in *Re Grand Jury Subpoena* in 2014.[38] Put another way, the government does not need actually to know all the information it seeks. It only needs to know the information exists and its location.

(b) Impact of the Scope of Inquiry

The scope of inquiry is critical in the smartphone context. If the device itself is the scope of inquiry, the testimonial statement would be about possession and control of the device. In that case, the government would only need to show possession and control of the device are a foregone conclusion.[39]

If the files on the device are the scope of inquiry, the government would need to show possession and control of the files themselves. This is a higher threshold as it requires that the government know exactly what it is looking for on the device. In *Hubbell*, it was held that it is not enough for the government to claim a businessman "will always possess general business and tax records".[40] Therefore, it will not be possible for the government to meet this threshold with a claim that certain types of information will always be stored on a phone.

There is recent academic opinion on both sides of this debate. Framing their arguments in the language of this article, Orin Kerr argues for a device scope[41] while Laurent Sacharoff argues for a files scope.[42] Both claim that their conclusion is the best application of constitutional doctrines and best serves policy interests. Sacharoff is concerned with ensuring the government's

34 At 411.
35 *United States v Hubbell* 530 US 27 (2000) at 40.
36 *Fisher*, above n 29, at 411.
37 *Hubbell*, above n 35, at 40.
38 *Re Grand Jury Subpoena* 383 F 3d 905 (9th Cir 2004) at 910.
39 In practice, this test is very easy to establish. See my discussion below in relation to the New Zealand position.
40 *Hubbell*, above n 35, at 45.
41 Orin S Kerr "Compelled Decryption and the Privilege Against Self-Incrimination" (2019) 97 Tex L Rev 767 at 779.
42 Laurent Sacharoff "Unlocking the Fifth Amendment: Passwords and Encrypted Devices" (2018) 87 Fordham L Rev 203 at 208.

access to personal information is as limited as possible, whereas Kerr finds more compelling the interests of law enforcement.

United States courts have considered both approaches, which suggests both tests might need to be met. The United States Court of Appeals for the Eleventh Circuit considered a case where the government wanted access to an encrypted drive belonging to a person suspected of sharing explicit material of children on the Internet.[43] The Court found that the act of production would be testimonial because the testimony of the decrypted files was not a foregone conclusion. The government could not show the suspect's knowledge of the "existence and location of potentially incriminating files" (files scope) and his "possession, control and access to the encrypted portions of the drives" (device scope) were a foregone conclusion.[44] The Court ruled against the government in respect of both the files scope and the device scope. Kerr criticises this case as either wrongly decided or confusingly reasoned. He argues that the Court confused the inquiry scope options and erroneously conflated them, and failed to set out and apply a clear test.[45]

A files scope has been applied at the United States District Court level.[46] Decryption was ordered after an Immigration and Customs Enforcement agent saw a file labelled in a way that suggested child pornography. The Court cited *Re Grand Jury Subpoena* and found that the foregone conclusion exception applied. The government, having seen the files, could demonstrate "reasonable particularity" of knowledge.[47]

In summary, the Fifth Amendment will generally protect users from being compelled to give up phone passwords. The only exception is where the government can show it already knows what information it is looking for and the user has control and possession of that information. This would likely require a device scope, but may it require a harder-to-satisfy files scope. Thus, there is a significant legal barrier to the effectiveness of search warrants on phones in the United States. To reduce this barrier, I argue in my proposed framework for a device scope.

2 Biometric Authentication

Different factors come into play with biometric authentication. Some might expect greater protection would be given to biometric information than to a simple password. This would be consistent with jurisprudence from the Supreme Court of Canada, which sets out a hierarchy of privacy interests: bodily privacy comes first, followed by special privacy and then informational privacy.[48] This is not, however, the analysis adopted in the United States in respect of the Fifth Amendment.

---

43 *Re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335 (11th Cir 2012).
44 At 1346.
45 Kerr, above n 41, at 770.
46 *Re Grand Jury Subpoena to Sebastien Boucher* D Vt 2:06-mj-91, 19 February 2009.
47 At 3.
48 *Her Majesty The Queen v Tessling* 2004 SCC 67, [2004] 3 SCR 432 at [21]–[23].

In United States law, physical acts are unable to trigger Fifth Amendment protection as they are not capable of being testimonial. This doctrine was set out in *Schmerber v California*, where it was held that Fifth Amendment protection could not apply to compulsory blood samples because being compelled to undergo a physical act involves "[n]ot even a shadow of testimonial compulsion".[49] In other words, being compelled to undergo a physical act does not meet the third element of the *Doe* test. United States courts have granted warrants requiring certain fingers to be placed on phones[50] and, recently, face scans.[51]

The *Schmerber* doctrine was applied in *Doe*. There, Stevens J discussed in his dissenting judgment the difference between compelling a suspect to reveal the combination to a wall safe and compelling a suspect to give up the physical key to a safe. His Honour resolved that forcing a suspect to reveal the combination to a wall safe would require them to "use [their] mind to assist the prosecution in convicting [them] of a crime", and the suspect would therefore be protected by the Fifth Amendment.[52] The majority in *Doe* stated as an aside that it did not disagree with this aspect of Steven J's dissent.[53] The Supreme Court later affirmed Stevens J's thinking in *Hubbell*.[54]

There is limited case law on how this test applies to fingerprints, but a Virginia circuit court found in *Commonwealth of Virginia v Baust* that supplying a fingerprint is analogous to Steven J's scenario of giving up the physical key to a wall safe.[55] The consequence of this finding is that there can be no viable argument that an order for a specified biometric test can be protected by the Fifth Amendment. This is the oddity of American constitutional law to which Apple's "cop button" responds.

There is one possible caveat to this finding: there may be testimony in selecting the finger that unlocks a phone.[56] Kerr argues there is potential for fingerprint entry to be protected by the Fifth Amendment because the suspect selects which finger to use. Kerr considers this act of selection to be testimonial and to trigger the same device scope he suggests for passwords.[57]

This result seems highly irregular and leads to a difference in treatment between fingerprint sensors and face scans. Given the majority of smartphone users probably use their dominant thumb to unlock their phone, Kerr's conclusion is also unlikely to be practically significant. Law enforcement could simply obtain a warrant to try all five fingers — five being

---

49 *Schmerber v California* 384 US 757 (1966) at 765.

50 Orin Kerr "Can warrants for digital evidence also require fingerprints to unlock phones?" *The Washington Post* (online ed, Washington, DC, 19 October 2016).

51 Thomas Brewster "Feds Force Suspect To Unlock An Apple iPhone X With Their Face" *Forbes* (online ed, Jersey City (NJ), 30 September 2018).

52 *Doe*, above n 28, at 219.

53 At 210, n 9.

54 *Hubbell*, above n 35, at 43.

55 *Commonwealth of Virginia v Baust* 89 Va Cir 267 (2014) as cited in Thompson and Jaikaran, above n 28, at 14.

56 Orin Kerr "The Fifth Amendment and Touch ID" *The Washington Post* (online ed, Washington, DC, 21 October 2016).

57 Orin Kerr "Judge rejects warrant provision allowing compelled thumbprints to unlock iPhones" *The Washington Post* (online ed, Washington, DC, 23 February 2017).

the maximum number of unlock attempts per current iOS security policy.[58] Some warrants have in fact been argued in this way.[59] There is also a theoretical argument that choosing a finger is not substantively different to locating a physical key that the government knows to exist.[60]

That said, it is possible courts will err on the side of caution and uphold the Fifth Amendment, rejecting a general order to unlock a phone where finger selection is required. The result of this, however, would be the divergence of two types of orders: orders to unlock a phone that require finger selection, and orders to unlock a phone with a specified finger.

The following table takes account of these two types of finger-unlock orders. It summarises the orders available if a device scope were assumed.

Court orders available	***Can law enforcement prove the suspect owns or controls the device?***	
	Yes	*No*
Order to unlock phone that requires finger selection	✓	×
Order to unlock phone with specified finger	✓	✓
Order to unlock phone with face scan	✓	✓
Order to disclose password	✓	×

Table 1

The first two rows show the distinction between orders to unlock with a particular finger and orders that require the suspect to select a finger. While consistent with doctrinal principles, this distinction seems even more odd than the idea that passwords and biometric authentication should be treated differently. Further, there is no situation where a face scan mechanism could trigger the Fifth Amendment because people only have one face. The result is different treatment of different biometrics. To avoid these discrepancies, my proposed legal framework is neutral with regard to unlocking mechanisms.

Compelling Manufacturers

The third major option for accessing an encrypted smartphone is compelling the manufacturer to enter the device.[61] This option can be split into two categories:

58 Apple Inc, above n 5, at 10–11.
59 Kerr, above n 50.
60 Kerr, above n 56.
61 See Figure 2.

(a) compelling manufacturers forcibly to enter existing devices; and
(b) pre-emptively requiring manufacturers to build devices with a back door for government access.

I will first consider compelling manufacturers to enter existing devices.

The Communications Assistance for Law Enforcement Act (CALEA), passed in 1994, gives law enforcement, upon presentation of a warrant, nearly instant access to all phone calls and SMS messages sent over traditional telecommunication networks.[62] It only applies, however, to traditional telecommunication carriers. It does not apply to manufacturers of smartphones or developers of Internet-based communication services.[63] For the carriers that are covered, it has a very significant effect. It acts as a pre-emptive requirement to ensure there is technical capability to fulfil law enforcement warrants on an ongoing basis. CALEA can therefore be thought of as requiring a back door for government access. Congress has had many opportunities to bring smartphone manufacturers and other services under CALEA but it has not as yet done so. Apple has argued courts should interpret this congressional failure to act as a specific intention not to subject Apple to obligations similar to those in CALEA.[64]

1 Ordering Manufacturers to Unlock Phones

Due to the inability to use CALEA, the United States government has relied on the more general power in the All Writs Act of 1789[65] to compel manufacturers to assist in cracking smartphones.[66] The key authority on the All Writs Act is *United States v New York Telephone Co*, where the Supreme Court held that the Act performs a gap-filling function:[67] it allows courts to compel third parties in ways that "effectuate and prevent the frustration of orders" made by the courts.[68]

New York Telephone Co concerned an order authorising Federal Bureau of Investigation (FBI) agents to install two pen registers — devices that would record the outgoing numbers dialled on a telephone but not the contents of the call.[69] The All Writs Act was used to compel the New York Telephone Co to assist the FBI agents in installing the pen registers by

62 Communications Assistance for Law Enforcement Act 47 USC § 1001–1010.
63 Section 1001(8).
64 *Apple Inc's Supplemental Response to Court's October 9, 2015 Order and Opinion* (23 October 2015) at 6. The relevant court order is *Re Order Requiring Apple, Inc to Assist in the Execution of a Search Warrant Issued by this Court* ED NY 1:15-mc-01902-MKB-JO, 8 October 2015.
65 All Writs Act 28 USC § 1651.
66 See Eric Limer "Most Useful Podcast Ever: Why Is the FBI Using a 227-Year-Old Law Against Apple?" *Popular Mechanics* (online ed, New York City, 24 February 2016). Limer argues that applying the All Writs Act to smartphones is undesirable because of how old the Act is. I contend this argument lacks merit. Judges are very well equipped to apply old law. Further, the All Writs Act was broadly drafted so it could be used in unpredictable circumstances in the future where the government might need the help of a third party to effect a court order.
67 *United States v New York Telephone Co* 434 US 159 (1977) at 183.
68 At 172.
69 At 167.

providing telephone lines. The judgment set out three broad inquiries to determine whether an order under the All Writs Act is valid:[70]

(1) Does the order place an unreasonable burden on the private party?[71]
(2) Is the order consistent with the intent of Congress?[72]
(3) Is the private party's assistance necessary?[73]

In respect of those three questions, the Court ruled:

(1) The burden was not unreasonable. The telephone company was to be compensated for its work, and it regularly performed similar work for its own billing purposes.[74]
(2) The order was consistent with the intent of Congress because Congress had supported the use of pen registers.[75]
(3) The company's assistance was indeed necessary.[76]

The United States government has relied on the analysis in *New York Telephone Co* to compel Apple and Google to unlock phones in at least 63 cases since 2008.[77] Most of these cases have been orders issued on the same day they were sought and many have been sealed or redacted. Generally, they have been orders to unlock phones where the company had direct capability to do so.[78]

(a) The San Bernardino iPhone Case

The most well-known instance of these rulings is the San Bernardino iPhone case.[79] It concerned the FBI's successful application for an order for Apple to provide assistance in unlocking the iPhone 5C owned by one of the deceased shooters in the December 2015 San Bernardino terrorist attack. This case was different to previous orders that had only required Apple to use its existing capabilities. The iPhone's encryption in this case meant it was not possible for Apple to unlock it using tools immediately at its disposal.[80] The magistrate judge ordered that Apple create and sign with its private keys a version of iOS that could be flashed onto the phone and would allow the FBI to brute-force crack the passcode.[81]

70 Thompson and Jaikaran, above n 28, at 18.
71 *New York Telephone Co*, above n 67, at 172.
72 At 172.
73 At 173.
74 At 174–175.
75 At 176.
76 At 175.
77 Matthew Segal "Lessons From the Government's 63 Prior Attempts to Make Tech Companies Unlock Devices" (31 March 2016) Slate <www.slate.com>.
78 Segal, above n 77.
79 *Re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* CD Cal ED 15-0451M, 16 February 2016.
80 At 2.
81 At 2.

Apple responded with a strongly worded public letter in which it announced its intention to appeal the case.[82] The FBI obtained a delay and then withdrew its request after unlocking the iPhone with the assistance of a private company.[83]

The appeal was never heard. If it had been, the court would have applied the test set out in *New York Telephone Co* and likely undertaken the following analysis:

(1) There is a much greater burden on Apple here than in previous cases. There is a real risk that this version of iOS would get out and that Apple's reputation, future sales and stock price would be impacted.
(2) There is no law or policy in force that indicates congressional intent that the government be unable to seek assistance of this kind. As mentioned earlier, however, Apple has claimed that Congress's failure to amend CALEA should be regarded as an intention not to subject Apple to obligations of that nature.
(3) Apple's assistance will be necessary if the FBI cannot find another way to get access.

Legal scholars agree that it is impossible to know which way the case would have been decided.[84] That being said, it is the first of these inquiries that would present the greatest barrier to the order's being upheld. There are strong policy reasons against orders of this type. It is undesirable for the law to allow courts to compel the development of dangerous hacking tools such as the one Apple would have been compelled to build here.

A final question must be considered to understand the impact of the San Bernardino case: would a similar order be technically possible today? There was discussion at the time that while the architecture of the iPhone 5C would have allowed an attack of the type ordered, Apple could redesign the hardware to prevent this happening in the future.[85] Current-generation smartphones use a much more advanced security stack, which Apple likely designed with the San Bernardino order in mind. Apple has not made any explicit claims as to whether a similar order would be possible today, but language in Apple's current security documentation seems to imply that a similar attack would not be possible on current-generation iPhones.[86]

---

82 Tim Cook "A Message to Our Customers" (16 February 2016) Apple <www.apple.com>.

83 Laurie Segall, Jose Pagliery and Jackie Wattles "FBI says it has cracked terrorist's iPhone without Apple's help" (29 March 2016) CNN <www.cnn.com>.

84 Orin Kerr "Preliminary thoughts on the Apple iPhone order in the San Bernardino case: Part 2, the All Writs Act" *The Washington Post* (online ed, Washington, DC, 19 February 2016).

85 Dan Guido "Apple can comply with the FBI court order" (17 February 2016) Trail of Bits Blog <https://blog.trailofbits.com>.

86 Apple describes an "immutable code" in a circuit within the Secure Enclave (the coprocessor that runs cryptographic operations in an iPhone). This terminology implies it is no longer possible to make changes to the code with a software update: Apple Inc, above n 5, at 8.

2 Pre-emptive Compulsion: Back Doors

If manufacturers have now prevented themselves from being compelled to break into a device, the only remaining option would be pre-emptively to require them to provide a system of access. This would be similar to how CALEA works in respect of telecommunications companies.[87]

The debate over universal back doors to encrypted systems flares up more frequently in the United States than anywhere else.[88] The United States has significantly more ability to effect a legislatively mandated back door than other countries due to the fact that Apple and Google are both American companies. While current law does not provide for encryption back doors, there is no reason an Act of Congress could not change that.

An encryption back door is a way of accessing encrypted data that involves bypassing the normal security mechanisms.[89] It is easy to see why such a system is desirable for the government. Taking the user out of the equation allows the government to circumvent Fifth Amendment issues. Further, it ensures access to devices even when the user is unavailable or deceased, avoiding a messy legal battle each time.

Law enforcement organisations have frequently argued for mandatory back doors into encrypted systems. Former FBI Director James Comey never hesitated to remind the public that encryption frustrates the FBI's ability to protect them from "terrorists and child molesters".[90] But Comey sought to reframe the concept: rather than taking a "back door" approach, he advocated "[using] the front door, with clarity and transparency, and with clear guidance provided by law".[91]

The main argument against back doors is that creating vulnerabilities in encryption protocols is dangerous — it leads to weaker protection, which in turn leads to harm from malicious actors.[92] From a technical perspective, this argument is a straw man. It fails to consider the best and most likely form of implementing a back door system: a system of key escrow.[93] In such a system, encryption protocols would remain strong but all encryption keys would be issued by the government and held in a secure registry accessible by court order.[94] This does not completely address the issue, however, as the registry could become a target. The government would be tasked with

87 Communications Assistance for Law Enforcement Act § 1002(a).

88 See Alfred Ng "Congress introduces bill to block government encryption backdoors" (11 May 2018) CNET <www.cnet.com>; Kieren McCarthy "They're back! 'Feds only' encryption backdoors prepped in US by Dems" (9 April 2018) The Register <www.theregister.co.uk>; and Patrick Howell O'Neill "Barr's call for encryption backdoors has reawakened a years-old debate" *MIT Technology Review* (online ed, Cambridge (MA), 24 July 2019).

89 Amie Stepanovich and Michael Karanicolas "Why An Encryption Backdoor for Just the 'Good Guys' Won't Work" (2 March 2018) Just Security <www.justsecurity.org>.

90 Seth Rosenblatt "FBI director demands access to private cell phone data" (16 October 2014) CNET <www.cnet.com>.

91 Rosenblatt, above n 90.

92 Robby Mook "Encryption keeps us safe. It must not be compromised with 'backdoors'" *The Guardian* (online ed, United Kingdom, 12 February 2018).

93 Mihir Bellare and Shafi Goldwasser "Verifiable Partial Key Escrow" (paper presented to the 4th ACM Conference on Computer and Communications Security, Zurich, April 1997) 78.

94 At 79.

protecting the most valuable database on Earth — and governments have not always been effective in keeping data safe.[95] A key escrow system also has significant scope for civil rights abuses as the only barrier against the government's cracking into smartphones would be the law.

Current FBI Director Christopher Wray describes a twist on this model that he believes is more "consistent with both the rule of law and strong cybersecurity."[96] He advocates a model similar to that used by messaging platform Symphony, where a third party custodian retains encryption keys for release in an investigation.[97] The independent custodian might be a company's solicitor, for example. This model would, however, be problematic to implement on a larger scale, and privacy advocates argue convincingly that it is nothing but a dressed-up version of the key escrow system.[98]

In addition to these issues, any back door system has two fundamental problems: not every product is going to use it and choosing who gets access to the back door is highly problematic. Banning encryption is both impossible and undesirable, and there will always be encryption software products available that do not participate in a back door system. The existence of the Internet means there is no way to prevent the global exchange of encryption software.

I therefore concur with the vast majority of scholarship on this issue. Encryption back doors will always be doomed to fail and should not be attempted, as failed attempts have the potential to cause significant harm.

United States Summary

The United States position is best summarised visually.

95 See for example Chris Morris "USPS Security Flaw Exposes Personal Data of 60 Million People" *Fortune* (online ed, New York City, 26 November 2018); BBC "China hackers steal data from US Navy contractor — reports" (9 June 2018) <www.bbc.com>; and Jim Forsyth "Records of 4.9 mln stolen from car in Texas data breach" (30 September 2011) Reuters <www.reuters.com>.

96 Chris Bing "The FBI Director thinks this company found an answer to 'going dark'" (8 March 2018) Cyberscoop <www.cyberscoop.com>.

97 David Gurle "Bank-DFS Agreement" Symphony Blog <www.symphony.com>.

98 Bing, above n 96.

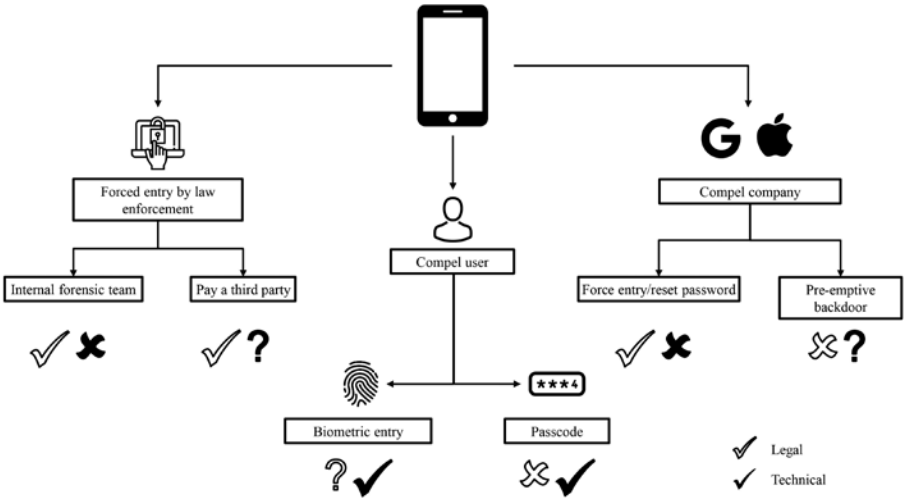

Figure 3

Figure 3 shows:

(1) Forced entry faces no legal barriers but is virtually impossible given technological trends.
(2) Compelling users faces no technical issues but may be legally barred as passwords and biometric authentication (save for face scans) may be protected by the Fifth Amendment.
(3) While lawful, compelling manufacturers forcibly to enter devices may be virtually impossible given technological trends. Compelling manufacturers pre-emptively to create back doors is technically possible but no laws exist to do this, largely because of the undesirable effects of such a system.

IV OTHER JURISDICTIONS

I will now briefly survey the positions taken in New Zealand and the United Kingdom before proposing the best way forward.

Law enforcement's ability forcibly to enter devices does not change in other jurisdictions given the barriers are technical, not legal. With regard to compelling manufacturers, outside of the United States there is extremely limited case law and similar technical barriers exist. There has been some discussion of pre-emptive back doors in other jurisdictions and there is significant evidence that a back door system operates in China.[99] However, I have already concluded that such a system is undesirable.

99 Stephen McDonell "China social media: WeChat and the Surveillance State" (7 June 2019) BBC <www.bbc.com>.

In light of this, in considering New Zealand's and the United Kingdom's position, I will not discuss the options of forced entry or compelling manufacturers. I will focus only on powers to compel users.

New Zealand

New Zealand has almost no problem with compelling users to unlock devices. New Zealand has a privilege against self-incrimination, contained in s 60 of the Evidence Act 2006. New Zealand does not, however, have anywhere near the same reverence for this right as the United States does. This is partially the result of the Fifth Amendment's being a constitutional right that cannot be abrogated by legislation, while New Zealand's Evidence Act specifically provides in s 60(3) that legislation may remove the privilege. Accordingly, both the New Zealand legislature and judiciary have been more willing to deviate from the privilege than their American counterparts where public policy goals would be better achieved by doing so.

New Zealand has a specific provision — s 130 of the Search and Surveillance Act 2012 — that obligates persons with the ability to access a device to assist the government in accessing it. Section 130 requires close reading to comprehend its meaning. Even then, it leaves room for ambiguity. It creates a wide power for persons exercising search powers to require specified persons to provide information or assistance in accessing data. Providing information or assistance must include giving up a password. The provision exempts a person from giving up information that incriminates them,[100] but this exception does not apply where the incriminating information is data stored on the device being accessed.[101] Section 178 of the Search and Surveillance Act then sets up an offence for failing to comply with a notice under s 130(1), with a maximum sentence of three months' imprisonment.

Unfortunately, despite the comprehensive scope of s 130, it fails to set unambiguously the limits of the self-discrimination exception. The Law Commission, in its 2017 review of the Search and Surveillance Act, agreed this section has uncertain effect.[102]

The language of s 130 has been judicially considered in the Court of Appeal,[103] but there is still uncertainty as to whether to take a completely narrow or a slightly broader reading of the provision. *R v Spark* concerned an alleged paedophile who had been persuaded by police to give up encryption codes for his computer hard drive.[104] He claimed he had been subjected to undue pressure to act.[105] This case concerned s 198B of the Summary Proceedings Act 1957, the predecessor to s 130 of the Search and Surveillance Act. Arnold J held that the existence of s 198B indicated Parliament's intention not to allow a user to deny the government access to a hard drive's

100 Section 130(2).
101 Section 130(3).
102 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017) at [12.160].
103 *R v Spark* [2008] NZCA 561.
104 At [3]–[5].
105 At [9].

contents.[106] His Honour stated "such a result would take the privilege against self-incrimination too far."[107] His Honour acknowledged that the subsections were "not easy to reconcile",[108] but it was not necessary for him to consider the provision's nuances beyond whether the privilege against self-incrimination could be relied upon.

1 Possible Readings of s 130

A narrow reading of the self-incrimination exception would be that it only applies where the password itself is incriminating; for example, the password is literally "I did the murder".[109] A broader reading would be that it applies where unlocking the device is incriminating — that is, where the act of unlocking the device is testimonial because it demonstrates a suspect has control of the device.[110] This reading of the section is similar to the act of production doctrine in United States jurisprudence in that it recognises the testimony inherent in unlocking the device. Alternatively, it can be thought of as adopting a device scope of inquiry.

The Law Commission suggests a third possible reading: the provision applies where the act of providing the password is incriminating, because it will lead to the discovery of incriminating information.[111] I reject this reading. Section 130(3) specifically states the existence of incriminating information "held in, or accessible from," the device cannot be reason to refuse to assist a search on the basis of the privilege. This is the position taken in *R v Spark*.[112] I also note the Law Commission considers it "plain" that the privilege ought not to be available where assistance would lead to the discovery of incriminating information.[113]

The Law Commission also considers the privilege should not be available to protect a person from disclosing the fact they know the access information.[114] Its position is that the privilege should only be available where the password itself is incriminating (the situation where the password is literally "I did the murder").[115] Even in this situation, the Law Commission considers the privilege only goes so far as to justify a refusal to give the password to an enforcement officer. Section 130 ought still to compel the suspect to assist in accessing the device in a way that does not reveal the privileged password; for example, entering the password on the device without saying what the password is.[116] That position makes sense: it would be highly irregular to allow a suspect's choice of password to defeat an order to unlock.

106 At [33].
107 At [33].
108 At [30].
109 Law Commission, above n 102, at [12.163].
110 At [12.163].
111 At [12.163].
112 *Spark*, above n 103, at [33].
113 Law Commission, above n 102, at [12.168].
114 At [12.168].
115 At [12.169].
116 At [12.169].

The wider problem with the Law Commission's view is that by rejecting the broader device scope reading, the testimony inherent in assisting law enforcement to unlock a device is ignored. As discussed in the context of the United States, there is an argument to be made that privilege should be available in cases where law enforcement cannot yet prove who the device owner is (for example, where the device has been found at a crime scene). However, due to enforceability issues, privilege in this case might be available even if not included in s 130.

2 Enforceability

To convict an accused of failing to assist under s 178, the Crown would need to meet the usual criminal law standard of proving guilt beyond reasonable doubt. Section 130 only covers persons with relevant knowledge of the device in question. If the Crown is unable to prove beyond reasonable doubt that the accused possesses the access information, it will not secure a conviction.

The impact of this is that even if there is no privilege the Crown cannot enforce s 130 where it cannot separately show that the suspect knows the access information. A suspect who would make a testimonial statement by unlocking the phone can claim they do not know the access information. The Crown cannot prove otherwise. The suspect would likely not even need to perjure themselves — they could simply plead not guilty and put the Crown to proof.

This enforcement problem is likely unavoidable. That is not an issue, however, as it is also normatively desirable — it prevents misuse of the compulsion powers. Further, it is unlikely to be a significant issue in practice because in the vast majority of cases it will be possible for the police to prove to a sufficient standard that the suspect is the device owner. Evidence of ownership could include emergency contact information, the phone number, stored SIM card contacts, cellular carrier account details and billing, cellular carrier usage and location history, linked Apple or Google accounts, linked email accounts, wallpaper photos, automatic connection to WiFi networks or Bluetooth devices, and forensic evidence such as fingerprints or DNA. Such articles of evidence are attainable without needing to unlock the phone. Given this wide scope, having to prove the suspect is capable of unlocking the phone should not be an impediment to police work.

This legal position runs a risk of abuse: criminals could ensure they use their device in such a way that it cannot be proved they own it. But given the wide range of possible evidence of ownership, this will be a minimal risk: it would simply be too hard to use a phone in any productive way without leaving some trace of ownership evidence.

3 Biometric Authentication

In New Zealand, there is no difference in the legal treatment of passwords and biometric authentication. The language of the s 130 duty to "assist access" does not differentiate between passwords and other authentication methods.

The only reason biometric authentication might be a more insecure method is a practical one: physically compelling a biometric scan is possible, whereas physically compelling someone to give up a password is not. It is worth noting this means Apple's "cop button" does not have the same legal effect in New Zealand as it does in the United States, except to that practical extent.

United Kingdom

The United Kingdom's legal framework is largely consistent with the model I propose. As a result, however, some elements of the United Kingdom's framework highlight problematic aspects of mine. The United Kingdom's legislative scheme for the investigation of encrypted data is pt III of the Regulation of Investigatory Powers Act 2000.[117] The notice obligations[118] are similar to New Zealand's, and s 53 of the Act creates an offence for failure to comply with a notice. It carries a maximum sentence of five years' imprisonment in national security or child indecency cases, or two years' imprisonment in all other cases.[119] Thus, the main difference between the New Zealand and United Kingdom positions is that the United Kingdom's punishment is more severe. While a terrorist or child pornographer in New Zealand can simply choose to take three months' imprisonment rather than give up their password, a similar person in the United Kingdom would go to prison for five years.

1 The Concerning Use of United Kingdom Law

There is one particular case where the United Kingdom government exercised its powers under the Regulation of Investigatory Powers Act that gives cause for concern.[120] In 2008, a schizophrenic man was sentenced to nine months' imprisonment under s 53 of the Act for failure to comply with a notice in exactly the sort of circumstances with which civil rights advocates take issue. The man was arrested without any link to terrorist activities. However, 9 ng of RDX, a powerful explosive, were found on his left hand. Forensics routinely discounted a result of fewer than 5 ng.[121]

A search uncovered several encrypted hard drives and the man was served a notice obligating him to provide the information to decrypt these drives. A paranoid man with a mistrust of authorities possibly linked to his schizophrenia, he refused to do so. Counter-Terrorism Command officers became suspicious of the man's non-compliance. "There could be child pornography, there could be bomb-making recipes," said one detective.

117 Regulation of Investigatory Powers Act 2000 (UK).
118 Sections 49–50.
119 Section 53(5)–(5A).
120 There is no available judgment of this case and I have relied on media reports to analyse it, primarily Christopher Williams "UK jails schizophrenic for refusal to decrypt files" (24 November 2009) The Register <www.theregister.co.uk>.
121 At 1.

"Unless you tell us we're never gonna know... What is anybody gonna think?".[122]

The man was sentenced to nine months' imprisonment after pleading guilty to the s 53 charge.[123] Assuming this case has been reported accurately, it might represent a problem with the legal framework I propose: a potential for unjust outcomes that disproportionately affect vulnerable members of society. I contend, however, that this case is a very specific example of the United Kingdom government's use of investigatory powers that should have been prevented in other ways. At some point in the case, a court ruled there was enough evidence to substantiate a search warrant for the man's encrypted hard drives. It is this decision that was unjust, not the decision to punish the man for failing to comply with the warrant.

This case presents no novel reason for separating search powers over physical spaces from search powers over digital ones. The issue of search warrants being granted in circumstances where they perhaps should not have been applies equally to all cases (though this is not the focus of this article). At any rate, it is better to have a possibly flawed legal test controlling search warrants than to allow criminals to use encryption to avoid searches.

2 Self-incrimination Defence

The United Kingdom has also considered the self-incrimination defence issue that the United States and New Zealand have grappled with. The United Kingdom search powers legislation does not explicitly reference a privilege against self-incrimination, but the issue has been raised judicially. The English Court of Appeal considered a case where the defendant breached a notice under the Regulation of Investigatory Powers Act.[124] The defendant claimed privilege against self-incrimination, but the Court took an extremely limited view of this. The Court considered "knowledge of the means of access to the data" — a device scope of inquiry — may engage the privilege but only where the data itself is incriminatory.[125] It was of the view that where the data is incriminatory the trial judge will have discretion to exclude evidence of the means by which the prosecution obtained access to it. The Court considered this was enough to resolve the self-incrimination problem.[126]

122 At 2.
123 At 3.
124 *R v S* [2008] EWCA Crim 2177, [2009] 1 WLR 1489 at [9].
125 At [24].
126 At [24]–[25].

V A WAY FORWARD

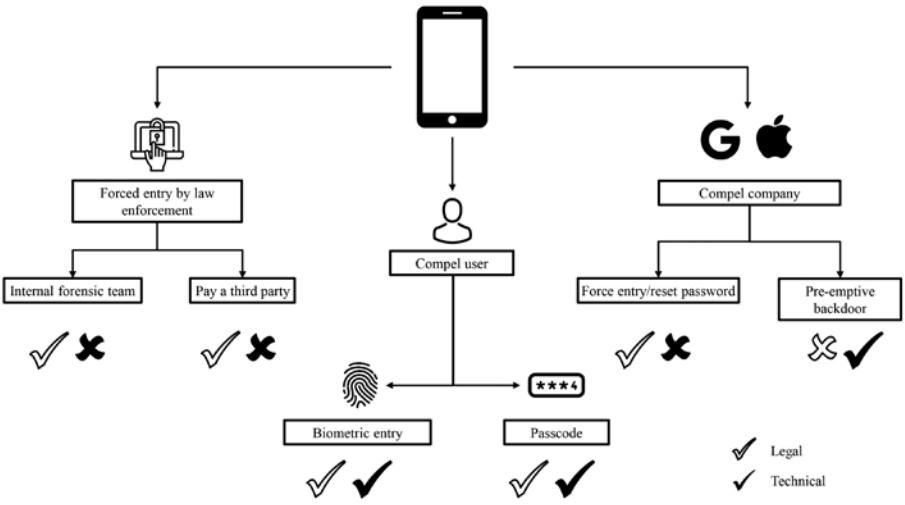

Figure 4

The legal framework I propose is summarised in Figure 4. It recognises that strong technical barriers exist to block forced entry and compulsion of manufacturers to unlock devices. Under my framework, a legal barrier to a pre-emptive back door exists. The only method of entry into smartphones that is both legally and technically available is compelling users to give up passwords and biometric data.

The legal framework to compel users to unlock their devices must have the following characteristics:

(1) There must be a positive obligation on suspects to assist law enforcement with searches of their devices.
(2) There must be a substantial punishment for failure to comply with an order to unlock a device. I suggest five years' imprisonment as a maximum sentence.
(3) Privilege against self-incrimination can only be relied upon where the prosecution cannot prove beyond reasonable doubt that the suspect has the ability to unlock the device.
(4) All types of biometric entry must be treated equally. Put differently, this framework must apply to any attempt to unlock a phone, even where no testimony from the suspect is required.

The first of these criteria is logically required to give effect to my proposed framework.

The second is also logically required, but the question of maximum sentence is subjective. Current maximum imprisonment durations range from

New Zealand's three months[127] (but note the Law Commission has recommended this be increased to six months[128]) to the United Kingdom's five years (in national security and child indecency cases)[129] to Australia's 10 years.[130]

The third criterion is more complex. The law should not punish people who genuinely cannot unlock a device, and this framework is not designed to be used to ascertain ownership. There are also doctrinal and rights issues involved in completely ignoring the privilege against self-incrimination, as well as possible enforcement issues. Given the range of evidential options for proving device ownership, the requirement to prove first that the subject of the order has the ability to unlock the device will rarely pose an issue.

The fourth criterion prevents differential treatment of entry methods that require statements and those that do not. It is normatively undesirable for there to be different legal consequences for different smartphone authentication methods. This criterion requires equal treatment of all types of biometric entry. This means face scan orders and the types of fingerprint scan orders that are legally available in the United States without a need for the government to prove first that the suspect owns the device would not be possible. Under my proposed framework, there would be greater protection for most biometric authentication, but possibly less protection for passwords and some fingerprint authentication, than there is in the United States currently.

VI SEARCH POWERS

This article has discussed the enforceability of a legally valid search power. It has not considered the legal mechanisms that create a legally valid search power. While I maintain these are two separate issues, they cannot be considered in isolation. The framework this article suggests is a powerful and dangerous legal tool that must be carefully controlled by strong, well-applied legal rights against unreasonable search and seizure.

This article argues that allowing legal tests to determine search powers is normatively more desirable than allowing malicious actors to use technology in a way that inhibits searches. That normative claim falls down where legal protections against unreasonable search and seizure are insufficient (that is, where they are substantively flawed) or ineffective (that is, where a lack of procedural rights prevents them from being effected). An example of how this could become problematic can be seen in pairing warrantless search powers with the suggested penalty for refusal to unlock a device. Allowing law enforcement officials to conduct the searches possible

127 Search and Surveillance Act, s 178.
128 Law Commission, above n 102, at [12.179].
129 Regulation of Investigatory Powers Act, s 53(5A).
130 Surveillance Devices Act 2004 (Cth), s 64A(8).

under the proposed framework without judicial authorisation creates room for significant injustices and invasions of privacy.

There is a line of cases establishing that electronic devices engage particularly significant privacy interests and so search warrants should always be required. The most noteworthy case recognising this concept was *Riley v California*, where the United States Supreme Court unanimously held that the warrantless search of a phone is unconstitutional.[131] The New Zealand Law Commission considered *Riley* in making its recommendation that warrantless search powers be replaced with a power to seize and secure a device pending a search warrant.[132] I concur with the *Riley* position and the Law Commission's recommendation.

VII SEARCHES AT THE BORDER

This article's analysis applies to searches at the border insofar as the ability of law enforcement officers to effect valid search warrants is concerned. Recognising that legal and policy debates around border searches have different features to those around regular searches, this article does not comment on what border search powers with regard to electronic devices are or should be available. That is an important area for legal scholarship, however, and should be the subject of its own research.

VIII CONCLUSION

Encryption and security will only become more and more important in future as more of our lives exist in digital spaces and the products we use become even smarter and more complex. Digital data will continue to grow in importance for law enforcement but there is no end in sight to the trend towards better secured data, nor should there be.

The legal frameworks that decide how searches are to be executed should be clear and principled. The public should be able to comprehend their legal rights and recognise that there is reason for them. In its current state, United States law, despite being the most established and influential in this area, fails to meet this standard.

The framework I propose is a principled compromise that allows secure technology to be maintained alongside effective law enforcement. Its adoption would be a significant step towards a legal system that competently deals with the realities of a modern, digital world.

131 *Riley v California* 573 US __ (2014).
132 Law Commission, above n 102, at [12.34] and [12.39].