THE PRIVILEGE AGAINST SELF-INCRIMINATION AND THE COMPELLED PRODUCTION OF A PASSWORD

Daniel Marc Hochstrasser

ORCID identifier: 0000-0001-7391-0169

Doctor of Philosophy

September 2019

Melbourne Law School

University of Melbourne

Submitted in total fulfillment of the requirements of the degree of Doctor of Philosophy

ABSTRACT

Over the past decade, the use of encryption to protect electronic devices, including smartphones and computers, has become commonplace. Most people use encryption daily, often unwittingly. This has consequences for law enforcement, which increasingly finds itself unable to access data on encrypted devices, even where a warrant has been obtained to search that device. A common response to this problem is for law enforcement officials to seek an order compelling a suspect in a criminal investigation to produce the password to the encrypted device. In response, suspects have argued that providing that information would infringe the privilege against self-incrimination as it might reveal incriminating information. This thesis considers whether the privilege against self-incrimination can prevent the granting of an order to produce the password. It does so by asking whether an order compelling the production of a password – what this thesis terms a compelled production order – falls within the scope of the privilege; by examining how Australia's understanding of the scope of the privilege compares to that adopted by courts in Canada, England and Wales and the United States; and by assessing how Australia, and the three comparator jurisdictions, have addressed this issue.

This thesis adopts a doctrinal approach. It identifies how courts in the four jurisdictions have previously established the boundaries of the privilege when considering related cases, being cases that are concerned with similar issues to compelled production order cases. Such cases include those involving orders for bodily samples and single question reporting obligations such as those imposed on motor vehicle owners. Once the scope of the privilege is identified through those related cases, and the reasoning behind those decisions analysed, the thesis considers whether compelled production orders fall within that scope and if they have been resolved in a manner consistent with those earlier cases. This thesis does not, therefore, engage with the various proposed rationales for the privilege but instead has a more pragmatic focus.

Recently, alternative means of accessing encrypted data, such as hacking powers for law enforcement and the power to compel a telecommunications company to remove

encryption from their products, have received growing attention. In England and Wales and Australia, such alternative encryption workarounds are, like compelled production orders, authorised by statute. Those statutory provisions, however, require that the order sought, be it a compelled production order or one authorising the use of an alternative encryption workaround, must be proportionate – a requirement that demands that the measure used is the least intrusive of the effective means available. This creates a symbiotic relationship between compelled production orders and the alternative encryption workarounds, one that has consequences for the scope of the privilege.

This thesis finds that while compelled production orders in Australia may fall outside the scope of the privilege in instances where the privilege has been abrogated, the use of a proportionality requirement in the relevant statutes means that the scope of the privilege has a fluid form and will contract or expand depending on the availability of an alternative encryption workaround.

DECLARATION

I declare that:

I. This thesis comprises only my original work towards the degree of Doctor of Philosophy.

II. Due acknowledgement has been made in the text of this thesis to all other material used.

III. The thesis is fewer than the maximum word limit in length, exclusive of the tables, maps, bibliographies, and appendices.

Daniel Hochstrasser

29 September 2019

PREFACE

This thesis was funded by an Australian Government Research Training Program Scholarship.

ACKNOWLEDGEMENTS

I am always surprised at what I learn on the way to my destination. When I enrolled in this PhD, I expected to spend three years learning about self-incrimination and encryption. And I did. But I also learnt about family. I learnt about the sacrifices a wife makes to enable a husband to become a student once more: the hard work to financially support our family; the encouragement for me when the thesis seemed all consuming; the patience when three years become more. I learnt about what it is like to grow a family, when my daughter arrived part way through my thesis. From her I learnt that a young daughter can inspire and help keep you motivated when spirits are flagging. (I also learnt that she can write three PhD theses in one week – though I did not learn how she managed that!) And from my mom and dad I learnt that even when one's children hit middle age, still family makes sacrifices for family, as was shown by my mom (with an always helpful hand from my dad) caring for my daughter (and imbuing in my daughter many of her unique mannerisms, hopefully to last a lifetime) while my wife worked full time and I…I did this. This, then, is a thesis that could only have been written with the love and support of my family, and those three women in particular.

Family is not enough though: you also need the right supervisors. I am fortunate to have had them. For any student it is true that their thesis could not have been completed without their supervisors' guidance and expertise. That is true in my case, but it is equally true that without the encouragement and support of Professor Jeremy Gans this thesis would not have commenced, let alone concluded. Professor Gans has mentored me from the earliest stages of this thesis and was instrumental in encouraging me to apply for entry into the PhD program. For his support I am indebted to him. Associate Professor Jacqui Horan helped supervise the early stages of my PhD, during which time she was a source of constant support, for which I remain grateful. Associate Professor Andrew Roberts joined the team at a relatively late stage (after Associate Professor Horan took up an opportunity at another university). His suggestions and fresh eye helped sharpen the focus of the thesis at an important stage in its writing. My thanks go out to him, too.

For those unnamed friends and family who have encouraged me during this process, too many to mention individually, thank you for your support.

And now I must go buy a ginger cat – the things a father promises his daughter he will do once the thesis has been submitted!

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

In 2006, the District Court for the Northern District of New York faced a novel issue.[1] During the execution of a search warrant as part of an investigation into the production of child pornography, a hard drive and USB flash drives were seized containing encrypted folders. Due to the encryption, law enforcement officials were unable to access the contents of those folders. As a result, they applied for and obtained a subpoena compelling the defendant to produce the encryption key to the folders. The defendant sought to quash the subpoena on the grounds that such an act of compulsion would infringe the privilege against self-incrimination. On the facts before it, the Court held that the defendant's privilege was not infringed.[2] Since that first decision, the issue of whether the privilege could be relied upon by a suspect to prevent a compelled production order being made against him or her has arisen in several other jurisdictions, including England and Wales, Canada and Australia.[3] There is evidence that it is a growing occurrence.[4] This thesis examines this issue by considering the following questions: does compelling the production of a password in Australia fall within the scope of the privilege; how does the Australian understanding of the scope of the privilege in relation to compelled passwords compare to that of the United States, Canada and England and Wales; and how has Australia addressed the issue of whether a password can be compelled from a suspect?

---

1 *United States v Pearson* (ND NY, No 1:04-CR-340, 24 May 2006).

2 The privilege against self-incrimination will frequently be described as simply the privilege in this thesis.

3 This thesis will use the term compelled production order to refer to any court order requiring a suspect to produce the password to an encrypted device, to decrypt the encrypted device or to produce an unencrypted version of the documents.

4 As one example, in the United States the Manhattan District Attorney's Office – which for the past few years has released an annual report on the impact of encryption on its performance of its duties – has published statistics showing that between 2014 and 2017, the number of encrypted smartphones that it encountered during investigations increased nine-fold: Manhattan District Attorney's Office, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (November 2017), 5 <https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf>.

WHY THIS ISSUE HAS ARISEN

Three changes have driven the development of this issue. The first is the increasing use of electronic devices to create and store electronic data, thereby creating the pool of data to which law enforcement may seek access. Secondly, encryption has become formidably strong. Encryption entails the use of an encryption algorithm to scramble data into a code which is unreadable without the encryption key.[5] Though encryption has been used for centuries, early encryption methods were at times relatively basic. For example, when transferring messages to his army, Julius Caesar would encrypt his messages by moving each letter forward three letters in the alphabet.[6] Applying that system today, an 'a' would become a 'd', a 'b' becomes an 'e' and so forth. This form of encryption, which is known as a substitution cipher,[7] is susceptible to being cracked due to its simplicity and the ubiquity of words such as 'the' in the message.[8] By contrast, modern encryption as used on today's electronic devices is created with sophisticated mathematical equations using the binary number system (which uses only two digits, zero and one).[9] Those encryption algorithms can create encryption keys that are 128 or 256 bits long. That is, the encryption key contains 128 or 256 zeros or ones in random order.[10] While Caesar's code could be defeated by trying each of the 26 possible versions until the correct one was identified, an encryption key that is 128 bits long contains approximately 300,000,000,000,000,000,000,000,000,000,000,000,000 possible keys.[11] With modern computing power, it is not possible to guess that many keys in a person's lifetime. For example, with a computer that is capable of guessing one million keys per second, after one year that computer would have only worked through 'a billionth of a billionth of the possible combinations'.[12] The result is the

---

5 Orin Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 *Georgetown Law Journal* 989, 993.

6 Robert Churchhouse, *Codes and Ciphers: Julius Caesar, the Enigma and the Internet* (Cambridge University Press, 2002) 2.

7 Ibid 3.

8 As there are 26 letters in the English alphabet, the Caesar code has only 26 possible versions, or keys. By writing out each of the 26 possible versions it was possible to break the code: ibid 13.

9 V Anton Spraul, *How Software Works: The Magic Behind Encryption, CGI, Search Engines and Other Everyday Items* (No Starch Press, 2015) 10.

10 Kerr and Schneier, above n 5, 993-94.

11 Spraul, above n 9, 16.

12 Ibid.

existence of encryption algorithms that, absent a flaw in the software, are all but unbreakable.

The third change is the increasing ease with which encryption can be used. Historically, encryption has relied on a private key system in which the same key is used both to encrypt and decrypt data. To use this form of encryption, the encryption key first needs to be securely distributed to the relevant parties – an act that cannot itself be protected by encryption as encryption only follows after the key has been delivered.[13] In the late 1970s, however, public key encryption was developed.[14] In this system, the public key – which is publicly available – is used to encrypt the data, and a separate private key known only to the user is used to decrypt the data.[15] It is the advent of public key encryption, which enables encrypted communications between two unrelated parties, that has been the primary driver behind the growth in the use of encryption.[16] It enables an ordinary consumer of modern electronics to use encryption, often without any inconvenience and potentially even without their knowledge. Since iOS 8, Apple has automatically encrypted all electronic data on iPhones and iPads.[17] Android software, too, offers the ability to encrypt data on devices running its software.[18] For computers, Microsoft offers an encryption program called BitLocker on the Pro version of Windows 10,[19] and there are several third party encryption programs that can encrypt either individual files or the entire hard drive of a computer.[20] Encryption is also used on many messaging platforms. Whatsapp, a messaging app that encrypts the messages sent

---

13 Bert-Jaap Loops, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer Law International, 1998) 36.

14 RSA, one of the most widely used public key algorithms, was first published by Ron Rivest, Adi Shamir and Len Adleman in 1978: Fred Piper and Sean Murphy, *Cryptography: A Very Short Introduction* (Oxford University Press, 2002).

15 See, eg, Nathan Saper, 'International Cryptography Regulation and the Global Information Economy' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 673, 675.

16 Nathan Saper, 'International Cryptography Regulation and the Global Information Economy' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 673, 675-76.

17 Cyrus Farivar, 'Apple Expands Data Encryption under IOS 8, Making Handover to Cops Moot' (18 September 2014) *Arstechnica* <https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/>. Since OS X Lion, full-disk encryption has been possible on Mac computers using FileVault, though it is not automatically enabled.

18 <https://source.android.com/security/encryption>.

19 <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>.

20 See, eg, <https://www.pcmag.com/article/347066/the-best-encryption-software>.

between users, has been downloaded more than 1.5 billion times and more than 60 billion messages are sent using the app daily.[21] Messages sent using Messages on iOS are also encrypted. All of these programs use public encryption keys.

While the products described use 128 bit or 256 bit encryption, they do not require the user to remember an encryption key of that length. Messaging apps perform the encryption and decryption in the background, without requiring the user to take any action.[22] Other software programs that do require the user to enter the encryption key avoid the need for the user to remember that encryption key by allowing them to use a passcode or similar such device instead. In this situation, the encryption key itself is encrypted and the passcode – which is created by the user – is used to unlock the encryption key, which in turn automatically decrypts the data.[23] This is the system used, for example, in iOS, where a user enters a short passcode, typically six characters long, which unlocks the encrypted device. Thus, while the passcode is not the actual encryption key, it operates as such.[24] Note that for simplicity sake, and to remain consistent with the terminology used in a particular case or statute, the terms encryption key, passcode and password have the same meaning in this thesis.

The result of these changes is an environment in which a significant proportion of consumers of electronic devices utilise some form of encryption. Moreover, for individuals engaging in criminal conduct, there are several third-party encryption programs that they can use to encrypt documents on computers and hard drives. While the past decade has seen an increase in the number of suspects protecting documents with encryption,[25] that number is expected to increase further as the use of encryption becomes even more commonplace. As those developments may make the issue of compelling the production of a password even more important in the future, it is valuable to understand the parameters within which the compulsion occurs and

---

21 <https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/>.

22 Kerr and Schneier, above n 5, 994.

23 Ibid.

24 Ibid.

25 Manhattan District Attorney's Office, above n 4, 5.

whether it is consistent with how the privilege has previously been applied in similar circumstances.

METHODOLOGY

When assessing whether the privilege applies to compelled production orders, that determination can be made either by reference to the rationale for the privilege (which would be a theoretical approach) or the scope of the privilege in the jurisdictions under examination (which, as will be seen below, is a doctrinal approach). The analysis in this thesis will be by reference to the scope of the privilege – that is, the doctrinal approach. The scope of the privilege refers to those instances in which courts have found that the privilege operates in respect of a particular search or order: it is the outer boundary of the privilege as determined by judicial decision-making when considering related orders. This approach is adopted in part because there is no single broadly accepted rationale for the privilege.[26] Several rationales have been advanced to explain the development of the privilege. It has been said of the privilege that: its purpose is to prevent abuses of power by the state;[27] it serves to require law enforcement officials to discover evidence against a suspect without the assistance of that suspect;[28] it prevents the admission into court of evidence that, obtained through compulsion, may be

---

26 See, eg, Ronald J Allen and M Kristen Mace, 'The Self-Incrimination Clause Explained and its Future Predicted' (2004) 94(2) *Journal of Criminal Law and Criminology* 243, 244 (where the authors note that 'the theoretical foundations of the Fifth Amendment are conventionally thought to be in disarray').

27 See, eg, *Environment Protection Authority v Caltex* (1993) 178 CLR 477, 440 (McHugh J); *Murphy v Waterfront Commission of New York Harbor* (1964) 378 US 52, 55; *Saunders v United Kingdom* (1997) 23 EHRR 313, 337.

28 See, eg, William Blackstone, *Commentaries on the Laws of England* (The Legal Classics Library, vol IV, 1765) 293; *Murphy v Waterfront Commission of New York Harbor* (1964) 378 US 52, 55; *Saunders v United Kingdom* (1997) 23 EHRR 313, 337; Ian Dennis, 'Instrumental Protection, Human Right or Functional Necessity? Reassessing the Privilege against Self-Incrimination' (1995) 54(2) *Cambridge Law Journal* 342, 353-54.

unreliable;[29] it protects 'the inviolability of the human personality';[30] and that it is necessary to prevent a suspect being placed in the cruel trilemma.[31]

The cruel trilemma, one of the oldest arguments that has been advanced to justify the existence of the privilege,[32] is said to arise when an accused is asked a question that requires him- or herself to incriminate him- or herself (through a truthful answer), commit perjury (through a lie) or commit contempt (through a refusal to answer). In the context of password compulsion, a demand on a suspect to produce a password to an encrypted device might require the suspect to: incriminate him- or herself if the password is produced and it leads to incriminating evidence; perjure him- or herself if the suspect falsely testifies in court that he or she doesn't know the password; or be convicted of contempt if he or she refuses to provide the password. The cruelty is thus said to arise from the fact that suspects are forced 'to do serious harm to themselves'[33] – that serious harm being criminal sanction, whether it be for the underlying offence, perjury or contempt of court. Notwithstanding the broad support that exists for the existence of the cruel trilemma, explanations for why it is cruel to expose a suspect to this trilemma are often unsatisfactory.[34]

---

29 See, eg, *Murphy v Waterfront Commission of New York Harbor* (1964) 378 US 52, 55; *Saunders v United Kingdom* (1997) 23 EHRR 313, 352; Dennis, above n 28, 348-49; Penney, above n 29, 250.

30 *Murphy v Waterfront Commission of New York Harbor* (1964) 378 US 52, 55. See also Andrew Ashworth, Self-Incrimination in European Human Rights Law – A Pregnant Pragmatism?' (2008) 30 *Cordoza Law Review* 751, 759 (where Ashworth refers to the 'need to protect suspect's will from coercion').

31 See, eg, *Murphy v Waterfront Commission of New York Harbor* (1964) 378 US 52, 55; David Dolinko, 'Is There a Rationale for the Privilege against Self Incrimination?' (1986) 33 *UCLA Law Review* 1063, 1090; Michael S Green, 'The Privilege's Last Stand: The Privilege against Self-Incrimination and the Right to Rebel against the State' (1999) 65(3) *Brooklyn Law Review* 627, 630; Dennis, above n 28, 358; Steven Penney, 'What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination Law in the Post-Charter Era. Part I: Justifications for Rules Preventing Self-Incrimination' (2003) 48 *Criminal Law Quarterly* 249, 250.

32 Dolinko, above n 33, 1090-1091.

33 R Kent Greenwalt, 'Silence as a Moral and Constitutional Right' (1981) 23(1) *William and Mary Law Review* 15, 39.

34 See, eg, Dolinko, above n 33, 1092 where he notes that some writers have acknowledged that they cannot explain why it is cruel but that they can 'feel that it is cruel' (citing Dorsey Ellis, Vox Populi v Suprema Lex: A Comment on the Testimonial Privilege of the Fifth Amendment' (1970) 55 *Iowa Law Review* 829, 838.

Despite the existence of the many rationales identified above, there is disagreement over whether any of them offer a satisfactory explanation for the privilege.[35] Indeed, it has been said of the privilege that 'it is difficult, if not impossible, to provide a compelling rationale for the privilege'.[36] As the rationale for the privilege remains disputed, this thesis does not ask whether compelled production orders are consistent with one of those disputed rationales; rather, it asks if the scope of the privilege encompasses compelled production orders. For the purposes of this thesis, then, the outer boundaries of the privilege are drawn not from a contested rationale for it, but from court decisions that are concerned with the application of the privilege to circumstances that share similarities with the compelled production of a password.[37] Such circumstances, which in this thesis are termed related orders, include the taking of bodily samples (such as fingerprints and blood samples); the use of the body to provide evidence (by, for example, requiring a suspect to provide a handwriting or voice sample) and the imposition of an obligation on the owner of a motor vehicle to identify who was driving the vehicle at the time that it was involved in a traffic infringement.

By analysing those related orders, it is possible to determine not only what the outer boundaries of the privilege are, but also what factors previous courts considered in determining those boundaries. Understanding the relevant considerations behind those decisions enables two things to be done. First, where the courts of a jurisdiction have granted a compelled production order, it is possible to assess whether the reasons behind that decision are, where relevant, consistent with the reasons that were relied

---

35 See, eg, Allen and Mace, above n 26, 245; William J Stuntz, Self-Incrimination and Excuse' (1988) 88 *Columbia Law Review* 1227, 1228 (where the author notes the existence of a general belief that the privilege 'cannot be squared with any rational theory' and that the explanations that have been provided 'have serious, if not insurmountable, problems'); Akhil Reed Amar and Renee B Lettow, 'Fifth Amendment, First Principles: The Self-Incrimination Clause' (1995) 93 *Michigan Law Review* 857, 857 (where the privilege is described as an 'unsolved riddle of vast proportions); Dolinko, above n 29, 1065-67 (where he argues that none of the rationales yet advanced to explain the privilege are adequate); Hamish Stewart, 'The Privilege against Self-Incrimination: Reconsidering Redmayne's Rethinking' (2016) 20(2) *The International Journal of Evidence and Proof* 95, 95 ('A persuasive rationale for the privilege against self-incrimination is elusive'); Green, above n 29, 628; Dennis, above n 28, 347.

36 Mike Redmayne, 'Rethinking the Privilege against Self-Incrimination' (2007) 27(2) *Oxford Journal of Legal Studies* 209, 210.

37 See, in this respect, R H Helmholz, 'Origins of the Privilege against Self-Incrimination: The Role of the European Ius Commune' (1990) 65 *New York University Law Review* 962, 963 where the author states that the privilege's past remains relevant to modern questions involving its scope.

upon when related orders were sought. Secondly, where, as is the case with the use of biometrics in Australia, no decision has to date been handed down on a specific issue, the reasons behind the related orders can be referred to for guidance on how courts will resolve this issue when it first arises in Australia.

This process is assisted by the use of comparative analysis. Each of the United States, Canada and England share a common law heritage, which has long recognised the privilege.[38] How courts in those jurisdictions have determined the outer boundaries of the privilege in respect of related orders and what they have held in respect of compelled production orders may be of assistance to Australian courts. For example, both England and Wales and the enacting Australian jurisdictions have introduced legislative measures providing for compelled production orders.[39] The provisions of the English statute and how courts have interpreted them may provide some guidance to Australia, both in terms of the content of the respective statutes and the interpretation of them. Furthermore, only the United States and Canada have reported cases involving decryption with biometrics. It may assist an Australian court considering this issue for the first time to understand how comparative jurisdictions have dealt with the issue.

While this thesis is concerned with how compelled production orders and the privilege interact, in one circumstance – when considering the role of alternative encryption workarounds – the role of the right to privacy is also relevant. It is helpful to understand why it is in just that one circumstance that the right to privacy is relevant. The right to privacy protects interests including bodily privacy, informational privacy and psychological integrity.[40] Relevantly, the right to privacy operates when a search is conducted by law enforcement.[41] In Australia, the right to privacy receives statutory but

---

38 Note, however, that each of these three jurisdictions has subsequently given constitutional or statutory recognition to the privilege, and the development of the privilege in those jurisdictions has some differences which are explored in this thesis, particularly in Chapters 1 and 2. Australia remains the sole jurisdiction in which the protections afforded by the privilege are found in the common law (with the exception of Victoria, the Australian Capital Territory and Queensland).

39 Not every Australian jurisdiction has a statute providing for compelled production orders. The Australian jurisdictions with such a statute are termed enacting jurisdictions in this thesis.

40 Jeremy Gans et al, *Criminal Process and Human Rights* (Federation Press, 2011), 301. See also *Pretty v United Kingdom* (2002) 35 EHRR 1; *Ivashchenko v Russia* (2018) 67 EHRR 20.

41 Gans et al, above n 37, 301.

not constitutional protection. In the United States and Canada, the right to privacy is incorporated in the protections against unreasonable search and seizure which are provided in the Fourth Amendment of the Constitution of the United States and s 8 of the *Canadian Charter of Rights and Freedom*[42] ('*Canadian Charter*') respectively. Importantly, the right to privacy is subject to lawful interference. Thus, Article 8 of the *European Convention on Human Rights* ('*ECHR*') speaks of how the right to privacy is subject to such interference as 'is in accordance with the law…'; in Victoria, the *Charter of Human Rights and Responsibility 2006* (Vic) ('*Victorian Charter*') states that a person shall not have their right to privacy 'unlawfully or arbitrarily interfered with'; and the *Canadian Charter* and the Fourth Amendment speak of 'unreasonable' searches and seizures. Thus, each of those provisions recognise that where the right to privacy is engaged, a search will remain lawful where it is authorised by law and is executed in a reasonable manner (or, in respect of England and Wales, in a manner that is proportionate and necessary in the interests of one of the aims identified in Article 8 of the *ECHR*).[43]

In the context of a compelled production order, in each of the jurisdictions under examination the order to compel a person to provide a password is made by a court after finding that law enforcement officials have a right to search the electronic device in question.[44] At that point in the process, the right to privacy does not – with one exception to be discussed below – provide a basis on which a court can refuse to grant a compelled production order, though it can operate to circumscribe the scope of the search to ensure that it is not overly broad and to regulate the manner in which the search is conducted.[45] The privilege, however, can provide a basis for refusing to make such an order, and has been successfully relied upon to prevent such orders being made.

---

42 *Canada Act 1982* c 11, sch B pt I.

43 See, eg, Ben Emerson et al, *Human Rights and Criminal Justice* (Sweet & Maxwell, 3rd ed, 2012), 311.

44 There are some exceptions to this under the English legislation, which will be discussed in Chapter 4.

45 See, for example, *Niemietz v Germany* (1993) 16 EHRR 97.

This position was set out clearly by the Supreme Court of the United States when, in respect of warrantless searches of a smartphone as an incident of arrest, it stated that 'our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest'.[46] Thus while the right to privacy operates to regulate the manner in which a search is conducted, including by requiring prior authorisation and thereafter regulating the scope and execution of the search, once those requirements are met the right to privacy is no longer a bar to the carrying out of that search. In contrast, it is precisely at this stage of the proceeding, when the search warrant has been issued and an order is sought compelling the suspect to provide the password, that the privilege potentially comes into play as a shield against the operation of such an order.

As noted above, however, there is, at least regarding England and Wales and Australia, one exception to the limited role played by the right to privacy in preventing the issuing of a compelled production order. In those two jurisdictions, compelled production orders can only be made where they satisfy the proportionality principle, which requires that there be no alternative means of obtaining the encrypted material which imposes a lesser infringement on the rights of the suspect. The determination of whether an alternative means of obtaining the material is less intrusive involves, amongst other things, weighing the impact on the right to privacy caused by compelled production orders against that caused by the alternative workarounds. It is only in this limited circumstance, therefore, that the right to privacy is considered in this thesis.

The concern of this thesis, then, is with the privilege against self-incrimination; the question of whether compelled production orders fall within its scope; and how the four jurisdictions have dealt with this issue. The right to privacy only arises for consideration in the limited circumstance described above. In the section below, chapter outlines for the five substantive chapters in this thesis are provided. Those outlines will explain how each chapter relates to the research questions.

---

46 *Riley v California* 134 S Ct 2473, 2493 (2014).

CHAPTER OUTLINES

This thesis comprises five chapters excluding this Introduction and the Conclusion. Chapter 1 identifies the scope of the privilege in the four jurisdictions. It considers how the privilege has evolved and how it applies to scenarios closely related to the compelled production of a password, including compelling bodily evidence (such as fingerprints and breathalyser samples) and statutory obligations to provide details of the driver of a motor vehicle that has been involved in a traffic violation. By analysing how courts have treated the privilege in respect of these related orders, it is possible to determine the scope of the privilege, a necessary precursor to understanding whether the compelled production of an encryption key fits within its borders. This analysis includes an assessment of how courts, in determining whether a particular act of compulsion by the state has infringed the privilege, have balanced the individual's right to the privilege against society's interest in the prosecution of criminal conduct. How those determinations have been made has been a key factor in identifying the boundaries of the privilege.

Finding that an order violates the privilege is not the only issue, however, as in each of the examined jurisdictions the privilege can be abrogated. Chapter 2 examines the circumstances in which such abrogation can occur. Abrogation of the privilege occurs when the privilege is no longer applied to a particular circumstance to which it previously applied. For example, the privilege protects a suspect from having to answer incriminating questions asked by the police. If a statute is passed requiring suspects to answer questions – even if the answers are incriminating – when asked by a police officer above a certain rank, the privilege has been abrogated in respect of questions asked by such an officer. Two critical issues arise with respect to the issue of abrogation. First, it is necessary to determine whether abrogation must be accompanied by a grant of immunity and, if so, the extent of such immunity (if any). Secondly, it is necessary to fully understand what is meant by abrogation. With regard to the first issue, Chapter 2 will show that in England and Wales and Australia abrogation can occur without a commensurate grant of immunity. The effect of this is that searches that would ordinarily be prohibited as a result of the privilege can now be performed. That outcome

is critical to the ability of English and Australian courts to compel the production of a password. With regards to the second issue, the case analysis in Chapter 2 also lays the foundation for further discussion of the meaning of abrogation, which occurs in greater detail in Chapter 5. This thesis will suggest in Chapter 5 that abrogation can be conceptualised in one of two ways. First, the act of abrogation can be understood to alter the boundaries of the privilege so that an act previously within the scope of the privilege now falls outside its borders; alternatively, the privilege can be understood not to alter the borders of the privilege but to hold that in a particular circumstance the privilege will not apply to a specific act notwithstanding that the act falls within the scope of the privilege. In the latter scenario the operation of the privilege is simply held in abeyance. The distinction between those conceptions, and the reasons for preferring the former to the latter, are discussed in Chapter 5 in the context of alternative workarounds. It is there argued that the existence of the alternative workarounds cause the scope of the privilege to expand or contract depending on the circumstances. That outcome is only possible under the first conception of abrogation outlined above.[47] Whether evidence obtained in breach of the privilege is inadmissible in court proceedings is also considered in Chapter 2.

Chapter 3 reviews the United States and Canadian cases on the compelled production of an encryption key and analyses whether those decisions remain consistent with the scope of the privilege as determined in Chapter 1. A key aspect of this analysis concerns the evidentiary burdens required to be satisfied before a compelled production order can be granted. In particular, the burdens imposed concerning the suspect's knowledge of the encryption key and the applicant's knowledge of the contents of the encrypted device are the focal point of judicial decisions on compelled production orders. Chapter 3 also considers the role of the privilege when an encrypted device can be unlocked with a fingerprint and an order is sought compelling a person to unlock that device in that manner. As will there be discussed, most of the case law on this issue holds that

[47] The reasons for this discussion occurring in Chapter 5 and not Chapter 2 is that Chapter 2 is concerned with the availability of abrogation and the circumstances in which it can take place. The precise mechanism by which it occurs is not relevant in that Chapter. The importance of the competing conceptions for abrogation only arises in Chapter 5 in the context of the alternative encryption workarounds and what they mean for the scope of the privilege.

decrypting a device with a biometric password does not fall within the scope of the privilege. The analysis in Chapter 3 will allow one to assess whether the United States and Canadian cases have been resolved consistently with the outcomes identified in Chapter 1; it will also enable comparisons to be made in Chapter 4 with the position that has been adopted in England and Wales and Australia in respect of alphabetic and numeric passwords.

Having, for purposes of comparative analysis, examined in Chapter 3 how the courts of Canada and the United States have responded to requests to compel the production of a password, Chapter 4 examines how Australia and England and Wales are responding to the same issue. Unlike Canada and the United States, both Australia and England and Wales have enacted statutory provisions enabling the granting of an order compelling a suspect to provide the password to an encrypted device.[48] In Australia, the legislation exists at a federal level and in some, though not all, states. As the legislation in the enacting Australian states and England and Wales is broadly similar, and the issues they raise the same, they are analysed together. This Chapter commences by briefly describing the relevant principles of statutory interpretation that will be utilised in analysing the respective statutes, before considering whether compelled production orders implicate the privilege. The latter question is relevant because if compelled production orders do implicate the privilege, statutes authorising compelled production orders will need to abrogate it. After concluding that in both jurisdictions compelled production orders requiring the production of an alphabetic or numeric password do engage the privilege, the Chapter proceeds to consider how the privilege has been abrogated to allow such orders to be made. Thereafter, the Chapter examines the evidentiary burdens imposed by the statutes regarding knowledge of the password and knowledge of the contents of the encrypted device. How those provisions have been interpreted by the courts is also analysed, and comparisons drawn to the approach adopted in Canada and the United States to those same evidentiary burdens.

---

[48] In the United States, no legislative response was required as the scope of the *All Writs Act 1789* 28 USC § 1651 is sufficient to obtain an order compelling the production of a password.

An important feature of the English statute is how its provisions interact with the *Human Rights Act 1998*, and specifically the protections afforded by it to the privilege. The *Human Rights Act 1998* incorporates into English law the provisions of the *ECHR*. Judicial decisions on this question are analysed. In Australia, Victoria (one of the states that has provided a power to compel the production of a password) has a human rights statute – the *Victorian Charter*. Though no judicial decision directly addresses whether the provisions of the Victorian statute comply with the requirements in the *Victorian Charter*, the *Victorian Charter* requirements are analysed to determine whether the Victorian statute is likely to comply with those requirements. Lastly, as England and Wales and Victoria have reached a different conclusion on this issue to that arrived at in Canada – where the *Canadian Charter* also recognises the privilege – the reasons for that difference are examined.

The final substantive chapter, Chapter 5, considers alternative encryption workarounds that may enable law enforcement officials to gain access to encrypted material. The use of such workarounds, which are described in the Chapter, has been facilitated in England and Wales and Australia through new statutory powers authorising their use. The significance of their availability as an alternative to a compelled production order is that the English and Australian statutes require compelled production orders to be a proportionate response before such an order can be made. For compelled production orders to be a proportionate response there must be no alternative, less intrusive means of accessing the encrypted material in an unencrypted form. This Chapter considers whether those alternative encryption workarounds satisfy those two requirements, of being equally effective and less intrusive.

The answer, it will conclude, is that the specific circumstances of each matter will play a role in determining whether the proportionate response is to use a compelled production order or one of the alternative workarounds, though it is possible that in certain circumstances compelled production orders will not be a proportionate measure. From that conclusion it will be argued that because law enforcement's ability to satisfy the requirements of the compelled production order legislation may depend on the availability or otherwise of a less intrusive alternative workaround, the scope of

the privilege expands and contracts depending on the availability of those workarounds. This is because where an alternative encryption workaround is available, the privilege is given its full scope to preclude the use of a compelled production order; where, however, no such alternative is available, the scope of the privilege is limited to enable a compelled production order to be made.

By operating in this fluid manner, the privilege demonstrates the pragmatic way in which it responds to potential infringements. This vein of pragmatism has run through the privilege from its earliest decisions, as evidenced in the cases discussed in Chapter 1. Those decisions recognise that notwithstanding the importance of the privilege, there will be occasions when the public interest requires some curtailment of its scope. In the case of compelled production orders, the use of less intrusive alternative workarounds – where they are available – can ensure that the scope of the privilege is always given the broadest possible remit while still accounting for the public interest.

The thesis concludes by finding that, depending on the circumstances, the privilege does not bar the granting of compelled production orders, not only in the enacting Australian jurisdictions but also in England and Wales and the United States. Canada is the sole jurisdiction of the four examined to have found the privilege to be a bar to such an order being made, though that finding is also, at least in part, a consequence of the related finding that there is no clear statutory power authorising the making of such orders. Those outcomes are consistent with how the privilege has been treated in each of the jurisdictions in respect of the related orders. They are, furthermore, consistent with an understanding that while the privilege is a long-standing and valued right in each of the four jurisdictions, it is at times a flexible right, one that may bend to the demands of the public interest where the injury caused to the privilege by the act in question is not too severe. Ultimately, with the increasing availability of alternative workarounds that may be less intrusive, compelled production orders will only remain compliant with the requirements of the privilege in those instances where they remain a proportionate response to the problem of encrypted material.

DEVELOPMENTS DURING THE WRITING OF THE THESIS

Whether a password can be compelled is a still evolving question, one that has yet to be determined by the highest court of any of the jurisdictions under examination. For that reason, and in the United States in particular, new cases continue to arise with regularity while formal determination of this question awaits. As it is not possible to address each new case that arose during the writing of this thesis, particularly as no decisions of a higher court arose during the final months of the thesis, with two exceptions – to be discussed below – decisions that were handed down after 1 November 2018 have not been considered.

In Australia, there has been both judicial and legislative activity during the final months of this thesis. In December 2018, the federal government passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ('*Assistance and Access Act*'), which authorises new alternatives to compelled production orders while simultaneously strengthening the existing powers to compel the production of a password. On 8 November 2018, the South Australian government introduced the Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2018, which amends the earlier Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 that was introduced by the previous government but never passed by the Legislative Council. In July 2019, that Bill was passed as the *Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019* (SA). Given the late date at which that Bill was introduced and passed, it has not been considered in detail. Where appropriate, however, parts of it have been discussed. On the judicial front, in late December 2018 a decision of the Federal Court, *Luppino v Fisher*,[49] was handed down which addressed the ability of law enforcement to compel a person to provide a password through means other than the specific statutory provisions adopted in the enacting Australian states to authorise compelled production orders. That decision is discussed in Chapter 4, as is the subsequent decision, *Luppino v Fisher (No 2)*,[50] handed down in July 2019.

---

49 [2018] FCA 2106 ('*Luppino (No 1)*').

50 [2019] FCA 1100 ('*Luppino (No 2)*').

Lastly, academic writing on this issue continues to grow, most notably in the United States. Where possible, relevant recent articles have been included in this thesis, including at least two by Orin Kerr. The most recent of his articles covers much of the same ground as this thesis, though only in respect of the United States' position.[51]

[51] The title of his article alone demonstrates the similarity with my thesis question: Orin Kerr, 'Compelled Decryption and the Privilege against Self-Incrimination' (2019) 97 *Texas Law Review* 767.

CHAPTER 1

THE SCOPE OF THE PRIVILEGE

1.1 INTRODUCTION

As set out in the Introduction, this thesis seeks to determine whether the privilege applies to compelled production orders. To answer that question, it will identify the scope of the privilege and analyse whether compelled production orders fall within that scope. The scope of the privilege, for purposes of this thesis, is the outer boundary of the privilege as determined by judicial decision-making when considering related orders. It is this issue – how courts have applied the privilege to related orders – that is the concern of this Chapter. Chapter 1 will therefore stand as the foundation on which Chapters 3 and 4 will be built, and it is in those Chapters 3 and 4 that cases concerning compelled production orders will be examined to analyse how the courts have dealt with those cases and whether the manner in which they have done so is consistent with the cases considered in this Chapter. That analysis will also reveal the differences that exist between the respective jurisdictions, which will assist in identifying what lessons, if any, Australia can draw from the comparator jurisdictions.

Understanding the scope of the privilege is important for a further reason: depending on whether compelled production orders fall within the scope of the privilege, the privilege may need to be abrogated to enable courts to grant such orders. This is an important issue because, as is discussed in Chapter 4, both England and Wales and Australia abrogate the privilege as part of legislative measures authorising the granting of compelled production orders. The manner in which that abrogation occurs is also relevant to Chapter 5 and the availability of alternative encryption workarounds because, as will be argued in that Chapter, the terms on which the abrogation occurs may have the effect of altering the scope of the privilege depending on the availability of such workarounds. Due to the important role played by abrogation, once the scope of the privilege has been determined in this Chapter, and before considering how the jurisdictions have dealt with compelled production orders in Chapters 3 and 4, Chapter 2 will consider the question of abrogation in each of the jurisdictions. It will examine

whether abrogation is permitted; if so, the terms on which it is permitted; and the circumstances under which evidence that has been obtained in breach of the privilege may be admissible in court proceedings.

Before then, Part 1.2 will consider what the related orders reveal about the scope of the privilege in the four jurisdictions. Those related orders include bodily samples (such as blood and breath samples), physical actions such as providing a writing sample, and single question reporting obligations such as motor vehicle reporting obligations that require the registered owner of a motor vehicle to provide the details of the driver of that vehicle at the time the vehicle was involved in a traffic violation. These orders feature elements that are similar to compelled production orders. For example, motor vehicle reporting obligations require the registered owner to answer one question, the answer to which may result in his or her prosecution for an offence. Compelled production orders are similarly restricted to asking only one question of the suspect, the answer to which is intended to lead to evidence that will be used against that same person. Where access to the encrypted device is sought using a biometric key, such as a fingerprint scanner, how courts have previously applied the privilege to bodily samples is relevant. The differences and similarities between the jurisdictions when considering these orders will be identified, including the role played by the act of production and foregone conclusion doctrines in the United States and the greater scope that Canada gives to the privilege than do the other jurisdictions.

Part 1.3 will then analyse the role that the weighing of competing interests has played in determining the scope of the privilege. As will there be discussed, in each jurisdiction courts have weighed the individual's right to rely on the privilege against society's interest in the investigation and prosecution of criminal offences, a process that has at times resulted in different outcomes between the jurisdictions. Finally, Part 1.4 provides a recapitulation of the findings in this Chapter. Those findings include identifying: a common understanding between the jurisdictions that the privilege is not absolute and can be limited in appropriate circumstances; that each of the four jurisdictions refer to common factors when determining whether to limit the privilege, factors that include the strength of the public interest and the extent of the infringement; and that while

Australia, England and Wales and the United States have achieved broadly similar outcomes in those weighing exercises, in Canada that weighing exercise has resulted in the privilege being given a broader scope than the other jurisdictions.

Considered first, in Part 1.2, is what the related orders reveal about the scope of the privilege in the four jurisdictions.

1.2 DETERMINING THE EDGES OF THE PRIVILEGE

In each of the four jurisdictions, the privilege applies to evidence that is compelled, incriminating and testimonial. The first two of those elements are relatively uncontroversial; it is the third element, the requirement that evidence be testimonial, that has been the decisive element in determining the outer parameters of the privilege. Accordingly, Part 1.2 below analyses how each of the four jurisdictions have determined whether the evidence that was sought in relation to the similar orders was testimonial.

1.2.1 The United States' approach to testimonial evidence

The privilege is protected in the United States through the Fifth Amendment to the Constitution of the United States, which provides that 'no person…shall be compelled in any criminal case to be a witness against himself'. Any analysis of the scope of the Fifth Amendment begins with the decision in *Boyd v United States*.[1] The case concerned a subpoena given to the appellant directing him to produce to the Court any documents or invoices containing details of the importation of plate glass from England. Those documents were intended to be used against Boyd in criminal proceedings.[2] Bradley J, writing for the majority,[3] held that such compulsion breached the Fifth Amendment as it compelled Boyd 'to furnish evidence against himself'.[4] In the years since the *Boyd* decision, there has been a move away from the broad interpretation it utilised, a change that is in part attributable to the evolving distinction between 'testimonial' and 'non-testimonial' evidence.

---

1 116 US 616 (1886) ('*Boyd*').

2 Ibid 617–8.

3 Miller J wrote a concurring opinion, with which Waite J joined.

4 *Boyd* 116 US 616, 634–5 (1886). At 637 Bradley J speaks of how requiring a person to provide his private papers involves 'compelling him to furnish evidence against himself'.

In *Holt v United States*,[5] the Supreme Court was asked to determine whether the Fifth Amendment was enlivened by compelling the defendant to try on a blouse that was believed to belong to him. The Court concluded that it was not, holding that the Fifth Amendment was intended to prohibit

> the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material. The objection in principle would forbid a jury to look at a prisoner and compare his features with a photograph in proof.[6]

This decision, drawing a distinction between communications and real evidence (in this instance, the accused's body), stands as the first step in developing the testimonial requirement for the privilege.

That the privilege does not extend to the use of the body as evidence was further confirmed when the Supreme Court held that the privilege did not prevent a person from giving a blood sample for purposes of determining if that person had been driving while under the influence of alcohol. Brennan J, who delivered the Court's opinion in *Schmerber v California*,[7] accepted that compulsion was present in the requirement that the accused submit to the blood sample withdrawal. The main question, however, was whether that compulsion required the accused to be a witness against himself.[8] Brennan J found that it did not, writing that:

> We hold that the privilege protects only an accused from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to those ends.[9]

---

5 218 US 245 (1910).

6 Ibid 252–3. This statement was identified by Marshall J in *United States v Mara* 410 US 19 (1973) at 35 as the beginning of the Court's shift towards limiting the privilege to testimonial evidence.

7 384 US 757, 761 (1966) ('*Schmerber*').

8 Ibid 761.

9 Ibid 761. Brennan J further noted that 'the privilege has never been given the full scope which the values it helps to protect suggest': at 762. See also *Breithaupt v Abram* 352 US 432 (1957) in which the Court held that it was permissible to draw a blood sample from an unconscious driver where the assessment of a police officer at the scene that the unconscious driver was under the influence of alcohol was justified.

Brennan J further noted that, because the privilege was not concerned with compulsion in respect of 'real or physical evidence', there was no 'testimonial compulsion upon or enforced communication by the accused' and that his only participation in the drawing of his blood was as a donor.[10] The finding that physical or real evidence did not infringe the privilege is, as will be discussed in Chapter 3, particularly important for the question of whether the privilege is infringed by a requirement to unlock an encrypted device through the use of a fingerprint or other biometric feature.

The *Schmerber* decision was followed by findings that neither voice exemplars[11] nor handwriting exemplars[12] fall within the scope of the privilege as neither entails the provision of information of a testimonial or communicative nature.[13] In respect of voice exemplars, Brennan J, delivering the opinion of the Court in *Wade*, found that a voice exemplar is used to identify a physical characteristic as opposed to requiring a suspect to 'speak his guilt' as the exemplar 'did not require him to disclose any knowledge that he might have'.[14] Brennan J, delivering the Court's opinion in *Gilbert* on handwriting exemplars, noted that the exemplar itself, 'in contrast to the content of what is written', was an 'identifying physical characteristic' outside the protection of the privilege.[15]

Each of *Schmerber*, *Dionisio*, *Mara*, *Wade* and *Gilbert*, however, contained strong dissents concerning the definition of testimonial and non-testimonial evidence. Those dissents raised three main objections. The first concerned the meaning of the concept of testimonial evidence and its role in the interpretation of the Fifth Amendment. Black J, in *Schmerber*, argued that blood that had been extracted for testing had 'both a

---

10 *Schmerber* 384 US 757, 764-65 (1966).

11 *United States v Wade* 388 US 218, 222 (1967) (Brennan J) ('*Wade*'); *United States v Dionisio* 410 US 1 (1973) ('*Dionisio*').

12 *Gilbert v California* 388 US 263, 266–7 (1967) (Brennan J) ('*Gilbert*'); *United States v Mara* 410 US 19 (1973) ('*Mara*').

13 Findings that once more received strong dissents from Warren CJ, Black, Fortas and Douglass JJ in *Wade*, and Black and Douglass JJ in *Gilbert*. In *Wade*, Black J argued that the privilege was designed to 'bar the Government from forcing any person to supply proof of his own crime': *Wade* 388 US 218, 245 (1967) (Black J). Fortas J spoke of how the privilege allows an accused to 'stand mute' (*Wade* 388 US 218, 260 (1967)) and that requiring a voice exemplar involved 'compulsion of the will of a man': *Wade* 388 US 218, 262 (1967).

14 *Wade* 388 US 218, 222 (1967).

15 *Gilbert* 388 US 263, 266–7 (1967).

"testimonial" and "communicative" nature' as 'the sole purpose…was to obtain "testimony" from some person to prove the petitioner had alcohol in his blood at the time he was arrested'.[16] He further expressed his discomfort at the importance placed on the words 'testimonial' and 'communicative' as they were susceptible to competing interpretations.[17] Black J concluded his opinion by calling for a 'broad and liberal construction' to be applied to the Fifth Amendment in accordance with existing case law, including the decision in *Boyd*.[18]

The second objection to this line of authority arose out of the handwriting and voice exemplar cases. In *Gilbert*, Fortas J distinguished *Schmerber* on the basis that a handwriting exemplar could not be obtained if the suspect was physically restrained – as is possible when blood is drawn – for it required a positive act by the suspect.[19] The accused's participation was no longer limited to that of a mere donor. In *Mara*, Marshall J wrote in dissent that the privilege was engaged in instances where a suspect was required to 'cooperate affirmatively' in order for the investigating officers to obtain the evidence sought.[20]

The third objection concerned the effect of the compulsion on the accused. Fortas J in *Wade* spoke of how compelling a person to provide a voice exemplar involved the 'compulsion of the will of a man'.[21] In a similar vein, Marshall J in *Mara* spoke of how

---

16 *Schmerber* 384 US 757, 774 (1966).

17 Ibid 774. Marshall J raised a similar objection by arguing in dissent in two subsequent cases that the language of the Fifth Amendment did not support restricting the privilege to only that evidence which was deemed to be testimonial: *United States v Dionisio* 410 US 1, 33 (1973); *Mara* 410 US 19, 34 (1973).

18 *Schmerber* 384 US 757, 776 (1966). Black J was to repeat his call for a liberal interpretation to be applied to the Fifth Amendment in *Gilbert* 388 US 263, 277–78 (1967) where he said that the Court's decision 'wholly unjustifiably detracts from the protection against compelled self-incrimination the Fifth Amendment was designed to afford'. See also *Gouled v United States* 255 US 298, 304 (1921) where it was said by Clarke J, who delivered the opinion of the Court, that the Fifth Amendment 'should receive a liberal construction, so as to prevent stealthy encroachment upon or "gradual depreciation" of the rights secured by [it], by imperceptible practice of courts or be well-intentioned, but mistakenly overzealous executive officers'.

19 *Gilbert* 388 US 263, 291 (1967). Fortas J raised the same objection in relation to voice exemplars: *Wade* 388 US 218, 260–61 (1967).

20 *Mara* 410 US 19, 33 (1973). See also *Dionisio* 410 US 1, 33 (1973) where Black J said that the privilege should apply in any instance in which a person had been compelled 'to cooperate affirmatively in securing incriminating evidence when that evidence could not be obtained without the cooperation of the accused'.

21 *Wade* 388 US 218, 262 (1967).

the taking of blood tests or the placing of a blouse on a suspect does not 'involve the sort of interference with an individual's personality and will that the Fifth Amendment was intended to prevent', an interference that does occur when a suspect is required to give a voice or handwriting exemplar.[22]

By the time the Supreme Court handed down its 1988 decision in *Doe v United States*, the majority of the Court had a response to the first two objections. Doe sought to resist a court order compelling him to instruct foreign banks to provide details of any accounts held by him with those banks. The order was worded so that no specific banks were identified, and Doe was not required to acknowledge that he held an account with the bank in question. Rather, the document was drafted in the hypothetical and instructed any bank 'at which I may have a bank account' to provide details of the account to the Grand Jury.[23] Blackmun J, delivering the Court's opinion, held that the order did not breach the privilege.[24]

Referring to two of the Court's earlier decisions, Blackmun J held that for a communication to be testimonial, it 'must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a "witness" against himself'.[25] This was because historically the privilege 'was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him'.[26] It was the absence of that element which meant that giving blood samples and voice and hand writing exemplars did not require a person to 'disclose any knowledge he might have, or to speak his guilt'.[27] By signing the statement

---

22 *Dionisio* 410 US 37 (1973).

23 *Doe v United States* 487 US 201, 205 (1988) ('*Doe II*'). The abbreviation *Doe II* is used because of the earlier case of *United States v Doe* 465 US 605 (1984), which also concerned the Fifth Amendment.

24 The wording of the order was critical in achieving this outcome, as the wording spoke only in the hypothetical; did not refer to a specific account; and by signing a document with that wording the accused did not therefore acknowledge the existence of a foreign bank account at the institution to whom the document was provided: *Doe II* 487 US 201, 215 (1988).

25 Ibid 210. Stated differently, '[t]he content itself must have testimonial significance' (at 211, fn 10).

26 Ibid 212. At 213, Blackmun J spoke of how the privilege 'is asserted to spare the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government'.

27 Ibid 211.

Doe was not compelled to communicate facts that related a factual assertion or disclosed information that was in itself incriminating, and therefore the communication lacked a testimonial element.[28]

Doe II is significant for present purposes for one further reason. In seeking to explain the distinction between communications that expressed the contents of one's mind – which were testimonial – and those that did not, Blackmun J, referring to an example given by Stevens J in his dissenting opinion in *Doe II*, discussed the example of the key to a safe. Where the safe in question required a physical key, compulsion to produce that key did not implicate the privilege as it did not require the suspect to reveal the contents of his or her mind. By contrast, where the safe contained a combination lock that required the entry of a code, the act of revealing that code was testimonial and therefore protected by the privilege.[29]

In *Pennsylvania v Muniz* the Supreme Court provided further guidance on how to determine whether a communication was testimonial. After being stopped while driving his motor vehicle, Muniz was instructed to perform a field sobriety test. He was unable to satisfactorily perform the test, during which he made repeated statements while slurring his words. He also failed to calculate the date on which he turned six years old. Brennan J, delivering the Court's opinion in respect of the slurred responses, held that that 'slurring of speech and other evidence of lack of muscular coordination' revealed in responses to direct questions did not constitute testimonial evidence.[30]

To reach this conclusion, Brennan J held that testimonial evidence, as defined in *Doe II*, includes responses to all questions that place the accused in the cruel trilemma,[31] which will be the case whenever a question requires an answer that will 'convey information or assert facts'.[32] The cruel trilemma, as discussed in the Introduction, arises whenever

---

28 Ibid 215.

29 Ibid 210, 219. See also *United States v Hubbell* 530 US 27, 43 (2000); *United States v Green* 272 F 3d 748, 753 (5th Cir, 2001).

30 *Pennsylvania v Muniz* 496 US 582, 592 (1990) ('*Muniz*').

31 Ibid 597. See the discussion of cruel trilemma in the Introduction.

32 Ibid 597.

a suspect is asked a question the answer to which is incriminating. In that circumstance, the suspect can answer truthfully, and self-incriminate; lie, and commit perjury if the lie is told in court; or refuse to answer and risk contempt of court. This Regarding the slurred statements, they were akin to a physical characteristic, one which did not require Muniz to reveal the contents of his mind.[33] In a sign of how the Court's approach to the privilege had developed, all but one of the Court's justices concurred in this finding. Notably, however, Brennan J found that Muniz's failure to calculate the date on which he turned six years old constituted a testimonial communication that infringed the privilege.[34] This was because when Muniz was unable to calculate the date, he faced the cruel trilemma: silence would be incriminating and an honest answer would lead to the inference that he was intoxicated, as would the wrong answer.[35]

Though no explicit response has been given by the courts to the argument that a voice exemplar involves the compulsion of a person's will and an interference with his or her personality, there is a response that can be given to it: neither compelling a person's will nor interfering with that person's personality constitutes a breach of the privilege. The taking of a blood sample will ordinarily be against the suspect's wishes and as such in defiance of his or her will, yet it does not infringe the privilege. It is an instance of compulsion, but compulsion alone is insufficient to establish a breach of the privilege. While the voice exemplar requires an affirmative act by the suspect, that alone does not make it an act in breach of the privilege as it is not an act requiring the suspect to disclose knowledge or speak his or her guilt. The requirements of compulsion and incrimination are satisfied, but not testimony.

As for the assertion that providing a voice exemplar interferes with one's personality, it is not entirely clear what is meant by that assertion. It cannot be the element of compulsion that interferes with a suspect's personality, or such interference would occur with blood samples and fingerprints too. Likewise, the suspect does not disclose

---

33 Ibid 598. This finding was consistent with earlier statements by the Brennan J that the privilege was intended to prevent a recurrence of the Star Chamber.

34 Ibid 598.

35 Ibid 599.

any of his or her knowledge while providing the voice exemplar, so his or her personality cannot be interfered with for that reason. The complaint only makes sense if the compulsion to make an affirmative, prima facie non-testimonial act in some way impinges on a person's personality in a way that a non-affirmative act does not, in so doing rendering that affirmative act a testimonial act. No explanation has been offered for how this distinction might arise or how a non-testimonial act is rendered testimonial by virtue alone of the compulsion of an affirmative act, and no obvious explanation presents itself. In any event, even if such a distinction could be drawn, interfering with one's personality has never been held to constitute a breach of the Fifth Amendment.

1.2.1.1 The act of production and forgone conclusion doctrines

There remains a further element of the evolution of the privilege to its present-day position in the United States that is essential to the issue of compelled production orders. In *Fisher v United States*,[36] a summons was served on Fisher's solicitor requiring him to produce specific documents, including documents prepared by Fisher's accountant that he (the accountant) had provided to Fisher, who had subsequently transferred those documents to the solicitor. White J, delivering the opinion of the Court, noted that the taxpayer's privilege against self-incrimination was not infringed by the compelled production by the solicitor of the identified documents.[37] After noting that 'several of Boyd's express or implied declarations have not stood the test of time',[38] the Court stated that the Fifth Amendment only applied when the accused was compelled to make an incriminating testimonial communication.[39] On the facts before it the Court held that the privilege was not engaged as Fisher was not required to give oral testimony, nor was he required to 'restate, repeat, or affirm the truth of the contents of the documents'.[40] Simply, the documents had been voluntarily prepared by someone other than Fisher and as such the privilege did not attach to them.[41]

---

36 425 US 391 (1976) ('*Fisher*').

37 Ibid 402.

38 Ibid 407.

39 Ibid 408, 409. But see the statements by Brennan J at 423 in which he rejects this analysis.

40 Ibid 409.

41 Ibid 409. See also at 397 where it was said that '[t]he Court has held repeatedly that the Fifth Amendment is limited to prohibiting the use of "physical or moral compulsion" exerted on the person asserting the privilege'.

However, the Court further held that independently of the content of a document, the act of producing a document can have a 'communicative aspect' if it 'concedes the existence of the papers demanded and their possession or control by the taxpayer'.[42] The act of production can also authenticate the evidence.[43] It is this last element that was said to be the basis for the privilege's application to documentary subpoenas.[44] Where any of those three elements is present, the act of producing a document may involve testimonial self-incrimination and would thus be protected by the privilege.[45] The Court further noted, however, that whether the act of production had a testimonial component would depend on the facts of each particular case.[46]

In particular, the act of production doctrine contains an exception for documents the production of which do not add to the sum of the state's knowledge because the state, independently of any information provided by the defendant, knows that the documents exist and are in the possession of the defendant,[47] and the state is able to establish the authenticity of the documents independently of information provided by the defendant.[48] In such instances the production of the documents is a matter of surrender, not testimony.[49] This exception is known as the foregone conclusion doctrine.

---

42 Ibid 410. See also *United States v Doe* 465 US 605, 614 (1984) where production of the documents was protected by the privilege as the respondent had not conceded the existence of the documents, as a result of which being compelled to produce them entailed admitting both their existence and the defendant's possession of them. It would also authenticate the documents.

43 *Fisher* 425 US 391, 410 (1976). For a discussion of this case and the act of production doctrine, see Phillip R Reitinger, 'Compelled Production of Plaintext and Keys' (1996) 1996 *The University of Chicago Legal Forum* 171, 180–186.

44 *Fisher* 425 US 391, 413 (1976) and the cases there cited.

45 Ibid 411. Marshall J and Brennan J in separate concurring decisions both rejected the act of production doctrine, stating that it was incompatible with previous decisions which held that the privilege lies in the content of the documents.

46 Ibid 410.

47 Ibid 411.

48 See *United States v Bright* 596 F 3d 683, 693 (9th Cir. 2010) as cited in Joshua A Engels, 'Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing' (2012) 33 *Whittier Law Review* 543, 563.

49 *Fisher* 425 US 391, 411 (1976) quoting *In re Harris* 221 US 274, 279 (1911).

On the facts in *Fisher*, the foregone conclusion doctrine was enlivened as the government knew that the documents existed, that they had been prepared by Fisher's accountant and that they were in Fisher's lawyer's possession.[50] The government was not relying on the 'truth-telling' of Fisher to prove the existence of the evidence in question nor Fisher's control of that evidence.[51] Furthermore, as Fisher had not prepared the documents himself he was not able to authenticate them, with the result that his act of production could not authenticate the documents.[52] There was therefore no testimonial component in producing the documents.

Importantly, the Court also discussed which acts by a suspect did not infringe the privilege because they were not testimonial. It noted that in refusing to extend the privilege to blood samples, the Court in *Schmerber* stated that '[s]ince the blood test evidence, although an incriminating product of compulsion, was neither petitioner's testimony nor evidence relating to some communicative act or writing by petitioner, it was not inadmissible on privilege grounds'.[53] It further observed that the giving of a handwriting exemplar albeit potentially incriminating and compelled was not 'sufficiently testimonial for purposes of the privilege'.[54] Those early pronouncements thus appeared to exclude physical evidence from the scope of the act of production doctrine, though it is to be noted that the Court in *Fisher* failed to explain what it meant by being insufficiently testimonial. While that wording leaves open the possibility that some physical evidence may be sufficiently testimonial to fall within the scope of the privilege, no guidance is given as to what sort of physical evidence might satisfy that requirement. More importantly, however, the decisions of the Supreme Court in respect of handwriting exemplars and other physical evidence such as voice exemplars do not talk in such qualified terms; instead, they are clear that such exemplars have no testimonial component.[55]

---

50 *Fisher* 425 US 391, 411 (1976).

51 Ibid 411. This meant that the government was not relying on contents of the accused's mind.

52 Ibid 413.

53 *Schmerber* 384 US 757, 765 (1966).

54 *Fisher* 425 US 391, 411 (1976).

55 See, eg, *Gilbert* 388 US 263, 265 (1967); *Wade* 388 US 218, 222-3 (1967).

Later decisions have clarified the scope of the act of production doctrine. In *Doe II*, a case in which the defendant objected to being compelled to sign a form authorising foreign banks at which he might hold funds to release details of those funds to the government,[56] the Supreme Court spoke of how the act of production will be testimonial where the defendant's communication 'explicitly or implicitly, relate[s] a factual assertion or disclose[s] information'.[57] Such will be the case where the act of production concedes the documents' existence; the defendant's possession or control of the documents; or the documents' authenticity in circumstances where the foregone conclusion doctrine is not satisfied. The Court further noted that it 'is the attempt to force him "to disclose the contents of his own mind"' that implicated the privilege.[58] Thus, in order for the act of production doctrine to be engaged, the act of production must itself have a testimonial element, and in order for it to have such an element the person producing the evidence must use the contents of his or her mind during that act of production. On the facts, the Court held that the act of signing the form was non-testimonial for reasons including that the government was not relying on Doe's 'truth-telling'.[59]

The act of production doctrine also applies where, because of the broad scope of a subpoena and the volume of documents required to be produced under it, a defendant is required to make 'extensive use of the content of his own mind' to identify the requisite documents, thereby rendering the act of production testimonial.[60] In *United States v Hubbell*,[61] Hubbell was being investigated for fraud and tax evasion. He was served with a subpoena demanding production of 11 categories of documents. The Court held that the privilege was implicated as the act of producing the documents was testimonial.[62] The subpoenas included a request for 'any and all documents reflecting,

---

56 The form did not require the defendant to acknowledge that he had an account at any of the banks in question, and copies of the form were sent to several banks without the government knowing if the defendant held an account with them or not.

57 *Doe II* 487 US 201, 210 (1988). In *United States v Hubbell* 530 US 27, 35 (2000), the Court spoke of communications that related 'either express or implied assertions of fact or belief'.

58 *Doe II* 487 US 201, 210 (1988). The Supreme Court made similar statements in its later decision in *United States v Hubbell* 530 US 27, 35 (2000).

59 *Doe II* 487 US 201, 215 (1988).

60 *United States v Hubbell* 530 US 27, 43 (2000).

61 530 US 27 (2000) ('*Hubbell*').

62 Ibid 41.

referring or relating to any direct or indirect sources of money or other things of value received by or provided to' Hubbell.[63] The breadth of that request was such that compliance with it was tantamount to providing a written response to a series of questions,[64] an action that required the accused to use 'the contents of his mind' to identify the documents requested.[65]

The *Hubbell* Court further found that the facts of the matter were 'plainly' outside the scope of the foregone conclusion doctrine as the government had 'not shown that it had any prior knowledge of either the existence or the whereabouts' of the documents.[66] In reaching this conclusion the Court held that it was insufficient for the government to argue that as the documents requested were ordinary business and tax records, 'a businessman such as the respondent will always possess [them]'.[67]

With this finding, the *Hubbell* Court did two things. First, it recognised that it was not the physical act of producing the documents that infringed the privilege, even though that act conceded the existence of the documents and the defendant's control of them; rather, it was the need for the defendant to use his mind to collate the documents that infringed the privilege. Secondly, it signalled that, where the government sought to rely on the foregone conclusion doctrine, more was required than simply an expectation that a defendant had the documents in question. In so doing, the Court significantly narrowed an already limited doctrine.

Through those decisions a handful of conclusions can be drawn: whether the act of production is a testimonial act is determined by the facts of the case; however, where the act of production is a merely physical act or one that does not require the defendant to use the contents of his or her mind, the privilege is not engaged;[68] and if the foregone

63 Ibid 41.
64 Ibid 42.
65 Ibid 43.
66 Ibid 45.
67 Ibid 45.
68 See also the comments in *Doe II* 487 US 201, 208-209 (1988) where the Court stated that '[i]f a compelled statement is not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence'. As physical acts are not testimonial, they do not engage the privilege even if they lead to incriminating evidence.

conclusion doctrine is satisfied – which requires the applicant to demonstrate more than a mere expectation that the defendant possesses the documents in question – the privilege is not infringed because the act of production is not testimonial. As will be discussed in Chapter 3, how the act of production and foregone conclusion doctrines have been applied to compelled production orders has been the decisive issue in the United States in determining whether such an order infringes the privilege.

What has been learnt thus far about the approach to the privilege found in the United States? Three competing developments have served to alternatively narrow, broaden and then narrow once more the scope of the privilege. The findings of the Supreme Court concerning physical evidence saw the privilege given a narrower remit than that granted in the *Boyd* decision. With the establishment of the act of production doctrine, however, pre-existing evidence, including physical documents (or, for present purposes, passwords), can now fall within the scope of the privilege if providing that evidence concedes that the documents exist; that they are in the possession or control of the person producing them; or the act of production authenticates the evidence. Where the act of production doctrine is satisfied, that act of production falls within the scope of the privilege unless the foregone conclusion exception – the final development that once more narrows the scope of the privilege – is met. As Chapter 3 will make clear, it is these two doctrines that lie at the heart of the United States' jurisprudence in the compelled production cases.

1.2.2 England and the European Court of Human Rights

Having set out the boundaries of the privilege in the United States in Part 1.2.1 above, attention now turns to the privilege in England and Wales. The starting point for this analysis is Article 6 of the *ECHR* and how it is understood to protect the privilege. This is because under s 3 of the *Human Rights Act 1998*, English courts are required to take account of any decision of the European Court of Human Rights that relates to a Convention right.[69] For that reason the decisions of the European Court will be considered first in this Part, before those of the English courts.

---

[69] *Human Rights Act 1998* c 42, s 3.

1.2.2.1 The European Court of Human Rights

The privilege is not mentioned in the text of Article 6. Rather, and as will be discussed in greater detail below while analysing the scope of the privilege under the *ECHR*, it has been implied into the text on the basis that the privilege lies 'at the heart of the notion of a fair procedure under Article 6'.[70] One of the first decisions of the European Court of Human Rights to examine the scope of the privilege was *Funke v France*.[71] French customs officers, acting under the Customs Code, sought access to bank statements for overseas bank accounts held by Funke. Funke, who had previously admitted the existence of the accounts,[72] refused to provide them. He was subsequently convicted for failing to produce the documents. On application to the European Court of Human Rights, Funke sought a determination that any requirement to produce the documents constituted a breach of the privilege. The Court, by a majority of eight to one, held that compelling a taxpayer to produce bank statements – which were believed to exist although it was not certain that they did – constituted a breach of the privilege.[73] In an opinion that revealed little about how this finding was reached – a finding that addressed this question in a mere four paragraphs – the majority limited itself to stating that the compulsion imposed on Funke was inconsistent with the right to remain silent and not to be forced to incriminate oneself.[74] The finding that the government did not know the documents existed is questionable, however, given that they knew the bank accounts existed.

Four years later the Court handed down its seminal decision in *Saunders v United Kingdom*.[75] The Department of Trade and Industry of the United Kingdom was investigating the circumstances surrounding a failed take-over bid. Under provisions of the *Companies Act 1985*, any failure to answer questions put by the Department during its investigation constituted a criminal offence. Saunders was one of the persons

70 *Saunders v United Kingdom* (1997) 23 EHRR 313, 337 [68].
71 (1993) 16 EHRR 297 ('*Funke*').
72 Ibid [7].
73 Ibid [44].
74 Ibid [44].
75 (1997) 23 EHRR 313 ('*Saunders*').

interviewed during the investigation. Transcripts of his interviews were provided to the police who brought charges against him based on those transcripts. He was subsequently convicted of various offences. On appeal Saunders argued that the use of the transcripts against him infringed the privilege. In an oft-quoted passaged, the majority stated that

> …the right to silence and the right to not incriminate oneself, are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and the fulfilment of the aims of Article 6. The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused…
>
> The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing...[76] (Emphasis added.)

On that basis, the majority of the Court held that the use of the statements was a contravention of the privilege.[77] While the above statement of the law does not expressly reference the distinction between testimonial and non-testimonial evidence in the same manner that courts of the United States do, it nevertheless reflects the same approach. Significantly, with this statement, the Court moved away from its decision in *Funke*. Where *Funke* found that pre-existing documents that were ordered to be produced did implicate the privilege, the *Saunders'* majority rejected that understanding of the privilege.

---

[76] Ibid 337–338 [68]–[69]. See also *Jalloh v Germany* (2007) 44 EHRR 32, [100].

[77] *Saunders* (1997) 23 EHRR 313, [76]. Note, however, the dissenting opinions, including that of Valticos J in which he stated that to elevate the privilege to an absolute rule 'would mean in many cases that society was left completely defenceless in the face of ever more complex activities in a commercial and financial world that has reached an unprecedented level of sophistication': at 350. Valticos J also called for 'a proper sense of proportion' in determining when the privilege should apply: at 350.

Saunders is also significant for a number of criticisms contained in the dissenting opinion of Martens J, one of which concerned the Court's references to the will of the accused.[78] After noting that one of the primary rationales for the existence of the privilege is the prevention of miscarriages of justice through the use of unreliable evidence that has been compelled from an accused, his Honour proceeded to argue that the majority in *Saunders* had placed excessive weight on a broader rationale for the privilege which held that respect for human dignity and autonomy meant that the primary concern of the privilege was now 'respecting the will of the accused'.[79] This shift in focus, Martens J argued, was inconsistent with the exemption for evidence that had an existence independent of the will of the accused as evidence having an existence independent of the will of a person is nevertheless still frequently obtained against that person's will.[80]

Notwithstanding the dissenting opinions, *Saunders* drew the same clear line concerning physical evidence emanating from an accused's body as is present in United States' law: it does not infringe the privilege.[81] The applicability of the privilege to pre-existing documentary evidence, however, was to remain unsettled. While *Saunders* was followed by *Heaney & McGuinness v Ireland*[82] which applied the *Saunders'* principles, just six months later in *JB v Switzerland*[83] those principles were disregarded.[84]

---

78 To which a second judge joined, and with which two other judges in dissent concurred.

79 *Saunders* (1997) 23 EHRR 313, 352–353 [9]. Martens J expressed his unease about excess weight being placed in this broader doctrine and stated that the broader privilege should always be capable of restriction 'to protect legitimate interests of the community': at [10]. A similar criticism of an equally broad approach to the privilege was made by L'Heureux-Dube J in *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3, [80].

80 *Saunders* (1997) 23 EHRR 313, 355 [12]. After questioning whether the results of a breathalyser test could truly be said to have an existence independent of the will of the accused, Martens J also presciently asked the question 'And what about a pin code or a password into a cryptographic system which are hidden in a suspect's memory?'.

81 See also *L v United Kingdom* [2000] 2 FLR 322, 331 where the Court held unanimously that the right not to incriminate oneself is primarily concerned with respecting the will of the accused person to remain silent and does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers and which has an existence independent of the will of the accused (eg documents, breath, blood, urine and tissue samples).

82 (2001) 33 EHRR 12. See at [40] where the Court noted that material having an existence independent of the will of the accused, 'such as documents or blood samples', do not infringe the privilege.

83 App. No. 31827/96, May 3, 2001.

84 This lack of consistency by the Court in its decisions is a source of much criticism: see Andrew L-T Choo, *The Privilege against Self-Incrimination and Criminal Justice* (Hart Publishing, 2013) at 22 and the references cited in footnote 2.

JB was being investigated for tax evasion. As part of the investigation by the Swiss tax authorities, he was – as was the case in *Funke* – instructed to provide all the documents he possessed relating to certain companies and to declare the source of his income. The requested documents included pre-existing documents and new ones that he was required to prepare. When he failed to provide the documents, he was fined. The Court found that the privilege had been breached. In a problematic passage, the Court stated that notwithstanding that the privilege is not infringed when, for instance, a blood or urine sample is compelled, 'the present case differs from such material which, as the Court found in the *Saunders* case, had an existence independent of the person concerned and was not, therefore, obtained by means of coercion and in defiance of the will of the person'.[85]

There are difficulties with this statement. In the first place, the Court's statement appears to be based on the idea that pre-existing documents do not have an existence independent of the will of the accused. This finding is necessary to avoid the *Saunders*' principle that pre-existing documents (and other pre-existing evidence) have an existence independent of the will of the accused and therefore do not implicate the privilege.[86] However, the Court provides no explanation for how it reached this conclusion beyond what is set out in the paragraph above, which is manifestly inadequate. As at least one subsequent court has noted, the documents in *JB v Switzerland* 'self-evidently had "an existence independent of the person concerned"'.[87] So implausible is the Court's attempt to distinguish *Saunders* that its decision appears to be a rejection of that case.

Secondly, the Court's enduring confusion over its use of the term 'in defiance of the will of the person' is also on display when the Court states that evidence is not obtained in defiance of the will of a person if that evidence has an existence independent of the person. That statement ignores that the taking of a blood sample from a person

85 *JB v Switzerland* App. No. 31827/96, May 3, 2001, [68].
86 *Saunders* (1997) 23 EHRR 313, 338 [69].
87 *Gold Nuts Ltd v Revenue and Customs Commissioners* [2016] UKFTT 82 (TC), [180].

suspected of driving while under the influence of alcohol is ordinarily done against that person's wishes, and as such in defiance of his or her will.

Jalloh v Germany[88] is an important but problematic decision of the Court that further confuses the Court's approach to the privilege. Jalloh had been convicted of drug trafficking largely on the basis of drugs that were retrieved from his stomach through the use of an emetic (which had been pumped into his stomach through a pipe inserted into his nose against his will).[89] In a surprising finding, the Court (by a majority of 11 to six) held that reliance on the retrieved drugs was a contravention of the privilege.

After accepting that the drugs constituted evidence that had an existence independent of the accused's will, the Court nevertheless concluded that the privilege had been infringed.[90] To reach that conclusion, it first found that the privilege was applicable on the facts. It did so for three reasons. First, the Court sought to distinguish bodily materials from the narcotics that Jalloh had swallowed. It did so on the basis that the real evidence in Jalloh's stomach was retrieved in defiance of his will, while the bodily samples identified in *Saunders* were still to be subjected to forensic examination in order to show the presence of drugs or alcohol.[91] Secondly, the Court held that more force was used here than is required to take a blood, urine or breathalyser sample, and that those tests concerned 'material produced by the normal functioning of the body'.[92] Finally, the Court held that the use of emetics violated Article 3 of the *ECHR* which prohibits the use of torture.

Having found the privilege applicable, to determine if it had been infringed the Court performed a balancing exercise that considered 'the nature and degree of compulsion used to obtain the evidence; the weight of the public interest in the investigation and punishment of the offence at issue; the existence of any relevant safeguards in the

88 (2007) 44 EHRR 32 ('*Jalloh*').

89 Ibid [11]–[13].

90 Ibid [123].

91 Ibid [113]. See also Choo, 'Privilege against Self-Incrimination and Criminal Justice', above n 85, 48-49 where he notes that this is consistent what is later said in *R v S(F)* [2009] 1 WLR 1489 in relation to the provision of an encryption key.

92 *Jalloh* (2007) 44 EHRR 32, [114].

procedure; and the use to which any material so obtained is put'.[93] The outcome of that assessment was that the privilege had been breached.[94]

There are grounds for being dissatisfied with the reasons given by the Court for finding that the privilege was applicable. As bodily samples themselves are incriminating – containing as they do evidence of the suspect's drug or alcohol use - the distinction that the Court drew between bodily samples and Jalloh's drugs is difficult to sustain. That the bodily samples need to be tested to reveal the drug or alcohol levels does not alter the fact that it is the sample itself which provides evidence of the criminal offence.

The *Jalloh* Court's decision also demonstrates the weakness of the European Court's test, and shows how it has evolved into its present, problematic form. In *Saunders*, the Court spoke of how the privilege was concerned with 'the will of an accused to remain silent' (emphasis added).[95] That statement broadly accords with the approach taken to the privilege in the United States. However, by the time the *Jalloh* decision was handed down, the Court had dropped the limiting words 'to remain silent' in favour of a test that merely focused on the will of an accused. That test has significant problems, not least of which is that almost any evidence obtained against an accused will have been so obtained against his or her will. The Court's test now ignores what it recognised in *Saunders* as the purpose of the privilege, namely the right not to be a witness against oneself (or, to adopt the United States' terminology, the right not to be compelled to give testimonial evidence). There is nothing testimonial about real evidence (though the act of producing it may contain testimonial elements), and the courts of the United States have accepted the use of an emetic to obtain real evidence from a suspect's stomach does not infringe the privilege.[96] In Canada, too, emetics have been found not to infringe an accused's *Canadian Charter* rights.[97] In this finding, therefore, the European Court of Human Rights stands alone.

---

93 Ibid [117]. This balancing test will be examined in greater detail in Part 1.3.2 below.

94 Ibid [123].

95 *Saunders* (1997) 23 EHRR 313, 338, [69].

96 See, eg, *Blefare v United States* 362 F 2d 870 (9th Cir, 1966); *United States v Briones* 423 F 2d 742 (5th Cir, 1970); *Barrera v United States* 276 F 2d 654 (5th Cir, 1960).

97 *R v Dumas* (1985) 23 C.C.C. (3d) 366 in which the court did not even consider the privilege when finding that the use of an emetic had not infringed the accused's *Canadian Charter* rights.

The Court's reliance on the fact that the evidence had been obtained in breach of Article 3 of the *ECHR* and that a greater degree of force had been applied to Jalloh than may ordinarily be used to obtain other bodily samples is also misplaced. The breach of Article 3 was, as the Court itself noted, grounds enough for the trial to be rendered unfair.[98] That finding is separate to a finding in respect of the privilege. The degree of force used is relevant only to Article 3, not Article 6. Force does not appear to have any relationship with testimony and self-incrimination. Moreover, it is a factor entirely in the control of the accused. Had he verbally objected to the emetics but given no physical resistance, he could have drunk the solution and there would have been no force involved.[99] Conversely, a person instructed to give a blood sample could provide physical resistance that may result in him needing to be physically restrained. Whether or not those orders implicate the privilege should not be determined on the basis of the vigour with which a suspect physically resists having evidence obtained from his or her body.

It is also unclear why it is relevant that blood is 'produced by the normal functioning of the body' but that drugs are not. Arguably, the fact that blood is an intimate part of a person's body, containing substantial personal information about that person, would suggest that it should receive greater, not less, protection than narcotics that have been consumed in order to avoid detection.

Finally, one last aspect of the Court's decision bears comment. In finding the privilege to have been infringed, the Court spoke of the 'nature and degree of compulsion used'. No definition is given, however, of what might constitute compulsion. On the facts in *Jalloh* that is understandable, as physically restraining Jalloh and giving him an emetic

---

That the privilege is not expressed mentioned in the decision is irrelevant: the *Canadian Charter* protects the privilege, and the Court was called upon to determine if the use of emetics infringed it. The Court's finding that the use of emetics could be compelled must of necessity include the finding that emetics do not infringe the privilege.

98 *Jalloh* (2007) 44 EHRR 32, [109].

99 See, eg, *United States v Espinoza* 338 F Supp 1304, 1307 (Cal, 1972) (where the suspect drank the solution upon threat of having a tube inserted into his stomach should he resist); *Blefare v United States* 362 F 2d 870, 872 (9th Cir, 1966) (where the suspect was initially offered a saline solution to drink). See, however, *United States v Guadalupe-Garza* 421 F 2d 876, 878 (9th Cir, 1970) where the suspect was handcuffed and forced to drink the emetic solution.

against his will clearly constituted compulsion. Similarly, threats of legal sanction are also clear examples of compulsion.[100] There may be instances, however, in which it is less clear whether compulsion is present or not. For instance, in the compelled production of a password scenario, would it constitute compulsion to trick a person into revealing his or her password? While no court has yet answered that question, courts of the United States, at least, have provided some guidance on what can constitute compulsion. The withholding of medical treatment while seeking a confession constitutes unlawful coercion which would cause any confession given to be a breach of the privilege;[101] the use of false statements, threats and emotional manipulation may, depending on the mental state of the suspect, constitute coercion that would result in an infringement of the privilege,[102] although ordinarily it will not constitute compulsion;[103] and 'threats, violence or express or implied promises sufficient to overbear the [suspect's] will and critically impair his capacity for self-determination' will affect the voluntariness of the suspect's actions, although the use of 'psychological pressure' is not ordinarily sufficient to have that effect.[104] Left undecided, however, is the possibility that actions by the police short of physical or legal compulsion may nevertheless constitute compulsion for purposes of the privilege where their conduct affects the voluntariness of the suspect's actions.

1.2.2.2 England and Wales

Throughout the European Court of Human Rights' inconsistent approach on this issue, the English courts have trodden a straighter path, one endorsing the approach in *Saunders* that pre-existing documents and other real evidence does not fall within the scope of the privilege. With regard to pre-existing documents, in 2001 the English Court of Appeal handed down its decision in *Attorney General's Reference (No 7 of 2000)*.[105] The issue before the Court was whether a person who was compelled under provisions

100 See, eg, *R v Kearns* [2002] 1 WLR 2815; *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3.

101 *Mincey v Arizona* 437 US 397-401 (1978); *Beecher v Alabama* 389 US 35, 36-8 (1967); *Reck v Pate* 367 US 433, 441-2 (1961).

102 *Outlaw v City of Cahokia* (SD Ill, No 16-cv-456-JPG-SCW, 26 April 2017).

103 *United States v LeBrun* 363 F 3d 715, 724-25 (8th Cir, 2004).

104 Ibid 724-25 (8th Cir, 2004) where the Court noted that 'this is a very demanding standard'.

105 [2001] 1 WLR 1879.

of the *Insolvency Act 1986* to produce pre-existing documents to the official receiver, on pain of conviction for contempt of court in the event of non-compliance, fell within the ambit of the privilege. The Court, following *Saunders* in preference to the earlier *Funke* decision, held that the privilege was not infringed in this circumstance. In so finding, the Court stated that the distinction drawn in *Saunders* between 'statements made and other material independent of the making of a statement, is not only one to which we should have regard, but is one which, it seems to us, is jurisprudentially sound'.[106]

The decision in *Attorney General's Reference (No 7 of 2000)* found support in the later decision of *R v Kearns*,[107] which concerned a demand for production of accounting records under the *Insolvency Act 1986*. In *R v Kearns*, the Court found that while the privilege was implicated where a defendant was forced to create the evidence in question, it was inapplicable to pre-existing evidence that was brought to the court's attention using compulsion.[108]

The ratio of *Attorney General's Reference (No 7 of 2000)* and *R v Kearns* was later applied to the search of a computer. In *C plc v P (Attorney General Intervening)*,[109] a search warrant of P's premises was obtained as part of proceedings in an intellectual property matter. At the time that the search was to be conducted, P stated that he would permit the search but would rely on the privilege in respect of any material that the search might disclose. The search revealed several computers that were put in the custody of the supervising solicitor's care so that they could be imaged. The computers were subsequently provided to computer experts to perform the imaging. While performing that imaging, material was found the possession of which constituted an offence. Longmore LJ, delivering the leading opinion, noted that since *Saunders* it had been accepted that the privilege did not apply to evidence 'that came into existence independently of (and usually prior to) any compulsory questioning of the defendant or any application of the court's compulsory discovery process'.[110] In accordance with the

106 Ibid [58].
107 [2002] 1 WLR 2815.
108 Ibid [52].
109 [2008] Ch 1.
110 Ibid [16] (per Longmore LJ, with whom Nourse LJ concurred).

Saunders' principles, and bound as the Court was by its earlier decision in *Attorney General's Reference*, Longmore LJ found that P could not rely on the privilege.[111]

The *Saunders* dicta has also been applied by Scottish courts in respect of bodily samples. Those decisions are persuasive precedents in English law. In *MacLean v HM Advocate*,[112] a case concerning the admissibility of a DNA sample from a mouth swab, the Appeal Court of the Scottish High Court of Justiciary found that 'the taking of fingerprints, bodily samples or DNA swabs from a detained or arrested suspect would not have struck us as raising any issue of self-incrimination'.[113] This finding was based on the principles set out in *Saunders* and *Jalloh* that the privilege does not apply to evidence having an existence independent of the will of the accused, which includes bodily samples.

Voice samples, too, have been found to fall outside the scope of the privilege. In *McFadden v HM Advocate*,[114] the appellant had been convicted of murder. Part of the evidence against him at trial included evidence of an identification parade at which he had been required to say a specific sentence. He appealed against his conviction on the basis that the statements he had made during the identification parade constituted a breach of the privilege. The Court held that the use of voice samples did not infringe the privilege. In so finding, the Court noted that voice samples were not concerned with the 'substantive content' of what was said, but rather with identifying features such as the speaker's timbre of voice, intonation, register, accent and pronunciation.[115] Those identifying features, the Court further noted, had been identified in *Jalloh* as evidence falling outside the scope of the privilege as it was evidence that had an existence independent of the accused.[116] The Court further found that the fact that the voice sample required 'some effort' from the accused which created new evidence did not render it a breach of the privilege.[117]

---

111 Ibid [34]–[36] (per Longmore LJ, with whom Nourse LJ concurred).

112 2012 JC 293.

113 Ibid 306.

114 2010 SCL 247.

115 Ibid 260 [35].

116 Ibid 261 [35]. This was said to be so because speaking was a natural human activity: at [25], [30].

117 Ibid 261 [30] where the Court refers to *Brown v Stott* [2003] 1 AC 681 for support for this position.

The English position, then, shares numerous similarities with that of the United States. Bodily evidence – which includes handwriting and voice exemplars, as well as blood samples – falls outside the scope of the privilege in both jurisdictions for the shared reason that it does not contain a communicative or testimonial element. In order for a communicative element to be present, that communication must disclose knowledge possessed by the person making the communication. Both jurisdictions also reject the application of the privilege to other pre-existing evidence, though that evidence may fall within the scope of the act of production doctrine in the United States. Note, too, that while England and Wales does not formally have the same act of production doctrine, the leading English case on compelled production orders appears to have adopted the principles behind that doctrine.[118] That case will be discussed further in Chapter 4. Lastly, both the English courts and the courts of the United States have rejected the use of the concept of an interference with a person's will or personality to determine whether the privilege has been infringed. In the United States, that concept was rejected in *Wade* and *Mara*, while English law has notably not picked up the concept even though it is found in the decisions of the European Court of Human Rights. Despite these similarities, some differences remain. In particular, the act of production doctrine appears to sit somewhat at odds with the independent existence test. Under the independent existence test, evidence having an independent existence, such as a pre-existing written document, does not fall within the scope of the privilege; under the act of production doctrine, however, that same evidence may now fall within the scope of the privilege. It is not clear from the case law how that tension is to be resolved.

1.2.3 Canada

The third comparator jurisdiction to be considered is Canada. The privilege has been described as 'one of the cornerstones of [Canadian] criminal law'[119] and one of the 'fundamental tenets of a fair trial'.[120] It provides that a person 'is not required to respond to an allegation of wrongdoing made by the State until the State has succeeded

118 *R v S(F)* [2009] [2009] 1 WLR 1489, 1497 [21].
119 *R v Henry* [2005] 3 SCR 609, [2].
120 *R v Collins* [1987] 1 SCR 265, [48].

in making out a prima facie case against him or her'.[121] Furthermore, any compulsion on a suspect to 'furnish evidence against him- or herself…violates the privilege against self-incrimination'.[122] Prior to the introduction of the *Canadian Charter*, the scope of the privilege was – as was the case in England and Wales prior to the *ECHR* – relatively narrow[123] and was reflected in two separate rules: the witnesses' privilege and the non-compellability of an accused.[124] While the non-compellability of an accused was strictly enforced, a witness could be compelled to testify – though he or she received immunity against prosecution in any subsequent proceedings.[125]

Under the *Canadian Charter* the privilege is given expression in a number of separate provisions, including ss 7, 10(b), 11(c) and (d) and 13. Section 7 provides that 'every person has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice'. This requires a court to: consider whether there is a risk of imminent deprivation; identify any relevant principles of fundamental justice, which include the privilege; and determine whether the deprivation is in accordance with those principles.[126] Where the deprivation is in accordance with the principles of fundamental justice, the privilege will not be infringed.

Section 10(b) provides a suspect with the right to counsel, a right that has been described by the Supreme Court as 'primarily aimed at preventing the accused or

---

121 *R v White* [1999] 2 SCR 417, [41] (Iacobucci J) referring to *R v P (M.B)* [1994] 1 SCR 555, 577-79 (Lamer J); *R v S (R.J.)* [1995] 1 SCR 451, [82]–[83] (Iacobucci J).

122 *R v White* [1999] 2 SCR 417, [42] (Iacobucci J) quoting *R. v. Jones*, [1994] 2 SCR. 229, 249.

123 *Thomson Newspapers Ltd v Canada* [1990] 1 SCR 425, [275] (L'Heureux-Dube).

124 *R v S (R.J.)* [1995] 1 SCR 451, [67] (Iacobucci J). See also Ed Ratushny, *Self-Incrimination in the Canadian Criminal Process,* Carswell's Criminal Law Series (Carswell Company Limited, 1979) 66; David M Paciocco, 'Self-Incrimination: Removing the Coffin Nails' (1989) 35 *McGill Law Journal* 73, 75.

125 *R v S (R.J.)* [1995] 1 SCR 451, [64]–[66] (Iacobucci J). The compellability of a witness, and his or her immunity, is provided for under ss 5(1) and (2) of the *Canada Evidence Act*, RSC 1985, c C-5.

126 *R v Herbert* [1990] 2 SCR 151; *R v White* [1999] 2 SCR 417, [38]–[40] (Iacobucci J); *R v S (R.J.)* [1995] 1 SCR 451, [45] (Iacobucci J); *Thomson Newspapers Ltd v Canada* [1990] 1 SCR 425. See also Paciocco, above n 124, 103; Andrew L-T Choo, 'Give Us What You Have – Information, Compulsion and the Privilege Against Self-Incrimination as a Human Right' in Paul Roberts and Jill Hunter (eds), *Criminal Evidence and Human rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012) 239, 247 where he states that 'the privilege is considered to be a "principle of fundamental justice" under section 7 of the Charter'.

detained person from incriminating herself'.[127] Section 11(c) provides that an accused cannot be compelled to give evidence, while s 11(d) provides for the presumption of innocence and the right to a fair trial, the latter of which incorporates the privilege and will typically provide the same protection as s 7.[128] Finally, s 13 grants use immunity, including for derivative evidence.[129] This prevents a suspect from experiencing indirect compulsion that results in incrimination, thereby ensuring that the state is unable to do indirectly that which s 11(c) prevents it from doing directly.[130]

It has been said of the privilege that it applies to 'any state action that coerces an individual to furnish evidence against him- or herself in a proceeding in which the individual and state are adversaries'.[131] The protection afforded by the privilege is not absolute, however, and depends on the specific context of each situation in which it arises.[132] For this reason, the privilege does not have a 'pre-defined scope'.[133] Moreover, the *Canadian Charter*, in s 1, allows for reasonable limits to be imposed on *Canadian Charter* rights, including the privilege.

Prior to the introduction of the *Canadian Charter*, the privilege was understood to only apply to 'testimonial compulsion' and was claimable only by a witness and an accused person who was non-compellable.[134] As such, bodily samples or bodily conditions – such as breathalyser samples or blood tests – and certain conduct over which the accused had no control did not invoke the privilege.[135] Early case law under the *Canadian Charter*

---

127 *R v Simmons* [1988] 2 SCR 495, 539 (L'Heureux-Dube J).

128 *R v Fitzpatrick* [1995] 4 SCR 154, [20] (La Forest J), citing *Thomson Newspapers Ltd v Canada* [1990] 1 SCR 425, 546 and *R v S (R.J.)* [1995] 1 SCR 451, 561–2.

129 *R v S (R.J.)* [1995] 1 SCR 451.

130 *R v Henry* [2005] 3 SCR 609, [2] citing *R v Dubois* [1985] 2 SCR 350, 358.

131 *R v Jones* [1994] 2 SCR 229, 249; *R v White* [1999] 2 SCR 417, [42].

132 *R v White* [1999] 2 SCR 417, [45] (Iacobucci J); *R v S (R.J.)* [1995] 1 SCR 451, [107]; *R v Fitzpatrick* [1995] 4 SCR 154, [26] (La Forest J).

133 *R v S (R.J.)* [1995] 1 SCR 451, [96] (Iacobucci J).

134 *Marcoux v R* [1976] 1 SCR 763, [9]; *R v S (R.J.)* [1995] 1 SCR 451, [67] (Iacobucci J).

135 *Marcoux v R* [1976] 1 SCR 763, [13]. In *Marcoux*, the Court held that an identification line-up did not implicate the privilege. See, also *R v Curr* [1972] SCR 889 where it was held that compelling a suspect to give a breathalyser sample did not infringe the privilege; *Attorney-General of Quebec v Begin* [1955] SCR 593 where it was held that taking a blood sample without consent did not invoke the privilege; *Reference re s 92(4) of the Vehicles Act, 1957 (Saskatchewan)* [1958] SCR 608 where it was held that provincial parliaments could impose an obligation on drivers to provide breath or blood samples; *Hogan v R* [1975] 2 SCR 574. See, eg,

on the use of bodily samples followed that understanding. In *R v Beare*,[136] in a unanimous judgment, the Supreme Court found that a statutory requirement to provide a fingerprint on arrest (as opposed to conviction) did not infringe the privilege under s 7 of the *Canadian Charter*.[137] In reaching its conclusion the Court weighed a number of considerations, including the fact that fingerprinting was 'an infallible tool of criminal investigation' the reliability of which was fully accepted;[138] the public interest in effective law enforcement;[139] the fact that fingerprinting did not involve a serious invasion of the suspect's body;[140] and an acknowledgement that fingerprinting occurred outside criminal investigations, both in business and civil service.[141]

Notably, the Court in *R v Beare* did not refer to the privilege in its judgment but limited itself to the question of whether the taking of fingerprints infringed the principles of fundamental justice, which include the privilege. Furthermore, the Court found that as the fundamental principles of justice were not infringed by the taking of the fingerprints, the use of those fingerprints in evidence could not infringe the fairness of the trial under s 11(d).[142]

Not all bodily samples, however, have been accorded this same treatment. In *R v Stillman*,[143] the State, without consent or statutory authority, took samples of a murder suspect's scalp and pubic hair, dental impressions and buccal swabs. The suspect objected to the use of that evidence at trial, arguing, amongst other things, that it infringed the privilege. Cory J, writing for the majority, held that the taking of those samples absent consent or authority was a breach of ss 7, 8 and 10 of the *Canadian Charter*,[144] and one that resulted in Stillman providing self-incriminating evidence.[145]

---

the discussion of the common law scope of the privilege by McLachlin J in *R v Stillman* [1997] 1 SCR 607, [200]-[208]. See, too, Paciocco, above n 125, 77, 85.

136 [1988] 2 SCR 387.

137 Ibid [71].

138 Ibid [21].

139 Ibid [31].

140 Ibid [35].

141 Ibid [35].

142 Ibid [69].

143 [1997] 1 SCR 607 ('*Stillman*').

144 Ibid [65].

145 Ibid [70].

Cory J's judgment, however, makes almost no reference to the privilege in discussing the breaches of ss 7, 8 and 10; it is only when discussing the exclusion of evidence under s 24(2) that the privilege is examined. Thus while his Honour finds the privilege to have been breached, he does not adequately explain why the taking of these bodily samples falls within the scope of the privilege other than to state that the privilege is breached on all occasions in which a suspect is 'compelled…to participate in the creation or discovery of self-incriminating evidence in the form of confessions, statements or the provision of bodily samples'.[146] This failure is all the more unfortunate given the clear statements made in McLachlin J's dissenting opinion that 'the privilege against self-incrimination is confined to testimonial evidence' and has never included physical evidence obtained from a suspect.[147] It is worth noting, too, that in the recent case of *R v Saeed*, the Supreme Court held that the taking of a penile swab from the accused did not infringe the privilege and was distinguishable from *Stillman*.[148] This finding was based largely on the fact that the penile swab was intended to obtain the DNA information of the complainant, not of the accused, even though the Court recognised that the swab was likely to contain the accused's DNA too.

Six years after *Stillman*, in the case of *R v B (S.A.)*,[149] the legality of DNA warrant provisions in the *Criminal Code* was challenged.[150] In determining whether s 8 of the *Canadian Charter* had been infringed because of a violation of the privilege, the Court noted that, in contrast with testimonial evidence, there was no question of the reliability of DNA evidence.[151] The more challenging question, however, was whether the DNA provisions constituted an abuse of power. To answer that, Arbour J held that it was necessary to consider the degree of coercion used by the state; the extent to which the relationship between the state and individual was adversarial at the time the sample

146 Ibid [73].

147 Ibid [198]. One of McLachlin J's objections to extending the privilege to bodily evidence, discussed at [205], was that there was no meaningful way to distinguish between DNA samples and a police photo or the identification line-up, both of which are accepted police techniques.

148 *R v Saeed* [2016] 1 SCR 518.

149 *R v B (S.A.)* [2003] 2 SCR 678.

150 *Criminal Code* RSC 1985, C-46.

151 *R v B (S.A.)* [2003] 2 SCR 678, [58].

was taken; and whether the compulsion increased or reduced the risk of an abuse of power by the state.[152] On balance, her Honour found that the public interest outweighed the individual's interest,[153] with the result that the provisions did not infringe the privilege under either ss 7 or 8.[154] The Court had previously reached the same outcome in respect of breathalyser testing.[155]

The Supreme Court has also considered statutory requirements to provide information in the context of a criminal investigation. Where a statutory obligation to report a car accident will mean the person giving the report is compelled to provide incriminating evidence, the use of that report against the person in criminal proceedings will constitute a violation of the privilege under s 7 of the *Canadian Charter*.[156] This is so because: in order to fully function in society, a person needs to be able to drive, with the consequence that the decision to drive could not be said to be a free choice;[157] the person making the statement is in an adversarial relationship with the State;[158] there is a risk that any statement might be unreliable;[159] and allowing the statement to be admitted could lead to abuse of power by the State.[160]

Though the Supreme Court has held that the privilege is not infringed by statutory obligations to provide information where no criminal investigation has commenced or is anticipated,[161] it has been noted that the act of producing the documents may have a communicative element that could result in their exclusion under the derivative evidence immunity.[162] In this manner Canadian law, like United States law, recognises that evidence that otherwise falls outside the scope of the privilege may move under the umbrella of its protection through certain acts of production.

---

152 Ibid [58].
153 Ibid [60].
154 Ibid [64].
155 *R v Bartle* [1984] 3 SCR 173, [58]. See also *R v Shepherd* [2009] 2 SCR 527.
156 *R v White* [1999] 2 SCR 417, [30].
157 Ibid [55].
158 Ibid [60].
159 Ibid [62].
160 Ibid [66].
161 *R v Fitzpatrick* [1995] 4 SCR 154; *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3, [46]–[53].
162 *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3, [52]-[53].

Despite that similarity, the Canadian jurisprudence evidences relatively significant departures from the positions adopted in the United States and England and Wales. Most notably, statements by the Supreme Court that the privilege may apply to any incriminating evidence that a suspect is compelled to produce or create go beyond the position adopted in the other jurisdictions. That understanding, which in *Stillman* was spoken of in the context of bodily evidence, indicates a scope broader than the act of production doctrine, which to date in the United States has only applied to documentary evidence and not other forms of physical evidence. Indeed, the act of production doctrine could not sensibly be applied to bodily evidence, such as DNA, as it is self-evident that each suspect has DNA and that the DNA is in his or her possession (those being two of the elements of the act of production doctrine). The act of production doctrine can thus only apply to evidence the existence of which, or the suspect's possession of which, is disputed. Similarly, in England and Wales the privilege has been found inapplicable to bodily evidence.

It is that broader understanding of the privilege evidenced in *Stillman* that is the reason that Canada is the only jurisdiction of those examined that extends the privilege to the taking of bodily samples in certain circumstances. It is to be noted, however, that while only Canada has applied the privilege to bodily samples, the European Court of Human Rights has applied the privilege to physical evidence that would not fall within the scope of the privilege in the United States, England and Wales or Australia. In *Jalloh*, the pumping of narcotics from a suspect's stomach was found to infringe the privilege. That finding, which this thesis criticised in Part 1.2.2, evidences a similarly broad conception of the privilege as that found in Canada.

1.2.4 Australia

How do the three jurisdictions discussed above compare to Australia? The Australian High Court has stated that the privilege against self-incrimination is a right that is 'deeply

engrained in the common law',[163] one that acts as 'a fundamental bulwark of liberty'.[164] This results from the privilege's essential purpose in ensuring that the prosecution bears the onus of proving the accused's guilt[165] in order to ensure a balance between the power of the state and the position of the accused.[166]

Importantly, the privilege in Australia rests on different moorings to the comparator jurisdictions as it does not have constitutional – or in the case of England and Wales, quasi-constitutional – recognition. It has therefore been said that when an Australian court is considering whether the privilege has been abrogated, 'the constitutional nature of this question [in the United States] is materially different from the statutory question of construction which arises' in Australian law.[167] As will be seen in the context of motor vehicle reporting obligations, this has allowed Australian courts to grant the privilege a relatively broad scope while simultaneously holding that it had nevertheless been abrogated by statute.

At an early stage, it was held that several bodily samples do not infringe the privilege where they are obtained pursuant to a valid power. For example, in *King v McLelland* the privilege was found to be inapplicable to breathalyser samples,[168] and that to allow a suspect to refuse to provide a breath sample would be to give the privilege 'a breadth of operation which it does not have'.[169] The Court in *King v McLelland* further noted that the privilege has only ever granted 'a right to refuse to answer incriminating questions', and that the history of the privilege showed that it was limited to 'testimonial

---

163 *Sorby v The Commonwealth* (1983) 152 CLR 281, 309 (Mason, Wilson and Dawson JJ); *Reid v Howard* (1995) 184 CLR 1, 5 (Deane J), 11 (Toohey, Gaudron, McHugh and Gummow JJ). See also *Environmental Protection Authority v Caltex Refining Co Pty Limited* 178 CLR 477, 532 (Deane, Dawson and Gaudron JJ); *X7 v Australian Crime Commission* (2013) 248 CLR 92, [104] (where the privilege is described as a substantive common law right and not a rule of evidence); *Lee v New South Wales Crime Commission* (2013) 251 CLR 196, 202 [1], 215 [24] (French CJ).

164 *Pyneboard Pty Ltd v Trade Practises Commission* (1983) 152 CLR 281, 294 (Gibbs CJ).

165 *Construction, Forestry, Mining and Energy Union v Boral Resources (Vic) Pty Ltd* (2015) 256 CLR 375, 395, [64]; *Do Young Lee v The Queen* (2014) 253 CLR 455, 466-467 [32]-[33].

166 *Construction, Forestry, Mining and Energy Union v Boral Resources (Vic) Pty Ltd* (2015) 256 CLR 375, 396, [68].

167 *A v Boulton* (2004) 207 ALR 342, 358 [64]. See also *Environmental Protection Authority v Caltex Refining Co Pty Limited* 178 CLR 477, 490 (Mason CJ, Toohey J).

168 *King v McLelland* [1974] VR 773, 778.

169 Ibid 776.

disclosures'.[170] In explaining the different treatment accorded to statements and fingerprints or other physical evidence emanating from the suspect, the Court stated that while incriminating statements create new evidence not previously existing, fingerprints or other physical features already exist and are not capable of being misrepresented.[171] In this regard blood and breath samples were indistinguishable from fingerprints.[172] The Court also noted that the people to whom the statute (which provided for the taking of breathalyser samples) applied and the statute's scope were clearly defined;[173] and the purpose of the statute was to 'combat the evil' of driving while intoxicated, which was a menace to society.[174]

Unsurprisingly, fingerprints have also been found not to infringe the privilege. The reasons for so finding include that no assistance is required from the accused as is the case with testimonial evidence;[175] the compulsory taking of fingerprints does not expose the accused to unreliable evidence;[176] and fingerprints, being a physical characteristic, do not fall within the scope of the privilege which is limited to 'answers given by the accused to questions asked of him'.[177]

This understanding of breathalyser tests – and other bodily samples – was confirmed by the High Court in *Sorby v The Commonwealth*. While the case concerned the potential abrogation of the privilege by the *Royal Commissions Act 1902* (Cth), Gibbs CJ noted in his judgment that:

> The privilege prohibits the compulsion of the witness to give testimony, but it does not prohibit the giving of evidence, against the will of a witness, as to the condition of his body. For example, the witness may be required to provide a fingerprint, or to show his face or some other part of his body so that he may be identified, or to speak or to write so that the jury or another witness may hear his voice or compare his handwriting.[178]

---

170 Ibid 776.
171 Ibid 777.
172 Ibid 777.
173 Ibid 778.
174 Ibid 779.
175 *Grollo v Bates* (1994) 53 FCR 218, 249.
176 Ibid 250.
177 *R v Carr* [1972] 1 NSWLR 608, 612. Special leave to appeal this decision was refused in *Carr v The Queen* (1973) 127 CLR 662.
178 *Sorby v The Commonwealth* (1983) 152 CLR 281, 292 ('*Sorby*'). See also *Grollo v Bates* (1994) 53 FCR 218, 250 where the Court stated that 'body, blood and breath content, and fingerprints,

Relying on *Sorby*, subsequent court decisions have held that neither voice samples[179] nor handwriting samples infringe the privilege.[180]

While the privilege in Australia follows the United States and England and Wales in relation to bodily evidence, there is evidence of it having a slightly broader scope than those jurisdictions in respect of motor vehicle reporting obligations. In *Loges v Martin*, the Victorian Supreme Court was asked to decide whether the owner of a motor vehicle could rely on the privilege to refuse to comply with a statutory requirement to provide details of the driver at a specified time. The Court held that the statute in question abrogated the privilege and that as the purpose of the statutory provision was to improve road safety, allowing a person to rely on the privilege would undermine that function.[181]

In *R v Hooper*, the Full Court of the South Australian Supreme Court was called upon to determine whether a statutory requirement imposed on the owner of a motor vehicle to provide details of the driver of a motor vehicle at a specified time infringed the privilege. The provision in question did not provide an express grant of immunity. As in *Loges v Martin*, the Court found that the privilege had been abrogated and that the owner of the vehicle was required to provide the information required under the provision.[182] For present purposes the importance of these two decisions is not the courts' assessment of the abrogation of the privilege, but rather their prior (implied) findings that the privilege was engaged by the motor vehicle reporting obligation – for if it had not been engaged, there would have been no need for its abrogation.

---

are not the person's creation but are objective elements of identity' and therefore not covered by the privilege.

179 *Bulejcik v The Queen* (1996) 185 CLR 375.

180 *R v Knight* (2001) 160 FLR 465.

181 *Loges v Martin* (1991) 13 MVR 405, 409. See also *R v Davis* [1976] 1 NSWLR 84 where the New South Wales Court of Criminal Appeal found that failure to comply with a similar statutory obligation was an offence.

182 *R v Hooper* (1995) 64 SASR 480, 486.

Lastly, although the privilege does not ordinarily apply to pre-existing evidence, it has been found to be applicable to orders to produce pre-existing documents. In *Sorby*, the High Court stated that

> it has been a firmly established rule of the common law, since the seventeenth century, that no person can be compelled to incriminate himself. A person may refuse to answer any question, or to produce any document or thing, if to do so may "may tend to bring him into peril and possibility of being convicted as a criminal".[183]

In its later decision in *Controlled Consultants Proprietary Limited v Commissioner for Corporate Affairs*, the High Court was even more emphatic, holding that a requirement to produce pre-existing documents on pain of punishment 'is quite inconsistent with the maintenance of the privilege against self-incrimination'.[184]

1.2.5 Assessment of the scope of the privilege in the selected jurisdictions

The following findings have been made in this Part. Canadian law grants a broader scope to the privilege than the other jurisdictions, one which appears to commence from the position that any compulsion to produce evidence, even where that evidence is pre-existing physical evidence, may infringe the privilege. Only the European Court of Human Rights – in *Jalloh* – has endorsed an understanding of the privilege that is similarly broad. As argued in Part 1.2.2, however, the *Jalloh* decision is inconsistent with earlier principles from the European Court of Human Rights; it is a decision that has not been adopted in English law; and the jurisprudence of the European Court of Human Rights suggests an uncertainty within the court as to what the privilege means.

With regard to bodily evidence, the Australian High Court has stated that 'the privilege…does not prohibit the giving of evidence, against the will of the person, as to condition of his body'.[185] The same position is adopted in England and Wales and the United States. That statement, which sits at odds with the Canadian position (and arguably the position in *Jalloh*) recognises that there is a distinction between testimony and evidence, that it is testimony that is protected by the privilege and that the

183 *Sorby* (1983) 152 CLR 281, 288 (Gibbs CJ).
184 (1985) 156 CLR 385, 392 (Gibbs CJ, Mason and Dawson JJ).
185 *Sorby* (1983) 152 CLR 281, 292 (Gibbs CJ).

compelling of evidence might not constitute testimony. Notably, however, while neither English courts nor those of the United States have found that certain motor vehicle reporting obligations infringe the privilege, Australian courts have adopted the same position as Canada in finding such obligations to implicate the privilege, thereby granting the privilege (at least until it is abrogated) a broader scope than that given to it in the United States and England and Wales.[186]

Notwithstanding the broadly consistent outcomes between Australia, England and Wales and the United States, the language of the privilege in each jurisdiction differs. Thus, the courts of the United States speak of the privilege only applying to testimonial evidence, whereas in England and Wales courts ask whether the evidence has an independent existence or is pre-existing. Australia adopts both terms. As for the act of production doctrine, while the United States is the only jurisdiction that formally speaks of such a doctrine, Australian, English and Canadian courts have recognised that the privilege may apply to pre-existing evidence if the act of producing that evidence has a testimonial component.

Lastly, the European Court of Human Rights has, at times, relied heavily on the test of whether evidence was obtained against the will of the accused. English courts, however, have refused to adopt this same test, and it has not been applied in the United States either. The use of this concept by the European Court of Human Rights has, this thesis argues, led to much of the inconsistencies in that Court's jurisprudence. Those inconsistencies do not arise from any conceptual difficulty with understanding the test; rather they are caused by the difficulty of applying it consistently in a way that does not capture evidence clearly falling outside the scope of the privilege. For example, a refusal to provide a fingerprint would mean that forcing a person to provide that fingerprint entailed compelled evidence against the will of that person. On its face, the privilege should be engaged; in practice, however, no jurisdiction extends the privilege to that bodily feature. Since reference to the will of the accused cannot therefore accurately

[186] In Australia, however, that finding is of limited consequence as such motor vehicle reporting obligations are accompanied by the abrogation of the privilege. As will be discussed in Chapter 2, in Canada the privilege cannot as easily be abrogated.

determine whether the privilege is engaged, its use by the European Court of Human Rights is likely to continue to sow confusion.

Having analysed the scope of the privilege in the respective jurisdictions in this Part 1.2, Part 1.3 considers the role that the weighing of competing interests has played in arriving at those respective positions.

1.3 WEIGHING OF INTERESTS

As already noted in Part 1.2, a common feature among the jurisdictions is the role played by the weighing of interests in determining the outer boundaries of the privilege. While the courts have frequently acknowledged the importance of the privilege, its role has regularly been set against competing factors that have been relied upon to limit the scope of the privilege. Some of those competing factors are relevant to determining whether the privilege encompasses compelled production orders. In this Part 1.3, the role of those competing factors and how they are balanced against an individual's right to the privilege is examined more closely.

1.3.1 Balancing in the United States

Of the four jurisdictions, the balancing of competing interests against the privilege is the least visible in the United States. Nevertheless, as is shown below, on several occasions the Supreme Court has relied on a balancing exercise in order to find that the privilege did not apply to a specific circumstance.

In *Breithaupt v Abram*,[187] a relatively early decision of the Supreme Court, the petitioner had been involved in a car accident in which three people in another car were killed. The petitioner, who was seriously injured, was found with an empty bottle of whisky in the glove compartment of the truck that he was driving. The unconscious petitioner was taken to hospital where, after alcohol was smelt on his breath, a blood sample was taken which revealed that his blood alcohol level was above the legal limit.[188] The petitioner was charged with and subsequently convicted of involuntary manslaughter, a conviction

187 352 US 432 (1957) ('*Breithaupt*').

188 Ibid 433.

he appealed against on that basis that reliance on the result of the blood test infringed the privilege against self-incrimination.

In finding that the taking of the blood sample did not infringe the privilege, Clarke J, in delivering the opinion of the Court, considered several factors that were deemed relevant to determining if there had been an infringement. First, the taking of a blood sample was a routine procedure, one that millions of people had voluntarily gone through.[189] Furthermore, several states had legislation in place that allowed the taking of such samples, a fact that 'negatives the suggestion that there is anything offensive about them'.[190] Those considerations alone meant the taking of the blood sample was not an action that shocked the conscience (and was not therefore one in breach of the privilege).[191]

Secondly, Clarke J gave weight to the importance of reducing traffic fatalities, which he noted were an increasingly common occurrence on United States' roads and about which the United States should be doing all it could to make driving safer. That included using modern scientific measures to strictly enforce the traffic laws.[192] In the words of Clarke J, '[m]odern community living requires modern scientific methods of crime detection lest the public go unprotected'.[193]

Thirdly, it was said that the minor violation suffered by the petitioner needed to be weighed against the interest of society in determining whether a suspect was driving while under the influence of alcohol. So weighed, the value of the blood sample and its deterrent effect on other drivers 'far outweighed' the invasion of the suspect's body.[194] As will be discussed in Chapters 3 and 4, it is arguable that compelling a password implicates the same considerations of similar weight. As the use of encryption grows, so too does the public interest in law enforcement being able to access encrypted

189 Ibid 436. See also *South Dakota v Neville* 459 US 553, 563 (1983).
190 *Breithaupt* 352 US 432, 436 (1957).
191 Ibid 436.
192 Ibid 439. See also *South Dakota v Neville* 459 US 553, 558 (1983); *Mackey v Montrym*, 443 US 1, 19 (1979) where the Court spoke of the 'compelling interest in highway safety'.
193 *Breithaupt* 352 US 432, 439 (1957).
194 Ibid 439.

material to which it has a lawful entitlement. At the other end of the scale, the infringement of the privilege, though not minor, is limited to the asking of a single question. It might be expected, then, that when a compelled production order is sought the public interest will outweigh the interests of the individual.

The weighing of interests has also been used to determine if the privilege was infringed by motor vehicle reporting obligations. *California v Byers*[195] concerned a requirement for a driver who had been involved in a car accident resulting in damage to property to stop and identify him- or herself. Byers argued that this requirement breached the privilege. At first instance, Byers' argument was successful. On appeal, the Supreme Court was asked to determine whether the provision infringed the privilege if it lacked an immunity provision.[196] At the outset, Burger CJ, delivering the opinion of the Court, noted that the tension between the protection afforded by the privilege and the state's desire for information was to be 'resolved in terms of balancing the public need on one hand, and the individual claim to constitutional protections on the other; neither interest can be lightly treated'.[197]

Burger CJ held that the statute only required of a person involved in an accident to stop at the scene – which was a non-testimonial action – and to disclose his or her name and address – which was 'an essentially neutral act'.[198] The testimonial element necessary for a breach of the privilege was therefore absent.[199] While acknowledging that the person's name and address identified him or her, and therefore may serve as a 'link in a chain of evidentiary factors', the Court's previous jurisprudence held that such evidence did not infringe the privilege as it did not itself provide evidence of criminal conduct.[200]

195 402 US 424 (1971) ('*Byers*').
196 Ibid 427.
197 Ibid 427.
198 Ibid 431–32.
199 Ibid 432.
200 Ibid 433–434.

Notably, Burger CJ also identified law enforcement concerns as a reason for finding the privilege inapplicable in certain circumstances. It was his opinion that 'constitutional values' such as the privilege are not

> of such overriding significance that they compel substantial sacrifices in the efficient pursuit of other governmental objectives in all situations where the pursuit of those objectives requires the disclosure of information which will undoubtedly significantly aid in criminal law enforcement.[201]

In a concurring judgment, Harlan J disagreed with Burger CJ by finding that stopping and providing one's name did have a testimonial aspect.[202] However, he found that when faced with the question of whether to give the privilege its 'full scope', the Court should consider two factors: 'the history and purposes of the privilege, and the character and urgency of the other public interests involved'.[203] With regard to the public interest, if the privilege was to be applied to the statute in question it would be able to be applied to every instance of self-reporting. This would have deleterious results for the efficiency of government, particularly where technological progress meant that government had an increasing need for certain information about its citizens to enable it to respond to the needs of society.[204]

The reasoning adopted in *Byers* is relevant to compelled production orders. Disclosing a password that may lead to incriminating evidence appears little different to disclosing one's name when such an action will lead to a criminal conviction. If the giving of one's name is an essentially neutral act, the giving of a password appears to warrant the same description. Indeed, as will be discussed in Chapter 4, the English Court of Appeal appears to have accepted this view. Also relevant from the *Byers* decision are the statements of Clarke J that modern living may require the use of modern scientific measures. The importance of that statement is in its finding that as society changes, some of those changes may require law enforcement changes to ensure that law enforcement is able to adequately protect the public. As noted in the Introduction to

---

201 Ibid 448. It bears noting that the concurring decision of Harlan J did not place any reliance in the idea that the privilege ought not to apply in instances where the disclosure of information would be of substantial assistance in a criminal prosecution.

202 Ibid 448.

203 Ibid 449.

204 451–2.

this thesis, encryption is an increasingly common facet of everyday life, something that many people use without even knowing it. As the growth of encryption has spread, evidence ordinarily obtainable by law enforcement officials has become harder to gather. Consistently with Clarke J's dicta, some restriction on the privilege may be appropriate to prevent the balance between individual rights and the public interest shifting too far in favour of the former.

The approach in *Byers* does, however, reveal some differences with the Australian jurisprudence on motor vehicle reporting obligations. As discussed in Part 1.2.4, Australian courts appear to accept that being compelled to provide driver details does implicate the privilege (though as will be discussed in Part 2.5.2., the statutes which grant those powers also abrogate the privilege). Despite that difference, when considering statutes of this nature Australian courts have engaged in the same weighing exercise that the court in *Byers* did and considered many of the same factors, with the only difference being that in *Byers* the outcome determined whether the privilege was engaged, whereas in Australia the outcome determined whether the privilege had been abrogated. The result in both instances was the same. The differences in this approach arise from the different rules each jurisdiction has regarding the abrogation of the privilege, an issue that is discussed in Chapters 2 and 4. Canada shares the Australian view that motor vehicle reporting obligations may infringe the privilege, but unlike Australia it has no tools such as the possibility of abrogation with which to alter the consequence of that finding.

1.3.2 Balancing in England and Wales

Reliance on a weighing of interests is explicitly undertaken by both the English courts and the European Court of Human Rights, though this was not always the case. While the early jurisprudence of the European Court of Human Rights held that the privilege was not absolute,[205] in both *Funke* and *Saunders* the Court showed some resistance to the idea of balancing the individual's interests against the public interest.

[205] See, eg, *Murray v United Kingdom* (1996) 22 EHRR 2, [47].

In *Funke*, the Court's decision was reached by overturning the earlier opinion of the European Commission of Human Rights. In respect of balancing, the majority opinion of the Commission stated that 'under the Convention System, there is an inherent balance between the legitimate interests of the community, on the one hand, and the individual rights it protects on the other'.[206] On the facts before it, and with that balancing exercise having been undertaken, the majority found that the privilege was not infringed. In one paragraph, however, the Court overturned the Commission's opinion, holding that the privilege had been infringed and with it the right to a fair trial under Article 6. Though the Court made no reference to the balancing of rights identified by the Commission, its rejection of the Commission's opinion without any reference to the balancing exercise performed by the Commission left open the question of whether that balancing exercise was appropriate.

The role of the public interest was subsequently considered in *Saunders*. After stating that the facts did not require the Court to decide whether the privilege was absolute or could be infringed in certain circumstances,[207] the Court proceeded to state that 'the vital public interest' in investigation and prosecuting fraud could not justify the use in criminal proceedings of compulsorily obtained incriminating statements made during a non-judicial investigation.[208] This approach, which refused to limit the scope of the privilege in order to account for the public interest,[209] was subsequently endorsed in *Heaney and McGuinness v Ireland* when the Court, after considering the *Saunders* decision, held that the 'security and public order concerns of the Government cannot justify a provision which extinguishes the very essence' of the privilege.[210]

---

206 *Funke* (1993) 16 EHRR 297, 314 [64].

207 An approach criticised in the dissenting judgment of Valticos J in which he stated that to elevate the privilege to an absolute rule 'would mean in many cases that society was left completely defenceless in the face of ever more complex activities in a commercial and financial world that has reached an unprecedented level of sophistication': *Saunders* (1997) 23 EHRR 313, 350.

208 Ibid 339–340 [74].

209 And which could easily be understood to afford the privilege an absolute nature that could not be subject to limitation: *Brown v Stott* [2003] 1 AC 681, 721 (Lord Hope).

210 *Heaney and McGuinness v Ireland* (2000) 33 EHRR 12, [57]–[58].

While the European Court of Human Rights was rejecting a balancing approach, the Privy Council, the decisions of which are persuasive authority in English courts, was accepting that the public interest played a significant role in determining the scope of the privilege. In *Brown v Stott*,[211] Brown was arrested at a superstore for theft. She was observed by the police to be drunk. After informing the police that she had travelled to the store by car, she was – pursuant to the *Road Traffic Act 1988* – instructed to identify whether she was the driver of the car. The issue before the Privy Council was whether being required to answer that question infringed the privilege. In separate concurring judgments, the Privy Council agreed that the right to a fair trial under Article 6 had not been infringed.

At the outset their Lordships expressed the clear view that the privilege was not to be treated as an absolute right under the *ECHR*.[212] Lord Bingham stated that the rights contained in Article 6 of the *ECHR*, including the privilege, were not absolute and were subject to 'limited qualification' if there was a 'proper public objective' behind the qualification.[213] When balancing the public and individual interests, any limitation on the privilege needs to be a proportionate response to the pursuit of a legitimate government aim.[214] To determine whether the government's aim is legitimate, consideration must be given to the public interest.[215] Their Lordships recognised that misuse of motor vehicles constituted a 'very serious problem' and thus the regulation of the use of motor vehicles constituted a legitimate aim in the public interest.[216]

---

211 [2003] 1 AC 681 ('*Brown*').

212 Ibid 722 (Lord Hope), 728 (Lord Clyde), 730 (Rt Hon Kirkwood). Lords Hope and Clyde were also critical of the *Saunders* decision for failing to fully examine the absolute nature or otherwise of the privilege.

213 Ibid 704. Lord Bingham further noted that the European Court of Human Rights had recognised that the *ECHR* required a balance to be achieved between the individual's rights and those of the community. See also the opinion of Lord Steyn who recognised that the privilege was not an absolute right and that a 'legitimate aim' can be taken into account in determining whether a breach has occurred: at 709.

214 Ibid 705 (Lord Bingham), 710 (Lord Steyn), 719, 722 (Lord Hope). See also the later decision in *R v K(A)* [2009] EWCA Crim 1640, [41] in which the Court of Appeal stated that the privilege and the right to a fair trial would not be violated provided 'the compulsion under which the information is obtained is of a moderate nature and the use of the evidence obtained by it represents a proportionate response to a pressing social need'.

215 *Brown* [2003] 1 AC 681, 720 (Lord Hope).

216 Ibid 704 (Lord Bingham), 710 (Lord Steyn), 722 (Lord Hope), 728 (Lord Clyde), 731 (Rt Hon Kirkwood). See also *R v Hertfordshire County Council, ex parte Green Industries Environmental Industries Ltd* 2 AC 412, 421 where the Court referred to the public interest in obtaining the information; *R v Kearns* [2002] EWCA Crim 748, [55] where the public interest required the

Their Lordships were further in agreement that the legislative provision in question was a proportionate response to the problem it sought to resolve. The legislation allowed but one question to be put to the suspect.[217] The answer to that question could not on its own incriminate the suspect (though it may provide a link in the chain of evidence that leads to conviction), and the consequences of non-compliance were 'moderate and non-custodial'.[218] Furthermore, Lord Bingham found that all motor vehicle drivers voluntarily subject themselves to a regulatory regime when they use a motor vehicle, that regime being imposed because of the potential harm caused by motor vehicles.[219] Finally, Lord Bingham stated that there was no obvious distinction between being required to provide a breath sample and to answer a question about who the driver of the vehicle was.[220] Of particular importance are Lord Bingham's comments regarding the fact that only one question could be asked the answer to which was not itself incriminatory – even though it might lead to incriminating evidence – for compelled production orders share that same feature.

Notwithstanding the apparent ambivalence shown by the European Court of Human Rights to a balancing of interests in *Saunders*, when handing down its decision in *Jalloh* the Court was explicit in stating that public interest concerns could be taken into account in determining whether there had been a breach of Article 6 – and by extension the privilege.[221] The Court found that under Article 6, the determination of whether a trial is unfair is made by weighing the public interest against the individual's interest in having the evidence against him obtained by lawful means. However, the public interest can never be such as to justify a measure that would 'extinguish the very essence of an applicant's defence rights, including the privilege…'.[222]

---

provision of the information. The Court also noted that the information could only be provided by the defendant.

217 *Brown* [2003] 1 AC 681, 705 (Lord Bingham), 710 (Lord Steyn), 723 (Lord Hope).

218 Ibid 705 (Lord Bingham), 728 (Lord Clyde), 731 (Rt Hon Kirkwood). See also *Weh v Austria* (2005) 40 EHRR 37, [54] where the Court noted that the question that was asked – who was the driver of the car? – was a simple question the answer to which was not 'in itself incriminating'.

219 *Brown* [2003] 1 AC 681, 705.

220 Ibid 705.

221 A lack of consistency by the Court in its decisions is a source of much criticism: see Choo, above n 85, 22 and the references cited in footnote 2.

222 *Jalloh* (2007) 44 EHRR 32, [97].

The reference to the essence of the privilege in *Jalloh*, terminology that has been adopted by later courts, appears to assign to the privilege two parts. At the heart of the privilege lies its core, one that cannot be limited in any way under Article 6. Beyond the core is a less vigorously protected penumbra. It is in the penumbra that, depending on the circumstances of each matter, the operation of the privilege may be restricted by statute. Certain acts can readily be identified which would fall within the essence or core of the privilege. It is uncontroversial that compelling a suspect to testify (without providing commensurate immunity), for example, would infringe the essence of the privilege. For if it was possible to compel such an action, it would be difficult to identify what, if anything, would be left of the privilege. By contrast, the extinguishment of the privilege in its penumbra does not limit its applicability to circumstances falling within its core. Identifying the boundary between the core and penumbra may not always be straightforward, however. To assist that determination and to identify if the 'essence' of the privilege has been extinguished, the Court in *Jalloh* identified the following factors that needed to be considered: 'the nature and degree of compulsion used to obtain the evidence; the weight of the public interest in the investigation and punishment of the offence at issue; the existence of any relevant safeguards in the procedure; and the use to which any material so obtained is put.'[223]

Though the wording of this test is different to the test applied by the Privy Council in *Brown*, in substance it is broadly the same. The public interest goes to the legitimacy of the government's aim in seeking a legislative limitation on the privilege, and the remaining three elements of the test are all factors to be assessed in determining whether the government's measures are proportionate.[224] On the *Jalloh* facts, the Court found that the measures were not appropriate as they used more force than was

---

223 Ibid [117]. Curiously, at para [101] the Court sets out the same test though without reference to the public interest.

224 See Andrew Ashworth, 'The Exclusion of Evidence Obtained by Violating a Fundamental Right: Pragmatism Before Principle in the Strasbourg Jurisprudence' in Paul Roberts and Jill Hunter (eds), *Criminal Evidence and Human rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012) 145, 152 where he notes that the Court applies 'proportionality reasoning'.

reasonable,[225] the public interest was at the lower end of the scale due to the small scale of the drug dealing involved,[226] and the evidence would be used to secure Jalloh's conviction.[227]

The *Jalloh* approach has been applied in subsequent cases heard by the European Court. In *O'Halloran and Francis v The United Kingdom*,[228] the question raised was whether the privilege was violated by requiring the registered owner of a motor vehicle to state who was driving the vehicle at the time it was caught speeding. The Court, after noting that the privilege was not absolute and that not all instances of direct compulsion would constitute a breach of the privilege,[229] proceeded to consider the factors set out in *Jalloh* to determine whether the measures in question extinguished the essence of the privilege.[230] The Court found that the information provided could not on its own result in a conviction;[231] there was no real risk of an unreliable admission;[232] drivers implicitly agreed to subject themselves to a regulatory regime;[233] the enquiry permitted by the legislation was limited;[234] and the public held an interest in having these matters

225 *Jalloh* (2007) 44 EHRR 32, [118].

226 Ibid [119]. This conclusion was criticised in the dissenting opinion of Judges Wildhaber and Caflisch who said that the assessment of whether the measures were proportionate should not be affected by the scale of Jalloh's drug dealing.

227 Ibid [121].

228 (2008) 46 EHRR 21 ('*O'Halloran and Francis*').

229 Ibid [53].

230 Ibid [55].

231 Ibid [60].

232 Ibid [59]

233 Ibid [57].

234 Ibid [58].

investigated and prosecuted.[235] As a result, the essence of the privilege had not been destroyed and, accordingly, the right to a fair trial had not been violated.[236]

As has been noted by Ashworth, the decisions in *Jalloh* and *O'Halloran and Francis* constitute a substantial rejection of the Court's original approach to the role of the public interest in determining whether the privilege has been violated.[237] Moreover, that shift appears to have been driven in large part by the decisions of the English judiciary and its use of the concepts of proportionality and balance.[238] Thus, despite the Court's early comments in *Saunders* that rejected a balancing assessment, by the time it handed down its decisions in *Jalloh* and *O'Halloran and Francis* a weighing of interests had become the Court's accepted approach.[239]

Two features of the motor vehicle reporting decisions analysed in this Part bear noting. First, the weighing exercise adopted by the English and European courts corresponds closely with that adopted in Australia and the United States with regard to motor vehicle reporting obligations. The Supreme Court of the United States has spoken of how the privilege should not 'compel substantial sacrifices in the efficient pursuit of other

---

235 Ibid [52]–[53]. The Court also rejected several arguments put forward by the applicants, including that 'the defendant could not be compelled on pain of penalty to provide information which only he was capable of providing' (at [40]) and that there were alternative means of obtaining the evidence that did no breach the privilege (at [41]). See also the Court's earlier decision in *Weh v Austria* (2005) 40 EHRR 37 in which the same issue arose. In that matter, however, the applicant did provide a response to the request for details of the driver of the motor vehicle, though the response given was inaccurate. The applicant was fined for providing misleading information. In a poorly reasoned judgment, the Court found that the privilege was not implicated, primarily on the basis that the applicant had not been charged with speeding but with failure to provide accurate information. As such, it was said, the issue of self-incrimination did not arise: at [50]. The Court also found that there was no suspicion directed to the applicant and that the possibility of the applicant being charged with speeding was 'remote and hypothetical': at [56]. The obvious problem with the Court's finding is that it was the compulsion to provide an answer that led to the false statement. Furthermore, in circumstances where the vehicle was registered in the applicant's name, he clearly would have fallen under suspicion and therefore it can hardly be suggested that the likelihood of being charged with speeding was remote.

236 *O'Halloran and Francis* (2008) 46 EHRR 21, [62]–[63].

237 Andrew Ashworth, 'Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism?' (2008) 30 *Cardozo Law Review* 751, 766. See also Ashworth, 'The Exclusion of Evidence Obtained by Violating a Fundamental Right', above n 225, 151.

238 Ashworth, 'Self-Incrimination in European Human Rights Law', above n 238, 764. See also Ian Dennis, 'The Human Rights Act and the Law of criminal Evidence: Ten Years On' [2011] 33 *Sydney Law Review* 333, 345.

239 See also Choo, 'Give Us What You Have', above n 127, 250.

governmental objectives' where limiting the privilege would 'significantly aid in criminal law enforcement'.[240] That language overlaps closely with the English requirement that there be a legitimate government interest in limiting the privilege. The result is that in both England and Wales and the United States, motor vehicle reporting obligations were found not to infringe the privilege after the competing interests had been weighed and a legitimate government interest identified. In Australia, the same balancing exercise resulted in a finding that the statute in question had abrogated the privilege, leading to the same results. Canada, alone, prohibits such obligations.

The second feature of these decisions is that the factors relied upon by the English and European courts are closely related to compelled production orders. In particular, like motor reporting obligations, compelled production orders seek to give effect to a proper public objective; the password on its own cannot result in a conviction; there is no risk of unreliable evidence; and the nature of the enquiry is limited. These common features suggest that compelled production orders may fall outside the scope of the privilege.

1.3.3 Balancing in Canada

In Canada, the question of whether the privilege has been infringed (and whether evidence obtained in contravention of the privilege is to be excluded from trial) involves a balancing of interests. In the context of s 7 of the *Canadian Charter*, the Supreme Court has stated that the application of the privilege requires 'balancing societal and individual interests as carefully as possible'.[241] In Part 1.2.3 above, several cases that engaged in a balancing exercise were considered. There is no need to repeat that analysis here. As those decisions demonstrated, each balancing exercise is determined on its own facts, with different factors considered on each occasion that a balancing exercise is performed. The result of this is that the outcomes of the balancing exercise will differ depending on the specific circumstances of each case.[242] The decisions of the

---

240 *Byers* 402 US 424, 448 (1971).

241 *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3, [75]. See also *R v White* [1999] 2 SCR 417, [47]; *Thompson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)* [1990] 1 SCR 425, [185] where La Forest J states that 'this court has made it clear that the community's interest is one of the factors that must be taken into account in defining the content of the principles of fundamental justice'.

242 *R v White* [1999] 2 SCR 417, [48].

Supreme Court in respect of similar orders reveal several factors that were applied in the balancing exercise which may be applicable to a compelled production order: any request for the password is likely to arise in adversarial proceedings;[243] the extent of the compulsion and consequent intrusion is limited;[244] the scope for abuse of power;[245] there is no risk of unreliable evidence;[246] the seriousness of the offence;[247] and the importance of the evidence in policing the offending conduct.[248]

The role of those factors in the specific context of the compelled production of a password will be further considered in Chapter 3.

1.3.4 Balancing in Australia

Australian courts routinely engage in a balancing exercise to determine whether the privilege is enlivened. In *Grollo v Bates*, the Federal Court held that the privilege was intended to ensure a balancing of 'the interests of accused persons, who until conviction are presumed to be innocent, with the interests of the victim and of the public'.[249] The Australian decisions on motor vehicle reporting obligations also identify a further occasion on which Australian courts engage in a balancing exercise: when determining whether a statute has abrogated the privilege.

Where courts have engaged in this balancing exercise, they have relied on considerations that include: the fact that bodily samples do not involve the creation of new evidence;[250] bodily samples and other real evidence do not entail a risk of unreliable evidence;[251] certain activities, such as driving a car, involve the person in question submitting to statutory obligations which may include an obligation to provide specific

243 *R v B (S.A.)* [2003] 2 SCR 678, [58]; *R v Fitzpatrick* [1995] 4 SCR 154, [36]-[37].

244 See, eg, *Stillman* [1997] 1 SCR 607, [90] (Cory J); *R v Beare* [1988] 2 SCR 387, [35]; *R v Fitzpatrick* [1995] 4 SCR 154, [38].

245 *R v Fitzpatrick* [1995] 4 SCR 154, [44]; *R v White* [1999] 2 SCR 417, [43]; *R v B (S.A.)* [2003] 2 SCR 678, [44].

246 *R v Beare* [1988] 2 SCR 387, [21]; *R v B (S.A.)* [2003] 2 SCR 678, [58]; *R v Saeed* [2016] 1 SCR 518, [59], [128].

247 *R v B (S.A.)* [2003] 2 SCR 678, [52]; *R v Saeed* [2016] 1 SCR 518, [128].

248 *Stillman* [1997] 1 SCR 607, [90] (Cory J); *R v Saeed* [2016] 1 SCR 518, [59], [128].

249 *Grollo v Bates* (1994) 53 FCR 218, 250.

250 *King v McLelland* [1974] VR 773, 777.

251 *Grollo v Bates* (1994) 53 FCR 218, 250.

information;[252] a statutory obligation to answer specific questions was strictly limited in scope;[253] and a provision requiring a suspect to provide an answer was intended to facilitate the investigation of offences, a purpose that would be severely undermined if a suspect could refuse to answer.[254] A number of those factors – which are the same as those relied upon by courts in England and Wales and the United States – are relevant to the requirement to provide a password to an encrypted device.

In Victoria and the Australian Capital Territory there is an additional element in play as both jurisdictions have human rights instruments that explicitly provide for the privilege against self-incrimination.[255] In Victoria, the *Victorian Charter* provides, in s 25(2)(k), that a person charged with a criminal offence has the right 'not to be compelled to testify against himself or herself or to confess guilt'.[256] However, this right, like all rights in the *Victorian Charter*, is not absolute and 'is subject to such reasonable limits imposed by law as can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom'.[257] How this operates in practice is evidenced in the case of *Re Application under the Major Crime (Investigative Powers) Act 2004*.[258]

Major Crime concerned a power under the *Major Crime (Investigative Powers) Act 2004* (Vic) which enabled a judge to issue a coercive powers order requiring a person to attend an investigation to give testimony. At the time that the matter was decided, s 39 of the Act provided that the privilege against self-incrimination was abrogated in exchange for which the witness was granted a direct-use immunity. As the Court there explained, '[a] 'direct use' immunity serves to protect the individual from having the compelled incriminating testimony used directly against him or her in a subsequent proceeding'.[259] The question before the Court was whether that immunity was compatible with the

252 *Loges v Martin* (1991) 13 MVR 405, 409.
253 *R v Hooper* (1995) 64 SASR 480, 486.
254 Ibid 486.
255 Queensland, too, is progressively introducing a new human rights statute that identifies the privilege as a protected right: *Human Rights Act 2019* (Qld).
256 The equivalent provision in the *Human Rights Act 2004* (ACT) is s 22(2)(i).
257 *R v Independent Broad-Based Anti-Corruption Commission* (2016) 256 CLR 459, 478 [71] (Gageler J).
258 (2009) 24 VR 415 ('*Major Crime*').
259 Ibid 422, [26].

protection granted by s 25(2)(k) of the *Victorian Charter*, or whether derivative-use immunity also needed to be granted. Derivative-use immunity provides 'a further step or protection' by '[insulating] the individual from having the compelled incriminating testimony used to obtain other evidence against that person'.[260]

Importantly, s 7 of the *Victorian Charter* states that the rights it recognises can be limited taking into account:

> (a) the nature of the right; and
> (b) the importance of the purpose of the limitation; and
> (c) the nature and extent of the limitation; and
> (d) the relationship between the limitation and its purpose; and
> (e) any less restrictive means reasonably available to achieve the purpose that the limitation seeks to achieve.[261]

Warren CJ noted that what the section requires is the striking of a balance between the privilege and the State's interest in investigating and prosecuting criminal conduct.[262] After considering the s 7 elements, her Honour concluded that s 25(2)(k) required the abrogation of the privilege to be accompanied by direct and derivative-use immunity.[263] A fuller discussion of this decision and the factors relied upon by Warren CJ takes place in Part 4.4.1.2 when considering the abrogation of the privilege in Victoria.

Notably, however, a finding that a statutory provision infringes the privilege does not invalidate that provision. Rather, the court is limited to issuing a declaration of inconsistent interpretation or, as occurred in *Major Crime*, interpreting the provision in such a manner as to remove the infringement.[264] In response to Warren CJ's conclusion in *Major Crime*, in 2014 the *Major Crime (Investigative Powers) Act 2004* (Vic) was amended through the insertion of a new s 39(4) which expressly excludes derivative-use immunity.[265] In passing that amendment, the Attorney-General, in providing the Statement of Compatibility, stated that the government viewed the amendment to be a

---

260 Ibid.

261 The equivalent provision in the *Human Rights Act 2004* (ACT) is s 28.

262 *Major Crime* (2009) 24 VR 415, 449 [149].

263 Ibid 451 [158].

264 *Victorian Charter* ss 32, 36. The interpretation of the *Victorian Charter* is considered further in Part 4.2.

265 The amendment was made through s 162 of the *Criminal Organisations Control and Other Acts Amendment Act 2014* (Vic).

'reasonable and justified limit on the privilege' taking into account the need for the provision to prosecute organised crime; the effect that derivative immunity would have in undermining the purpose of the legislation; the absence of any 'improper questioning techniques' which may affect the reliability of the evidence; and the fact that the evidence's admission would not undermine the accused's right to a fair trial.[266]

1.4 RECAPITULATION OF MAIN FINDINGS

Several relevant issues have been identified in the preceding analysis. In determining the scope of the privilege in respect of similar orders, courts have relied heavily on the use of a balancing exercise. This is the result of an acceptance by the courts that the privilege does not grant an absolute entitlement, but rather one that is subject to certain limitations which are identified using the balancing exercise. Across the jurisdictions that balancing assessment relied on common factors, at the heart of which was the need for a legitimate public objective. In respect of both the orders examined in this Chapter and compelled production orders, that requirement is satisfied. A legitimate public objective is not sufficient, however, as the mechanism used to achieve that objective must be proportionate. To adopt the terminology of the European Court of Human Rights, that mechanism must not extinguish the essence of the privilege. Whether it has that effect or not depends on the extent of the infringement imposed by the provision. In the case of both motor vehicle reporting obligations and compelled production orders, that infringement is limited to the asking of a single question the answer to which itself is not directly incriminating though it is expected to lead to incriminating evidence. This is an important factor as each of the United States Supreme Court, Privy Council and European Court of Human Rights have stated that providing one's name is a neutral act that does not implicate the privilege.[267] Note, however, that there are differences between providing one's name and providing the encryption key to an electronic device. Most notably, one's name is not a secret and can be found through other means.

---

266 Victoria, *Parliamentary Debates*, Legislative Assembly, 26 June 2014, 2382 (Robert Clark, Attorney-General).

267 *Byers* 402 U 424 (1971), 431-32; *Brown* [2003] 1 AC 681, 705 (Lord Bingham), 728 (Lord Clyde), 731 (Rt Hon Kirkwood); *O'Halloran and Francis* (2008) 46 EHRR 21, [60]; *Weh v Austria* (2005) 40 EHRR 37, [54].

Common to any weighing exercise of this nature is the strength of the public interest in law enforcement having the statutory power in question. While the public interest in motor vehicle reporting obligations and the taking of bodily samples for investigatory purposes is clear, the public interest in compelled production orders depends on the frequency with which encryption is encountered by law enforcement. If it is rarely encountered, the public interest may be low. As noted in the Introduction, however, it appears to be an increasingly common issue.

Further factors identified in this Chapter in respect of the related orders include the absence of a risk that any evidence obtained through the use of the provision in question is unreliable; the fact that no new evidence was created through the act of compulsion; and the potential sanction that may result from the use of information obtained using the provision in question. Those same factors are relevant to compelled production orders, and how each jurisdiction has weighed those factors provides some guidance for how they will respond to compelled production orders.

Across Australia, England and Wales and the United States, the outcome of that balancing exercise has been broadly consistent, with the result that the scope of the privilege in each of those jurisdictions is relatively uniform. For example, all of those jurisdictions accept restrictions on the privilege in respect of bodily evidence and other pre-existing evidence. For the privilege to apply, the suspect must disclose incriminating information or speak his or her guilt. This finding is relevant to compelled production orders which require the act of decryption to occur through the use of a fingerprint or other biometric feature, for it suggests that such conduct falls outside the scope of the privilege.

The exceptions to that uniformity are Canada and the decision of the European Court of Human Rights in *Jalloh*, both of which apply a broader scope to the privilege. In Canada, this feature is apparent in respect of motor vehicle reporting obligations, where it is the only jurisdiction to prohibit such obligations where they may lead to criminal charges, and the use of bodily evidence. In respect of the latter, bodily evidence initially appears

to fall within the scope of the privilege as it is evidence that an accused is coerced into providing. Importantly, though, that position is softened by the use of a balancing exercise that considers the public interest in determining whether the privilege has been breached. It is through such balancing that the use of fingerprints, blood samples and breathalyser tests have been allowed – evidence which is plainly obtained through the accused's coercion. Nevertheless, as the compelled production of an encryption key bears many similarities to motoring vehicle reporting obligations, Canada's divergence on this issue portends further differences in respect of compelled production orders.

There remains one further area of divergence between the jurisdictions, and it concerns when they utilise the balancing approach. In Canada, England and Wales and the United States, the balancing exercise is performed to determine the boundaries of the privilege.[268] While Australian courts have at times used balancing to determine the contours of the privilege, they have also engaged in a balancing exercise to determine whether statutory obligations impliedly abrogate the privilege. As will be discussed in greater detail in Chapter 2, the reason that this balancing exercise occurs when considering the question of abrogation is in part due to the relatively permissive rules in Australia regarding abrogation. Unlike Canada and the United States, Australia allows the abrogation of the privilege without a grant of direct and derivative-use immunity. With abrogation available as a tool to avoid the consequences of a specific act falling within the scope of the privilege, there is less need to find a way at the outset to keep that act beyond the privilege's reach.

With Chapter 1 having identified the scope of the privilege in respect of similar orders and the considerations that were relied upon to determine that scope, Chapters 3 and 4 will discuss whether compelled production orders fall within the scope. Chapter 3 is concerned with that question in respect of Canada and the United States; Chapter 4, England and Wales and Australia. The separation of the four jurisdictions into these two groups is the result of the different approaches adopted by the United States and Canada, and England and Wales and Australia, with the latter two jurisdictions

[268] Though on occasion Canadian courts also utilised it to determine whether evidence obtained in breach of the privilege should be excluded: see, eg, *Stillman* [1997] 1 SCR 607.

introducing broadly similar statutory responses to deal with the issue of compelled production orders.

Before then, however, Chapter 2 will consider the issues of abrogation and the exclusionary rules. The results of the decisions examined in this Chapter reveal the importance of those issues. In England and Wales and the United States, motor vehicle reporting obligations fell outside the scope of the privilege. In those jurisdictions for that particular search, therefore, issues of abrogation and exclusionary rules do not apply. By contrast, both Australia and Canada have recognised that motor vehicle reporting obligations can infringe the privilege. In this situation, abrogation and the exclusionary rules determine whether that finding on the scope of the privilege is determinative or not. In Australia, the privilege does not bar such obligations as it is abrogated to allow for them to be imposed; in Canada, by contrast, no such abrogation occurs. Thus, whether motor vehicle reporting obligations can be imposed is not determined solely by the scope of the privilege, but also by a jurisdiction's rules concerning abrogation and the exclusion of evidence. In the same way, the question of whether compelled production orders can be granted requires consideration not only of the scope of the privilege, but also of its possible abrogation and the exclusionary rules of the jurisdiction in question. Those latter issues are examined next in Chapter 2.

CHAPTER 2

EXCLUSIONARY RULES AND THE ABROGATION OF THE PRIVILEGE

2.1 INTRODUCTION

In Chapter 1, how the privilege has been applied to orders bearing similarities to compelled production orders was considered. That analysis was undertaken because the outcome of those decisions helps determine the scope of the privilege in the comparator jurisdictions, and the reasons that the courts relied upon in reaching their determinations may provide some guidance as to how those same courts will respond to an application for a compelled production order. In Chapters 3 and 4, this thesis will consider whether the manner in which the selected jurisdictions have resolved cases concerning compelled production orders is consistent with the principles identified in Chapter 1. Before then, however, this Chapter considers three issues that are relevant to the scope of the privilege: when is evidence that is obtained in breach of the privilege admissible in court; if compelled production orders infringe the privilege, can the privilege be abrogated; and if it can be, what conditions must be satisfied for that abrogation to occur?

The importance of these questions lies in the central role that abrogation plays in the Australian approach to compelled production orders and certain other related orders. In examining the scope of the privilege in Chapter 1, it was found that Australian courts stood apart from those in England and Wales and the United States in holding that certain motor vehicle reporting obligations infringed the privilege. Having so held, however, those courts further found that the statutory provisions imposing the motor vehicle reporting obligations abrogated the privilege. That those statutes had abrogated the privilege was determined after performing a balancing exercise that involved several of the same factors that the courts of England and Wales and the United States had relied upon to find that the privilege was not engaged by motor vehicle reporting obligations. In Chapter 4, it will be seen that Australian courts have continued this approach with compelled production orders: while such orders are likely to infringe the privilege, the statutory provisions that authorise the making of them also abrogate the

privilege. This Chapter analyses the principles regarding abrogation of the privilege not just in Australia, but in the comparative jurisdictions too. That will enable an examination of the similarities and differences that exist between the jurisdictions, which will help explain why abrogation of the privilege is a feature of compelled production orders in Australia and England and Wales but not Canada and the United States.

As was noted in Chapter 1 when considering the scope of the privilege, the status of the privilege in each of the jurisdictions differs. In Canada and the United States, the privilege receives constitutional protection; in England and Wales, the relevant provisions of the *ECHR* are incorporated into English law through the *Human Rights Act 1998*; and in Australia, the privilege receives no federal statutory or constitutional protection (though state-based legislation in Victoria and the Australian Capital Territory gives statutory recognition to the privilege).[1] These differences play a central role in the ease with which, and the conditions under which, abrogation may occur. In short, where constitutional protection is granted to the privilege, abrogation is not lightly undertaken and when it is strict conditions regarding immunity are imposed. By comparison, abrogation is easiest in Australia, where federally the privilege is found in the common law alone. More stringent rules concerning abrogation in the United States and Canada also make their respective exclusionary rules more significant – for if the privilege is infringed by a compelled production order, and the privilege cannot readily be abrogated, the question arises as to what happens to evidence obtained in breach of the privilege.

Parts 2.2 to 2.5 consider each of the jurisdictions in turn. For each jurisdiction, consideration is given to the ability of the legislature to abrogate the privilege; what, if any, immunity must be given to compensate for that act of abrogation; and the rules under which the courts of each jurisdiction exclude evidence that has been obtained in breach of the privilege. Part 2.6 analyses those findings.

---

[1] Queensland, too, has recently implemented a human rights statute the provisions of which will progressively commence in coming years: *Human Rights Act 2019* (Qld).

The first jurisdiction examined is the United States.

2.2 UNITED STATES

2.2.1 Exclusion of evidence

The exclusionary rule in the United States regarding evidence obtained in breach of the Fifth Amendment was set down in *Miranda v Arizona*.[2] For purposes of this thesis, that case and its exclusionary rule can be briefly described. As part of a rape investigation, the police apprehended Miranda and put him in a police line-up in which he was identified by the victim. He was thereafter placed in an interrogation room and interrogated for two hours by two police officers, after which he confessed to the offending. He was convicted on the basis of that conviction. At no point prior to his interrogation, however, was he informed of his right not to incriminate himself or the right to speak to a lawyer.[3] On appeal to the Supreme Court, the admissibility of his confession was challenged.

In finding that Miranda's confession was inadmissible, the Court held that the 'prosecution may not use statements…stemming from custodial interrogation of the defendant unless it demonstrates the use of procedural safeguards effective to secure the privilege against self-incrimination'.[4] The need for such safeguards arose because the entire purpose of police interrogation 'was to put the defendant in such an emotional state as to impair his capacity for rational judgment'.[5] To ensure that a suspect's Fifth Amendment rights are given effect to, the suspect must be informed of his or her right to speak to a lawyer and not to incriminate him- or herself.[6] The failure to comply with those requirements results in a breach of the privilege, the result of which is the exclusion of any evidence from trial that was obtained through that breach.

Thus, in the context of a compelled production order, if a suspect is informed that he or she is not required to disclose the password and chooses to do so, he or she has acted

---

2 384 US 436, 491-2 (1966).
3 Ibid.
4 Ibid 444.
5 Ibid 465.
6 Ibid 467-9.

voluntarily and the privilege is not implicated. If, however, he or she is not advised of his or her rights and is coerced or tricked into providing the password in breach of the privilege, any evidence subsequently found on the electronic device in question will be inadmissible.

2.2.2 Abrogation of the privilege and grants of immunity

In *Kastigar v United States*,[7] the Supreme Court set out the essential principles concerning grants of immunity. Two questions arose in that matter: could a witness be compelled to give evidence if the government granted the witness immunity; and, if so, did the witness need to be granted direct immunity (for his or her testimony), direct and derivative-use immunity (for evidence discovered from the compelled testimony), or full transactional immunity (which grants immunity from prosecution for the offence to which the testimony relates)?[8] Powell J, delivering the Court's opinion, answered the first question in the affirmative.[9] With regard to the second question, Kastigar argued that for the immunity to satisfy constitutional requirements it needed to provide full transactional immunity.[10] Powell J rejected that argument, holding that the immunity only needed to be 'coextensive with the scope of the privilege', which would occur if direct and derivative-use immunity was granted.[11] The privilege, Powell J noted, was not intended to prohibit prosecution, but merely the use (and derivative use) of compelled testimony in such prosecution.[12]

In the United States, then, the constitutional status of the privilege impacts not only the exclusionary rules but also the ability of the legislature to abrogate the privilege. In both

---

7 406 US 441 (1972).

8 The witnesses in question were refusing to provide evidence notwithstanding the grant of immunity.

9 *Kastigar v United States* 406 US 441, 448 (1972).

10 This argument was based on the Court's earlier decision in *Counselman v Hickman* 142 US 547 (1892).

11 *Kastigar v United States* 406 US 441, 449 (1972). See also *Murphy v Waterfront Commission of New York Harbor* 378 US 52 (1964) (Goldberg J) at 54 and 79 where it is said that the grant of direct and derivative-use immunity places a witness 'in substantially the same position as if the witness had claimed his privilege'.

12 *Kastigar v United States* 406 US 441, 453 (1972). See also *Murphy v Waterfront Commission of New York Harbor* 378 US 52, 107 (1964) where White J, in a concurring opinion, states that the grant of immunity 'must be as broad as, but not harmfully and wastefully broader than, the privilege against self-incrimination'.

circumstances the outcome is straightforward: the privilege, as a constitutional right, cannot be abrogated without a grant of immunity that is 'coextensive with the scope of the privilege', which includes both direct use and derivative use immunity; and where evidence is obtained in breach of the privilege, its exclusion automatically follows. As will be seen in Part 2.3 below, the same position broadly holds true in Canada – the other jurisdiction in which the privilege receives constitutional protection.

2.3 CANADA

2.3.1 Exclusion of evidence

Prior to the introduction of the *Canadian Charter*, evidence that was obtained unlawfully was nevertheless broadly admissible in proceedings provided it was relevant, even if the illegality entailed the breach of a right contained in the Bill of Rights.[13] Thus while involuntary admissions were automatically excluded, any derivative evidence found as a result of those admissions was admissible on the basis that its reliability outweighed any self-incrimination concerns.[14]

Since the introduction of the *Canadian Charter*, the exclusion of evidence has been governed by the provisions of s 24(2), which provides that:

> Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

The wording of the section gives rise to two elements that need to be satisfied before evidence is to be excluded: the evidence needs to have been obtained in a manner that violated a *Canadian Charter* right; and the admission of that evidence must bring the administration of justice into disrepute.[15]

---

13 Robert J Sharpe and Kent Roach, *The Charter of Rights and Freedoms* (Irwin Law, 2009), 299; Peter W Hogg, *Constitutional Law of Canada* (Carswell, 2011), 41.2; *The Queen v Wray* [1971] SCR 272, [40]; *Hogan v R* [1975] 2 SCR 574, 48 DLR (3d) 427. See, however, *R v Rothman* [1981] 1 SCR 640 in which the Court held that confessions could be excluded where they might be untrue or where their admission would bring the administration of justice into disrepute.

14 The *Queen v Wray* [1971] SCR 272. See also *R v Grant* [2009] 2 SCR 353, [117].

15 See, eg, *R v Strachan* [1988] 2 SCR 980, [45]; *R v Bartle* [1994] 3 SCR 173, [47].

In respect of the first element, the Supreme Court has held that it does not require a strict causal connection between the *Canadian Charter* breach and the obtaining of the evidence in question.[16] Instead, the 'entire chain of events during which the Charter violation occurred and the evidence was obtained' is to be considered.[17] Thus, if the evidence is obtained 'as part of the same transaction or course of conduct' that constituted a breach of the *Canadian Charter*, a sufficient relationship for purposes of s 24(2) will have been established.[18] The first element can therefore be satisfied by a mere temporal connection, though the existence of a temporal connection is not necessarily determinative and each case is to be assessed on its own merits.[19] The relationship requirement can also be satisfied by a causal connection or a contextual connection, or a combination of a temporal, causal and combination connection.[20]

The second element of the s 24(2) test is whether admitting the evidence would bring the administration of justice into disrepute. Until 2009, the leading decisions on this element were *R v Collins*[21] and *Stillman*.[22] In *Collins*, the Court stated that the disrepute with which s 24(2) was concerned was that which would result from admitting evidence that would affect the fairness of the trial.[23] The disrepute was to be judged through the eyes of 'a reasonable man, dispassionate and fully apprised of the circumstances of the case'.[24] The Court in *Collins*, and later *Stillman*, identified three factors that needed to be considered to determine if the admission of the evidence would bring the administration of justice into disrepute.[25]

---

16 See, eg, *R v Bartle* [1994] 3 SCR 173, [48]; *R v Strachan* [1988] 2 SCR 980, [48]; *R v Wittwer* [2008] 2 SCR 235, [21]; *R v Burlington* [1995] 2 SCR 206, [115].

17 *R v Strachan* [1988] 2 SCR 980, [55]. See also *R v Burlington* [1995] 2 SCR 206, [41].

18 *R v Wittwer* [2008] 2 SCR 235, [21].

19 See, eg, *R v Strachan* [1988] 2 SCR 980, [55].

20 *R v Wittwer* [2008] 2 SCR 235, [21]. The Court found temporal, causal and contextual connections in this matter: at [22].

21 [1987] 1 SCR 265 ('*Collins*').

22 [1997] 1 SCR 607.

23 *Collins* [1987] 1 SCR 265, [42] (Lamer J).

24 Ibid [44] (Lamer J).

25 One of the effects of the *Collins* test was to lower the threshold at which exclusion of evidence became necessary compared to the earlier test prior to the *Canadian Charter*. Under the pre-*Canadian Charter* test, evidence was only excluded where its admission would shock the community: *R v Burlington* [1995] 2 SCR 206, [70] (L'Heureux-Dube J); *Collins* [1987] 1 SCR 265, [52] (Lamer J).

The first factor was the nature of the evidence and whether its introduction would affect the fairness of the trial. Conscriptive evidence, which included any evidence obtained (including derivative evidence) through compelling a suspect 'to incriminate himself at the behest of the state by means of a statement, the use of the body or the production of bodily samples', always rendered a trial unfair.[26] The second factor was the seriousness of the *Canadian Charter* violation and the cause of the violation;[27] and the third involved assessing the consequences of excluding the evidence against those of admitting it.[28]

In *R v Grant*, the Court amended the *Collins*/*Stillman* test. McLachlin CJC and Charron J wrote the majority judgment. Their Honours noted that the concept of trial unfairness under the first leg of the *Collins* test had introduced new problems and left little work for the remaining two legs of the test.[29] One of the problems caused by the test was the near automatic exclusion of evidence that was deemed to be conscriptive,[30] an outcome inconsistent with the language used in s 24(2).[31] In place of the *Collins*/*Stillman* test, the Court identified the following three elements that needed to be assessed in a s 24(2) enquiry:

> (1) the seriousness of the Charter-infringing state conduct (admission may send the message the justice system condones serious state misconduct), (2) the impact of the breach on the Charter-protected interests of the accused (admission may send the message that individual rights count for little), and (3) society's interest in the adjudication of the case on its merits.[32]

Under the first leg of the test, the focus of the enquiry is the preservation of public confidence in the judicial system. This necessarily entails an examination of the gravity of the state's conduct that resulted in the *Charter* violation, with exclusion of evidence

---

26 *Stillman* [1997] 1 SCR 607, [80].

27 *Collins* [1987] 1 SCR 265, [49] (Lamer J).

28 Ibid [50] (Lamer J).

29 *R v Grant* [2009] 2 SCR 353, [62] ('*Grant*').

30 *Grant* [2009] 2 SCR 353, [64]–[65]. See also David M Paciocco, 'Self-Incrimination: Removing the Coffin Nails' (1989) 35 *McGill Law Journal* 73, 77, 97.

31 *Grant* [2009] 2 SCR 353, [60]. See also Hogg, above n 13, 41-12 where Hogg notes that the definition of conscriptive evidence as applied by the courts was so broad it included self-incriminating evidence that had been voluntarily provided by the suspect.

32 *Grant* [2009] 2 SCR 353, [71].

more likely in cases of severe or deliberate breaches.[33] Evidence will be more likely to be admitted where the police officers acted in good faith.[34]

The second leg of the test is concerned with the severity of the impact of the breach on the accused's *Canadian Charter* rights: the more serious the infringement, the greater the effect on the repute of the justice system and the more likely the exclusion of the evidence.[35] The seriousness of the infringement is assessed by looking at 'the interests engaged by the infringed right and [examining] the degree to which the violation impacted on those interests'.[36]

The third leg considers whether the admission or exclusion of the evidence will assist or hinder the truth-seeking function of the courts.[37] Merely because evidence is reliable does not mean it will be admitted where there has been a *Canadian Charter* breach, though 'the reliability of the evidence is an important factor in this line of enquiry'.[38] In a similar vein, the importance of the evidence to the state's case is also relevant – the more important the evidence, the more likely it is to be admitted.[39]

As for the effect that the new test would have in practice, the majority noted that certain evidence, including statements made by an accused in breach of the privilege, would remain presumptively inadmissible.[40] In respect of bodily evidence such as DNA and breathalyser tests that were obtained in a manner that breached the *Canadian Charter*, McLachlin CJC and Charron J found that bodily samples 'are not communicative in nature', thereby 'weakening self-incrimination as the sole criterion for determining their admissibility'.[41] That bodily samples are also highly reliable sources of evidence

---

33 Ibid [73].

34 Ibid [75]. This suggests a change from the early jurisprudence of the Court: Hogg, above n 13, 41-17 and the cases there cited, including *R v Therens* [1985] 1 SCR 613.

35 *Grant* [2009] 2 SCR 353, [76].

36 Ibid [77].

37 Ibid [79].

38 Ibid [80]–[81].

39 Ibid [83]. In *R v Saeed* [2016] 1 SCR 518, Abella J in dissent notes at [160]-[162] that this third leg has given rise to some confusion in the case law, with courts frequently departing from the guidelines set out in *Grant*.

40 *Grant* [2009] 2 SCR 353, [92].

41 Ibid [105].

favoured their admission,[42] as did the fact that some bodily evidence could be obtained by less intrusive means than others.[43]

The issue of derivative evidence was also altered by the Court's decision. In place of the automatic exclusion of evidence that could not have been discovered but for the *Canadian Charter* breach,[44] the three legs of the s 24(2) test are to be applied instead.[45] Discoverability remains a relevant consideration, however, as it relates to the causal connection between the self-incriminating act and the evidence – the causal connection being reduced in instances where the evidence is otherwise discoverable.[46]

How will that exclusionary rule operate in respect of encrypted electronic data? Where the police obtain access to encrypted material through a breach of the privilege, that material will be excluded under s 24(2) and the *Grant* test. For example, in *R v Shin*,[47] Shin's apartment was searched pursuant to a search warrant. During the search a cell phone belonging to Shin was found. Shin was arrested and questioned in violation of his *Canadian Charter* rights, during which he revealed the password to the phone. At trial, evidence of the contents of that phone was excluded under s 24(2).[48] There is little about that outcome that is surprising. The *Canadian Charter* infringement was serious, in bad faith, and eviscerated Shin's right to the privilege. The admission of such evidence would have caused substantial damage to public confidence in the judiciary.

2.3.2 Abrogation of the privilege and grants of immunity

Canadian law recognises that where a statute seeks to compel a person to provide incriminating evidence, that compulsion will ordinarily only be lawful if the person in question is granted immunity, including derivative-use immunity.[49] This position arises

---

42 Ibid [110].

43 Ibid [103]–[104]. Note, however, that the taking of more intrusive bodily samples, such as a blood sample, would be more likely to be excluded than a less intrusive measure such as fingerprinting: at [109].

44 See, eg, *Thompson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)* [1990] 1 SCR 425, [209]-[211].

45 *Grant* [2009] 2 SCR 353, [121].

46 Ibid [122].

47 *R v Shin* 2015 ONCA 189.

48 Ibid [45].

49 *British Columbia (Securities Commission) v Branch* [1995] 2 SCR 3, [7], [40].

from an understanding that the grant of immunity is intended to operate in the same manner as the privilege that it displaces.[50] As the purpose of the privilege is to prevent a person from being conscripted to provide evidence against themselves,[51] a grant of immunity needs to be broad enough to encompass derivative evidence, which is understood to be any evidence that 'results, in fact, from a compelled disclosure'.[52] Not all derivative evidence, however, will be excluded under s 24(2), and thus not all derivative evidence requires a grant of immunity. If the evidence could have been obtained without the suspect's participation and without a breach of the *Canadian Charter*, immunity is not required.[53]

In respect of both the exclusionary rules and abrogation, Canada and the United States share many similarities. Regarding abrogation, it can only occur in circumstances where direct and derivative-use immunity is granted in exchange for that act of abrogation. In the context of compelled production orders, that requirement means they are of no assistance to prosecuting the recipient of the order, a substantial problem as many such orders are sought for that purpose. As for the exclusionary rules in the two jurisdictions, both *Miranda v Arizona* and *Grant* will have the effect of excluding any evidence obtained from unlawfully compelling a suspect to provide his or her password to an encrypted electronic device.

2.4 ENGLAND

Under English common law, evidence that is relevant and reliable is admissible in court regardless of the way it was obtained, even if obtained through illegal means.[54] There existed, however, a judicial discretion to exclude evidence that would be unfair or

50 *R v S (R.J.)* [1995] 1 SCR 451, [84] (Iacobucci J).

51 Ibid [88] (Iacobucci J).

52 Ibid [170] (Iacobucci J).

53 Ibid [191], [197], [200] (Iacobucci J).

54 See, eg, *R v Button* [2005] EWCA Crim 516, [12] citing *R v Sang* [1980] AC 402; *Allan v United Kingdom* (2002) 36 EHRR 12, 143; *R v Khan (Sultan)* [1997] AC 558; *Khan v United Kingdom* (2001) 31 EHRR 45, 1016. See also *R v Hertfordshire County Council, ex parte Green Industries Environmental Industries Ltd* [2000] 2 AC 412 at 421 where Lord Hoffmann noted that English courts treated the admission of an involuntary statement differently to evidence obtained as a result of that statement.

prejudicial to the accused.[55] With the introduction of the *Police and Criminal Evidence Act 1984* ('*PACE*'), the exclusion of evidence is primarily determined under s 78 of that statute. It provides that:

> In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.[56]

The starting position, then, is that while there is no automatic exclusionary rule in circumstances where evidence is obtained in breach of the privilege, such evidence may be excluded under s 78. How s 78 is to be interpreted will be considered after a brief examination of the approach taken by the European Court of Human Rights to Article 6 of the *ECHR* and the right to a fair trial. This is because both provisions seek to achieve the same purpose and the European Court of Human Right's opinions on Article 6 are relevant to, and have influenced the interpretation of, s 78 of *PACE*.

The European Court of Human Rights has recognised that rules regarding the exclusion of evidence are 'primarily a matter for regulation under national law'.[57] As a result, when asked to rule on the effect of improperly obtained evidence on the conduct of a trial, the Court does not as a matter of principle exclude illegally obtained evidence; rather, it determines whether the admission of the evidence undermines the suspect's right to a fair trial.[58] In Chapter 1, the role of balancing in determining the scope of the privilege was examined. That discussion showed how the *Jalloh* Court identified four criteria that are to be assessed to determine if the essence of the privilege has been extinguished.[59] If such extinguishment has occurred, the trial will be unfair if the

---

55 See, eg, *R v Sang* [1980] AC 402. This discretion has been retained in s 82(3) of *PACE* which provides that the Act does not 'prejudice any power of a court to exclude evidence…at its discretion'.

56 The use of the word 'may' in s 78 is potentially misleading. Where the court has determined that the admission of the evidence would render the trial unfair, the evidence is required to be excluded: *R v Chalkley* [1998] 2 Cr App R 79, 105.

57 *Gafgen v Germany* (2011) 52 EHRR 1, [162]. See also *Ibrahim v United Kingdom* (2015) 61 EHRR 9, [196]; *Jalloh* (2007) 44 EHRR 32, [94].

58 *Schenk v Switzerland* (1988) 13 EHRR 242, 265 [46]; *Khan v United Kingdom* (2001) 31 EHRR 45; *Heglas v Czech Republic* (2009) 48 EHRR 44; *Ibrahim v United Kingdom* (2015) 61 EHRR 9, [196].

59 Those criteria are: the compulsion used to obtain the evidence; the public interest; procedural safeguards; and how the material was used.

evidence obtained in breach of the privilege is admitted.[60] This approach was subsequently applied in *O'Halloran and Francis*.[61]

Building on that foundation, in *Gafgen v Germany*[62] the applicant had abducted and killed a child before demanding a ransom from the child's parents. The applicant was arrested after collecting the ransom and, while held by police, was threatened with physical harm if he failed to reveal the location of the child, who was still believed to be alive. As a result of the threats, the applicant gave the location of the body. Following his conviction for murder and kidnapping, the applicant challenged his conviction on grounds including that the confession and real evidence found as a result of that confession had been obtained in breach of the privilege. The admission of evidence obtained as a result of those breaches was said to constitute a breach of Article 6 of the *ECHR*.

The Court stated that in assessing whether the proceedings as a whole were fair, it was necessary to consider whether Gafgen had an opportunity to challenge the authenticity of the evidence; whether the evidence was reliable; how the evidence was obtained; whether the manner in which the evidence was obtained affected its reliability; and whether the evidence was decisive in the Court reaching its decision.[63] On the facts, the Court held that the privilege had not been infringed as it was only implicated in instances where the government used evidence obtained in breach of the privilege to secure the accused's conviction, which had not occurred in this matter as the conviction was found to have been based on a second confession given at trial.[64]

While the factors set out by the Court in *Gafgen v Germany* to determine trial fairness sit slightly at odds with the Court's test in *Jalloh* concerning breaches of the privilege,

---

60 *Jalloh* (2007) 44 EHRR 32, [117]-[123].

61 *O'Halloran and Francis* (2008) 46 EHRR 21.

62 (2011) 52 EHRR 1.

63 Ibid [164].

64 Ibid [186]. This finding was the subject of a strong dissent by Rozakis, Tulkens, Jebens, Ziemele, Bianku and Power JJ. They argued, at [O-II6], that the second confession on which the majority said the trial judge's decision was based only occurred after the tainted evidence had already been admitted and Gafgen's guilt established. Without the tainted evidence first having been admitted, it was highly unlikely that Gafgen would have made the second confession.

they are directed to the same purpose and reference largely the same considerations. The tests can, therefore, be reconciled by an approach which recognises that where evidence has been obtained in a manner that destroys the essence of the privilege, that factor alone renders the trial unfair.[65] If the essence of the privilege is not destroyed, however, trial fairness will not be infringed. This understanding is consistent with the Court's oft-repeated statement that the privilege and the right to silence are 'generally recognised international standards which lie at the heart of the notion of fair trial procedures under art.6'.[66] Furthermore, it continues the approach adopted in *Saunders* which identified the connection between the privilege and the exclusionary rule.[67]

With that background, the recent decision of the Supreme Court in *Beghal v Department of Public Prosecutions*[68] reiterates the principles regarding the abrogation of the privilege and grants of immunity and provides guidance on the treatment of evidence obtained through compulsory questioning where the privilege has been abrogated. The defendant had been stopped and questioned at the airport on her return from a visit to France where her husband was in custody on terrorism offences. The questioning was in accordance with the *Terrorism Act 2000*, which allowed nominated officers to detain and question a person for six hours without the need for reasonable suspicion in order to assess whether the person may have been involved in acts of terrorism. Beghal refused to answer the questions, which constituted a violation of the Act for which she

---

65 Such an approach is consistent with statements made by the Court in *Heglas v Czech Republic* (2008) 48 EHRR 1018, [40] where the Court, in relation to the role of the public interest, stated that it 'cannot justify measures emptying the applicant's rights of defence of their very substance, including that of not contributing to its own incrimination…'. See also Andrew L-T Choo, 'Give Us What You Have – Information, Compulsion and the Privilege Against Self-Incrimination as a Human Right' in Paul Roberts and Jill Hunter (eds), *Criminal Evidence and Human rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012) 239, 250 where he states that Article 6 is breached where the essence of the privilege has been destroyed.

66 *Gafgen v Germany* (2011) 52 EHRR 1, [168].

67 *Jalloh* (2007) 44 EHRR 32, [O-II15]. The majority in *Saunders* was clear in stating that the use of evidence obtained in breach of the privilege constituted a 'marked departure' from 'one of the basic principles of a fair procedure' under Article 6, and that the complexity of the crime and the public interest in having such crimes investigated did not justify such a marked departure: *Saunders* (1997) 23 EHRR 313, 340 [74]. See also the concurring opinion of Walsh J, in which he held that the trial was unfair because evidence was admitted which had been obtained in breach of the privilege: *Saunders* (1997) 23 EHRR 313, 344.

68 [2016] AC 88 ('*Beghal*').

was subsequently convicted. She appealed her conviction on grounds that included the violation of her privilege against self-incrimination.[69]

Lord Hughes delivered the leading judgment of the Court. His Lordship noted that the privilege is not absolute and may be abrogated by statute, either expressly or by necessary implication.[70] Where a statute compelled a person to answer questions, the statute might expressly exclude the privilege; provide immunity in respect of any answers given; or do neither of those things.[71] On the facts before him, Lord Hughes found that the privilege was not intended to apply to a person subject to compulsory questioning under the Act.[72] He found so for two reasons: first, the risk of prosecution in respect of an answer was low as the legislation was aimed at information for purposes of prosecuting others; and secondly, s 78 of *PACE* would result in the exclusion of any evidence deriving from those answers.[73]

Both reasons are relevant to the thesis question. The first because compelled production orders are often sought to find evidence against the recipient of the order, meaning the risk of prosecution is high. That suggests compelled production orders are more likely to implicate the privilege. Regarding the second reason, Lord Hughes stated that s 78 provided for the exclusion of evidence where the manner in which it had been obtained rendered the trial unfair. His Lordship thereafter found that there was no circumstance in which evidence obtained under the compulsory powers in issue before him would not fall to be excluded from trial.[74] This was so as 'evidence obtained from the defendant himself…by means of legal compulsion is a classic case of evidence which it will be unfair to admit.'[75] Furthermore, Article 6 of the *ECHR*, which bound the Court under the *Human Rights Act 1998*, fortified this finding as it, too, required exclusion of

---

69 Ibid 102-3 [12]-[13].

70 Ibid 117 [61]. See also *Bishopsgate Investment Management Ltd v Maxwell* [1993] Ch 1 (where the Court noted that if statutes are silent on the granting of immunity, courts are inclined to find that no immunity has been granted); *R v K(A)* [2009] EWCA Crim 1640, [19]; *Phillips v News Group Newspapers Ltd* [2013] 1 AC 1, [11]; *R v Mushtaq* [2005] UKHL 25, [49] (also [2005] 1 WLR 1513).

71 *Beghal* [2016] AC 88, 118 [63].

72 Ibid 118 [64]. This finding was disputed by Lord Kerr in dissent at [115].

73 Ibid 118 [65].

74 Ibid 118 [65].

75 Ibid 118 [66].

compulsorily obtained answers.[76] As will be discussed further in Chapter 4, the question that arises from this decision is whether the act of providing a password is to be categorised in the same way as questioning under the *Terrorism Act 2000*, with the result that, if it is, such evidence ought to be automatically excluded from trial.

2.5 AUSTRALIA

2.5.1 Exclusion of evidence

Until relatively recently, the exclusion of evidence was dealt with under the common law. In *R v Ireland*, Barwick CJ held that where evidence was obtained by unlawful or unfair means, judges had a judicial discretion to exclude that evidence.[77] In deciding whether to exercise that discretion, the judicial officer needed to consider the public interest in securing a conviction and the 'public interest in the protection of the individual from unlawful and unfair treatment'.[78] The Court's statements on this issue were later considered in *Bunning v Cross*, a case concerning the admissibility of an illegally conducted breathalyser test which showed the accused to have a blood alcohol reading in excess of the statutory maximum. After noting that *R v Ireland* correctly stated the law regarding judicial discretion, it was observed by Stephen and Aickin JJ that the balancing assessment did not require that unfairness to the accused be placed at the central point of the enquiry; rather, the balancing assessment was 'concerned with broader questions of high public policy, unfairness to the accused being only one factor which, if present, will play its part in the whole process of consideration'.[79]

Factors that Stephen and Aickin JJ took into account in finding that a breathalyser test should be admitted included the lack of any deliberate disregard of the law by the police;[80] the fact that the illegality did not affect the 'cogency of the evidence';[81] and the

---

76 Ibid 118 [66]. It is to be noted that the privilege was found not to be enlivened on the facts: at [69].

77 *R v Ireland* (1970) 126 CLR 321, 335.

78 Ibid 335.

79 *Bunning v Cross* (1978) 141 CLR 54, 72, 74-75. On the facts, Stephen and Aickin JJ found that there was no unfairness to an accused in having an unlawful but properly performed breathalyser test admitted into evidence, as there was no unfairness in admitted real evidence that had been found on an accused pursuant to an unlawful search: at 77-78.

80 Ibid 79.

81 Ibid 79. See also the opinion of Barwick CJ at 64-65.

nature of offence.[82] Barwick CJ, in a concurring judgment, noted that another relevant factor was the prejudice that may arise from the exclusion of the evidence.[83]

The discretion described in *Bunning v Cross* is not the only discretion under which evidence can be excluded. In *Police v Dunstall*,[84] the High Court, in considering a challenge to the admission of breathalyser test results, described the exclusionary rules available to courts. The Court noted that there were three discretions by which evidence could be excluded: the general 'fairness discretion' set out in *R v Lee*,[85] which provides for the exclusion of voluntary statements where they were obtained as a result of a trick or other police conduct; the *Christie*[86] discretion, which provides for exclusion where the probative value of the evidence is outweighed by the risk of prejudice to the accused; and the *Bunning v Cross*[87] discretion described above.[88] The majority also noted that intermediate appellate courts had recognised a further residual discretion to exclude evidence where its admission would result in unfairness to the accused.[89] Nettle J, in a concurring opinion, stated that there was 'no doubt' that such a residual discretion exists.[90] The purpose of the general fairness discretion is to ensure 'a fair trial according to law', which may require the exclusion of otherwise admissible evidence where its admission created a risk that justice would miscarry.[91]

Since the enactment of the uniform evidence legislation in many Australian jurisdictions, however, the exclusionary rules are governed by statute.[92] The *Christie* discretion is provided for in s 137 of the uniform legislation; the *Bunning v Cross* discretion in s 138

---

82 Ibid 80.

83 Ibid 64-65.

84 (2015) 256 CLR 403

85 (1950) 82 CLR 133, 159.

86 *R v Christie* [1914] AC 545.

87 (1978) 141 CLR 54.

88 *Police v Dunstall* (2015) 256 CLR 403, 416-17 [26] (French CJ, Kiefel, Bell, Gageler and Keane JJ).

89 Ibid 416-17 [26] (French CJ, Kiefel, Bell, Gageler and Keane JJ).

90 Ibid 429 [59]. See also *Harriman v R* (1989) 167 CLR 590, 594-5 (Brennan J); *Haddara v R* (2014) 43 VR 53, 61-62 [24]-[26], 70 [50]; *Rozenes v Beljajev* [1995] 1 VR 533, 548.

91 *Police v Dunstall* (2015) 256 CLR 403, 435 [83]. The general unfairness discretion is applied after weighing the public interest against those of the defendant: at 424 [48] (French CJ, Kiefel, Bell, Gageler and Keane JJ). See also *Haddara v R* (2014) 43 VR 53, 58 [14].

92 *Evidence Act 1995* (Cth); *Evidence Act 1995* (NSW); *Evidence Act 2001* (Tas); *Evidence Act 2008* (Vic); *Evidence Act 2011* (ACT); *Evidence (National Uniform Legislation) Act 2011* (NT).

and the *Lee* discretion in s 90.[93] As for the residual general fairness discretion, the Victoria Court of Appeal has held that it remains available to judges and has not been removed by the introduction of the uniform legislation.[94]

2.5.2 Abrogation of the privilege and grants of immunity

Given the importance of the privilege, it is presumed that the legislature does not intend for its abrogation.[95] However, abrogation can occur by statute, through express words or by implication.[96] Where the statutory obligation to provide answers is expressed in general terms, the privilege can only be impliedly excluded if 'it appears from the character and purpose of the provision in question that the obligation was not intended to be subject to any qualification'.[97] Abrogation may also be implied if a failure to do so undermines the purpose of the statute.[98] In *R v Hooper*, when assessing whether a motor vehicle reporting obligation had been impliedly abrogated, the Full Court of the South Australian Supreme found that it had been for reasons that included: the questions that were capable of being asked of the suspect were strictly limited;[99] the purpose of the provisions was to enable the police to investigate and prosecute offences, a purpose that would be 'severely' limited if the privilege was applicable;[100] and it would be impractical to expect a police officer to adjudicate on whether a claim of privilege was reasonable.[101]

While the privilege affords protection against both direct-use and derivative-use evidence,[102] where the privilege has been abrogated there is ordinarily no requirement

---

93 *Haddara v R* (2014) 43 VR 53, 56-57 [4]-[9], 77 [70].

94 Ibid 57 [12], 70-71 [51].

95 *Sorby* (1983) 152 CLR 281, 289 (Gibbs CJ).

96 Ibid 289 (Gibbs CJ).

97 *Police Service Board v Morris* 156 CLR 397, 409. See also *Sorby* (1983) 152 CLR 281, 289 (Gibbs CJ), 309 (Mason, Wilson, Dawson JJ); *Pyneboard Pty Ltd v Trade Practices Commission* 152 CLR 328, 341 (Mason ACJ, Wilson and Dawson JJ).

98 *Mortimer v Brown* [1970] 122 CLR 493.

99 *R v Hooper* (1995) 64 SASR 480, 486.

100 Ibid 486.

101 Ibid 486.

102 *Reid v Howard* 184 CLR 1, 6 (Deane J); *Sorby* (1983) 152 CLR 281, 310 (Mason, Wilson, Dawson JJ).

for immunity to be provided.[103] For example, in both *Loges v Martin* and *R v Hooper* a statutory obligation to provide details of the driver of a motor vehicle was held to abrogate the privilege without a concomitant grant of immunity.[104] If immunity is granted, however, as it frequently is, there is no requirement that derivative-use immunity be given; courts have frequently upheld legislation that abrogated the privilege and provided only a direct-use immunity in exchange.[105] Importantly, where abrogation of the privilege has occurred, none of the exclusionary discretions identified in Part 2.5.1 above will apply as that evidence will not have been unlawfully or unfairly obtained; its probative value will outweigh the risk of prejudice; and there will be no trial unfairness.

Notwithstanding the above principles, in Victoria – and potentially in the Australian Capital Territory and Queensland – both direct and derivative-use immunity may be required when the privilege is abrogated. So much was made clear in the *Major Crime* decision, in which Warren CJ held that the *Major Crime (Investigative Powers) Act 2004* (Vic), which abrogated the privilege but provided only direct-use immunity in respect of any testimony given, needed to be read to include a derivative-use immunity in respect of evidence that could not have been found but for the testimony compelled under the Act.[106] This conclusion was based on the effect of s 25(2)(k) of the *Victorian Charter*, which stated that a person charged with a criminal offence could not be compelled to testify against him- or herself. As the Australian Capital Territory and Queensland have human rights statutes which provide equivalent protection, it is presumed that the same principles apply in respect of legislation in those jurisdictions. Importantly, however, and as discussed in Chapter 1, the rights protected under the *Victorian Charter* are

---

103 See, eg, *A v Boulton* (2004) 204 ALR 598. See also the *Taxation Administration Act 1953* (Cth) sch 1, s 353-10.

104 See Part 1.2.4.

105 See, eg, *Sorby* (1983) 152 CLR 281, 316 (Brennan J); *Hamilton v Oades* (1989) 166 CLR 486 (in respect of the *Companies (New South Wales) Code*)); *R v Independent Broad-Based Anti-Corruption Commissioner* (2016) 256 CLR 459 (the *Independent Broad-Based Anti-Corruption Commission Act 2011* (Vic)); *X v Callanan and Anor* [2016] QCA 335 (the *Crime and Misconduct Act 2001* (Qld)); *A v Boulton* (2004) 204 ALR 598; *A v Boulton* (2004) 207 ALR 342 (the *Australian Crime Commission Act 2002* (Cth)). See also the Australian Law Reform Commission, *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws*, Report No 129, 324 where a list of Commonwealth legislation abrogating the privilege is discussed.

106 *Major Crime* (2009) 24 VR 415, 451 [158].

always subject to limitation, and any infringement of the privilege does not render a statutory power invalid. As will be discussed further in Part 4.4.1.2, the legislature can override or disregard the court's opinion.

2.6 CONCLUSION

As noted in the introduction to this Chapter, the source of the privilege in the four jurisdictions plays a central role in determining not only the ability of each jurisdiction to abrogate the privilege, but also the scope of their exclusionary rules. In Canada and the United States, the constitutional moorings of the privilege mean that its abrogation cannot take place unless direct and derivative-use immunity is granted in exchange for that act of abrogation. The effect of granting that immunity, however, would be to render impotent the use of a compelled production order to prosecute the recipient of the order. The exclusionary rules in those two jurisdictions are equally uncompromising. In Canada, though the *Grant* test appears to provide greater flexibility than the rule in the United States, *R v Shin* demonstrates that in practice exclusion of the evidence will follow where access to encrypted data is obtained through the breach of a *Canadian Charter* right.

The position is markedly different in England and Wales and Australia. In each of those jurisdictions, it is possible to abrogate the privilege without a grant of immunity. The difference between those two jurisdictions arises when evidence obtained as a result of such abrogation is sought to be admitted. In England and Wales, the Supreme Court in *Beghal* held that where the privilege is abrogated by statute with no grant of immunity, evidence obtained as a result of that abrogation will be excluded under s 78 of *PACE* if its admission would affect trial fairness. Critically, the legislation at issue in *Beghal* entails the destruction of the essence of the privilege as it requires the suspect to respond to extensive questioning. It is inevitable that this will affect trial fairness. The scope of the infringement of the privilege in *Beghal* was, therefore, significantly larger than that imposed by a compelled production order, and the evidence obtained from the questioning in *Beghal* could itself be incriminating. By contrast, a password is not itself incriminating and it is only the derivative evidence that may flow from knowledge of that password which might incriminate. As will be discussed in greater detail in

Chapter 4, incriminating evidence found using compelled production orders appears not to infringe the essence of the privilege, with the result that exclusion under s 78 of *PACE* need not follow.

In contrast to England and Wales, in Australia the exclusionary rules have a narrower scope than s 78 of *PACE*, and where abrogation has occurred by statute those exclusionary rules will not operate to exclude evidence found as a result of that act of abrogation. In the context of derivative evidence obtained through the abrogation of the privilege without a grant of derivative-use immunity, it has been noted by the Supreme Court of Victoria that 'there do not appear to be any reported cases where derivative evidence has been excluded for such reasons'.[107] Thus, though in practice the English and Australian positions are as one on the admission of evidence obtained as a result of a compelled production order, nevertheless s 78 of *PACE* appears to have a broader theoretical scope than do the Australian exclusionary rules.

In one respect, however, the exclusionary rules in all four of the jurisdictions may operate in tandem. In *R v Ford*, a decision of the Supreme Court of Queensland that is discussed in greater detail in Chapter 4, Ford was stopped and searched during the early hours of the morning by police officers performing foot patrols. During the search, which revealed an iPhone and $390 in Ford's possession, one of the police officers recognised Ford as a person who the officer had previously arrested for possession of 31 MDMA tablets. The officers further observed that Ford appeared nervous, as a result of which they informed him that he was to be subject to a partial strip search. Ford responded by removing a bag with pills from his pants. In response, the police started questioning Ford, during which they asked for the password to his phone, which he provided. Ford had not been informed of his rights prior to this request.[108] At trial, Ford successfully sought to have evidence of the contents of the iPhone excluded. In finding that exclusion was appropriate, the Court noted that without the password the contents of the phone could not have been viewed;[109] the police officers had failed to use the

107 Ibid 432-3 [68]-[74].
108 *R v Ford* [2017] QSC 205 [6]-[10].
109 Ibid [19].

compelled production order provisions provided in the relevant statute;[110] and the evidence had been obtained in breach of Ford's rights.[111]

In each of the jurisdictions, therefore, seeking to obtain the encrypted data in a manner that infringes the privilege (or another of the suspect's rights) will – or, in the case of Australia, is likely to[112] – result in the exclusion of the relevant evidence. This position is most stark in Canada and the United States, where the legislature cannot avoid the consequences of that exclusionary rule by abrogating the privilege – as can be done in Australian and England and Wales. The consequence of this is that the scope of the privilege in Canada and the United States is determinative, with a finding that a compelled production order infringes the privilege decisive in prohibiting the admission of that evidence by any means. By contrast, even if the scope of the privilege in Australia and England and Wales is broad enough to encompass compelled production orders, the ability of those jurisdictions to abrogate the privilege without grants of immunity provides an avenue for them to obtain that encrypted data. This pattern is fully evidenced in the discussions of compelled production cases in the following two Chapters.

110 Ibid [25].

111 Ibid [50].

112 The Australian position is arguably also supported by the decision in *Luppino (No 1)* [2018] FCA 2106. Although that case did not concern the exclusion of evidence, its finding that a password cannot be compelled unless the privilege has been abrogated suggests that where such compulsion has taken place in the absence of an act of abrogation, the fruits of that search are likely to be excluded.

CHAPTER 3

COMPELLED PRODUCTION ORDERS IN THE UNITED STATES AND CANADA

3.1 INTRODUCTION

Chapter 1 considered the scope of the privilege in the four jurisdictions. While each jurisdiction weighs competing interests to determine the outer edges of the privilege's reach, the results of that exercise differ between jurisdictions. Most notably, Canada was found to give a broader scope to the privilege, with its Supreme Court holding that the privilege may apply to any self-incriminating evidence that a suspect is compelled to create or discover. Under those principles, motor vehicle reporting obligations and some bodily samples fell within the scope of the privilege. In comparison, each of Australia, England and Wales and the United States accorded the privilege a narrower field of operation. In those jurisdictions, the privilege was found to be inapplicable to bodily evidence as the production of that evidence did not constitute testimony. The English position, it should be reiterated, stands at odds with the decision of the European Court of Human Rights in *Jalloh*, a decision that English courts have not followed. With regard to motor vehicle reporting obligations, the three jurisdictions held that the privilege did not preclude the granting of such orders. Importantly, though, how the three jurisdictions resolved the issue of motor vehicle reporting obligations differed. In the United States, the privilege did not encompass those orders; in England and Wales, such an order engaged the privilege but its abrogation did not destroy its essence, with the result that the order could be made; and in Australia, though such orders fell under the umbrella of the privilege, the privilege had been abrogated to allow the order to be made. The issue of abrogation and a jurisdiction's exclusionary rules therefore proved to be as important as the actual boundaries of the privilege.

How the jurisdictions dealt with abrogation and their exclusionary rules – an issue considered in Chapter 2 – was found to be a product of the privilege's standing in each jurisdiction. In the United States and Canada, the privilege receives constitutional protection. Any abrogation thus requires a commensurate grant of direct and

derivative-use immunity, rendering such immunity a substantial bar to the prosecution of the suspect who provides a password. In those two jurisdictions, then, the scope of the privilege was determinative. By contrast, in England and Wales the privilege receives statutory recognition through the *Human Rights Act 1998* while in Australia it is protected by the common law and human rights statutes in some of the states and territories, including Victoria and Queensland. In both England and Wales and Australia, abrogation can occur without a grant of immunity, although should such abrogation occur in England and Wales, evidence obtained as a result of that abrogation may be inadmissible under s 78 of *PACE*. The different moorings of the privilege have therefore resulted in the jurisdictions adopting a different focus. In the United States, for example, should a court wish to avoid the strictures of the privilege it can only do so by finding the privilege inapplicable; in Australia and England and Wales, however, a court can find the privilege engaged but abrogated. This affords Australia and England and Wales greater latitude in determining the role of the privilege to a specific order.

This Chapter will consider how Canada and the United States have dealt with applications for compelled production orders, paying attention to whether the decisions reached by the courts of those jurisdictions, and the reasons for those decisions, are consistent with the principles that were identified in Chapters 1 and 2. Fidelity to the principles identified in those Chapters is important as it may impact the ability of that jurisdiction to provide a model for Australia on how to deal with compelled production orders. As this Chapter will show, while the principles regarding the scope of the privilege that were discussed in Chapter 1 arise from decisions of the Supreme Courts of the United States and Canada, to date decisions on compelled production orders in those jurisdictions predominantly occur at the lower court levels, with relatively few appellate decisions. Neither Supreme Court has considered the issue of compelled production orders. If, therefore, decisions on compelled production orders do not conform with established principles, that increases the likelihood that those decisions and the reasons for them will not survive a challenge to the highest court. That outcome reduces their present value for purposes of comparative analysis.

While Canada and the United States stand apart from Australia and England and Wales due to the constitutional protections given to the privilege in those jurisdictions, it is not solely for that reason that they are discussed together in this Chapter. Rather, it is partly because while Australia and England and Wales have enacted specific statutes to authorise compelled production orders, in Canada and the United States such orders are required to fit within the existing powers granted to law enforcement. This Chapter examines whether the existing statutory powers are sufficient to authorise a compelled production order; it also assesses the factors that the courts of Canada and the United States have relied upon to resolve these applications, and the weight that they have been given. The considerations relied upon by those courts may be relevant to Australian courts, and substantial similarities in approach would provide an endorsement of sorts to the approach adopted in Australia. Conversely, the existence of any differences may provide an alternative model that Australia could draw from.

This Chapter starts by examining the Canadian approach to compelled production orders in Part 3.2. Of the jurisdictions that are examined, it is the one that is least able to provide guidance to Australian courts. This is predominantly a result of its approach to the privilege, which, as discussed in Chapter 1, is out of step with the other jurisdictions.

Part 3.3, which constitutes the greater part of this Chapter, is devoted to the United States' case law. Of particular importance in the United States is the application of the foregone conclusion doctrine. As the discussion in this Part will reveal, there exists a dispute in the case law over the application of that doctrine to the question of what knowledge an applicant must have about the contents of the encrypted device. That dispute will be analysed, and comment made on which of the competing tests more accurately applies existing doctrine. Part 3.3 also considers additional issues that have arisen in the cases in the United States. They include whether the form of the order affects the applicability of the privilege and the authentication requirements under the foregone conclusion doctrine.

Lastly, recent technological developments have meant that increasing numbers of smartphone users lock and unlock their devices using biometric features – typically a

fingerprint but increasingly one's iris or face too. This Chapter will analyse the case law from both jurisdictions on compelled decryption where a biometric password of this nature is used.

3.2 COMPELLED PRODUCTION ORDERS IN CANADA

In this Part of the Chapter, consideration is given to how Canadian courts have responded to applications for compelled production orders. As Chapter 1 showed, Canadian courts have been more robust than others in defending the borders of the privilege, most notably in the context of motor vehicle reporting obligations and certain bodily samples. That approach has been replicated in the response by Canadian courts to compelled production orders, with the result that Canada is the only jurisdiction to find that a password or fingerprint can never be compelled. Regrettably, however, this position appears to have been reached with limited discussion of the reasons for it.

The leading Canadian decision on the use of compulsion to require a suspect to reveal a password was handed down by the Court of Appeal of Quebec in *R v Boudreau-Fontaine*.[1] The police received a phone call from a resident expressing concern that a person in a car parked on a neighbourhood street might be connecting to wireless networks in the area in order to steal personal information. Two police officers drove to the neighbourhood and approached the respondent in his car. As they were doing so, they noticed him close his laptop. One of the officers believed he saw the laptop open on the MSN website's chat page before being closed. The respondent was sweating and nervous. After asking the respondent a few questions, the officers checked his details with police headquarters. The check revealed that the respondent had a conviction for making and distributing child pornography and that one of the requirements of his parole was that he could not access the internet.[2] At this point the respondent was arrested and his computer seized. The police obtained a search warrant for the computer requiring the respondent to reveal any relevant passwords. The respondent complied with the warrant. An analysis of the computer, which the

1 2010 QCCA 1108 ('*Boudreau-Fontaine*').
2 Ibid [7]–[12].

respondent admitted he was the sole user of, revealed that on the night in question immediately prior to his arrest he had been on the MSN website.[3]

At trial the respondent successfully had the evidence of his computer use excluded on the ground that by being compelled to provide the password he had been 'conscripted' into giving evidence against himself.[4] The exclusion of that evidence was taken on appeal by the Crown. On appeal, the Court rejected the notion that the respondent could be compelled to incriminate himself in the manner that had occurred.[5] The Court noted that the computer evidence was essential to the government's case and that the order to provide the password 'was commanding the appellant to give essential information with the specific intent of having him incriminate himself'.[6] The law, the Court further noted, 'will not allow an order to be joined compelling the respondent to self-incriminate'.[7]

The content of the search warrant was also criticised by the Court. The warrant purported to authorise the computer search on the basis of ss 487(2.1) and (2.2) of the *Criminal Code*.[8] Those provisions relevantly provided that:

> (2.1) A person authorised under this section to search a computer system in a building or place for data may (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system'…
> (2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search (a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorised by this section to search for.

The Court held that neither of those provisions gave a justice of the peace the power to 'order a suspect to self-incriminate this way'.[9]

---

3 Ibid [18]–[20].
4 Ibid [24].
5 Ibid [39].
6 Ibid [39].
7 Ibid [39].
8 RSC 1985, C-46.
9 *Boudreau-Fontaine* 2010 QCCA 1108, [46].

Having found the search and seizure unlawful, the Court considered whether the evidence needed to be excluded.[10] While acknowledging that the computer evidence was 'physical evidence that existed without the breach of the respondent's rights', the Court noted that it was also derivative evidence that was obtained by breaching the respondent's rights.[11] The breach was a serious one for which there were no mitigating circumstances,[12] one which had a substantial impact on the accused's rights.[13] In favour of the admission of the evidence, however, was the fact that its exclusion would undermine the correct adjudication of the matter.[14] On balance, however, the Court held that despite the 'very high reliability' of the evidence, it was required to be excluded.[15]

Two separate findings are thus presented by *Boudreau-Fontaine*. The first is that evidence obtained through an unlawful compelled production order in breach of the privilege is to be excluded from trial. The second is that the provisions relied upon by the Crown in support of the compelled production order did not authorise such a measure. This raises the question of whether a statutory provision which specifically authorises the making of such orders would still cause a breach of the privilege requiring the exclusion of that evidence. This issue was addressed in *R v Talbot*,[16] a decision of a single judge of the Ontario Court of Justice.

Talbot's smartphone was seized pursuant to a search warrant. As it was protected by a passcode, the Crown sought an order compelling Talbot to assist the police by providing the passcode. In two respects this case differs from *Boudreau-Fontaine*. First, the assistance order was sought under s 487.02 of the *Criminal Code*, a different provision to that relied upon in *Boudreau-Fontaine*. Section 487.02 provides that a warrant 'may

---

10 The Court noted that the trial judge made his decision prior to the Supreme Court handing down its decision in *Grant* [2009] 2 SCR 353, though it further noted that the result would have been the same under the *Grant* test: *Boudreau-Fontaine* 2010 QCCA 1108, [56], [72].

11 *Boudreau-Fontaine* 2010 QCCA 1108, [57].

12 Ibid [59]-[60].

13 Ibid [67]. It was relevant, too, that the evidence was essential to the prosecutor's case and could not be obtained through other means: [42]-[44].

14 Ibid [68].

15 Ibid [71].

16 2017 ONCJ 814 ('*Talbot*').

order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorisation or warrant'.[17] Notably, the Court in *Talbot* found that the provision in question applied to the accused, with the result that there existed a power under which a compelled production order could be made.[18]

That finding led to the second feature of this decision: its determination of whether a compelled production order infringed the privilege. In *Boudreau-Fontaine*, the compelled production order had been granted at first instance and complied with before being challenged at trial and on appeal. Thus, the question on appeal primarily concerned s 24(2) of the *Canadian Charter* and the admission of that evidence. By contrast, *Talbot* was concerned with whether the granting of such an order infringed the privilege. Unsurprisingly, the Court held that it did. Compelling Talbot in this manner would infringe the privilege, which was a 'principle of fundamental justice' under s 7 of the *Canadian Charter*.[19] Though the Court acknowledged that the state's interests 'must be balanced against protecting an individual's right to self-incrimination', on the facts that balance favoured a finding that the privilege was infringed.[20] This was so despite Talbot being offered direct-use immunity with regard to the passcode and his knowledge of it.[21]

While the statutory provision relied upon in *Talbot* is not as explicit as the statutory powers granted in England and Wales and Australia to compel the production of a password, its wording is broadly similar to the provision that has been successfully relied upon in the United States. Prima facie, the Canadian provision appears to cover compelled production orders, though it is perhaps significant that the Australian and English statutes expressly provide that the assistance that can be compelled includes assistance to obtain access to encrypted material. For this reason, some caution must be adopted when relying upon this part of the *Talbot* finding. Even allowing for such

17 RSC 1985, C-46.
18 *Talbot* 2017 ONCJ 814, [15]-[16].
19 Ibid [38].
20 Ibid.
21 Ibid.

caution, however, it is likely that the privilege would be effective even in the face of an expressly worded statute. This, in large part, is because of how the English and Australian statutes operate. As will be discussed in Chapter 4, both of those jurisdictions rely on the abrogation of the privilege without a grant of immunity for their respective statutes to operate effectively. Abrogation on those terms is not permissible in Canada, however. As the *Talbot* decision shows, a grant of direct-use immunity is insufficient to satisfy the requirements of the privilege, and while a grant of direct and derivative-use immunity would enable the privilege to be abrogated, it would also undermine the purpose of the order.

As noted in the introduction to this Chapter, access to encrypted material is no longer protected by numeric or alphabetic passwords alone. Increasingly, biometrics can unlock encrypted devices such as smart phones. What have Canadian courts had to say about the compelled use of biometrics? In *Re Impression Warrant Application (s. 487.092)*,[22] the Crown sought to compel the suspect to use his fingerprint to unlock his phone. It relied on s 487.092(1) of the *Criminal Code* for authority to do so. That section provides that:

> A justice may issue a warrant in writing authorizing a peace officer to do anything, or cause anything to be done under the direction of the peace officer, described in the warrant in order to obtain any handprint, fingerprint, footprint, foot impression, teeth impression or other print or impression of the body or any part of the body in respect of a person if the justice is satisfied:
> (a) by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been committed and that information concerning the offence will be obtained by the print or impression; and
> (b) that it is in the best interests of the administration of justice to issue the warrant.[23]

Conacher JP, adopting what his Honour described as a contextual approach, held that the section authorised 'tangible items that have physical properties' to be searched, seized and reported on.[24] It did not, however, authorise the taking of a fingerprint to continue a search.[25] On that basis the application was denied.[26] Furthermore, in a brief

---

22 2016 ONCJ 197, 129 WCB (2d) 485 ('*Impression Warrant*').
23 *Criminal Code* RSC 1985, C-46
24 *Impression Warrant* 2016 ONCJ 197, 129 WCB (2d) 485, [11].
25 Ibid [12].
26 Ibid [14].

obiter Conacher JP noted the 'residual concern' that providing the fingerprint would require the suspect to assist the police in their investigation in a manner that appeared to infringe the privilege. His Honour further noted, however, that he did not need to decide that issue.[27]

For present purposes this decision provides two findings. First, s 487.092(1) of the *Criminal Code* does not grant law enforcement a power to compel a suspect to assist in decrypting his or her own encrypted device. Secondly, under Canadian law the privilege appears to encompass acts of decryption using a biometric feature. Such an outcome is consistent with the principles identified in Chapter 1, for the use of a biometric feature does not alter the fact that the suspect is being compelled to engage in an act that will result in the police gaining access to material that incriminates the suspect. Nevertheless, it is also an outcome that separates Canada from the other jurisdictions, where the use of a biometric feature has been found not to infringe the privilege. In those other jurisdictions, the courts have been tolerably clear in reiterating that the privilege does not apply to bodily features, even where they are used to grant access to incriminating material.

This thesis has only identified one decision that appears to buck the orthodoxy, though it is distinguishable as it involved a search at the border. In *R v Buss*,[28] Buss sought to enter Canada from the United States. At the primary inspection he appeared nervous, as a result of which he was sent for a secondary inspection. At the secondary inspection he was asked for and provided the password to his phone and laptop. Upon searching those devices, child pornography was found on the laptop. While the Court's discussion of the state's search powers at the border – which constituted the overwhelming majority of the judgment – is not relevant for present purposes, the Court did, in rejecting the challenge to the lawfulness of the search, hold that 'I do not find that, in this context, the requirement to provide a password offends the right to be free from self-incrimination'.[29] For two reasons, however, little weight can be placed on this

27 Ibid [15].
28 *R v Buss* 2014 BCPC 16.
29 Ibid [33].

decision. First, border searches attract a lower level of scrutiny than do searches elsewhere as 'there is a reduced expectation of privacy at the border'.[30] That alone makes them unsuitable for comparison with a search that is not performed at the border. Secondly, it is likely that this decision was wrongly decided. Notwithstanding the lower threshold at the border, 'the border is not a Charter-free zone'.[31] As every other case on compelled production orders has rejected the availability of such an order, it is unlikely that the lower threshold could justify a different result.

As noted several times in the preceding paragraphs, two separate issues have arisen when Canadian courts have considered compelled production orders. The first is the necessary statutory authority to order a compelled production order. While *Boudreau-Fontaine* and *Re Impression Warrant* rejected the use of the provisions relied upon in those matters, in *Talbot* the Court held that a broad power to require a person to assist in the execution of a warrant did provide the necessary authorisation. That finding, however, only leads to the second issue, which is whether the scope of the privilege precludes the making of that order (regardless of whether there is a statutory power that encompasses compelled production orders). With the exception of *R v Buss*, each of the decisions here considered have found the privilege to bar the granting of a compelled production order, and there is little challenge to that position by other court decisions. Indeed, the opposite is true: in several matters in which potentially incriminating evidence was believed to be located on an encrypted drive, the state made no apparent effort to compel production of the password, presumably on the understanding that such compulsion is impermissible under Canadian law.[32] Until such time as this question is taken to the Supreme Court, the Canadian position with regard to the privilege is relatively settled.

3.3 THE UNITED STATES

30 Ibid [19].

31 Ibid [35].

32 See, eg, *R v M(C)* 2012 MBQB 141, 101 WCB (2d) 168; *R v Seguin* 2015 ONSC 1908, 120 WCB (2d) 234; *R v Burke* 2015 SKPC 173, 126 WCB (2d) 584.

The Canadian position revealed two lessons: first, that consistently with previous applications of the privilege in that jurisdiction, compelled production orders infringe the privilege and are therefore unlawful; and, secondly, doubts exist over whether there is a statutory basis on which a compelled production order can be sought. Both issues arise in the United States, too, though the latter issue appears to have been conclusively resolved. Under the *All Writs Act*,[33] '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'. That power, long established in United States' law, has proven to be the primary basis by which compelled production orders have been authorised.[34] It is a power that has also survived direct challenge. In *United States v Apple Mac Pro Computer*,[35] the appellant challenged the ability of the *All Writs Act* to authorise the granting of a compelled production order. The Court of Appeals for the Third Circuit rejected that challenge, finding that the *All Writs Act* applied to anyone who was able to frustrate the administration of justice or the execution of a court order, a category into which the appellant fell.[36]

The scope of the privilege is a more challenging issue, and one on which the case law is, at times, strikingly divided. As noted in Chapter 1, the act of production and foregone conclusion doctrines lie at the heart of the compelled production cases. Part 3.3.2 analyses how the foregone conclusion doctrine has been applied in compelled production order cases. There are three issues that arise from its use: what evidence must the applicant have regarding the suspect's knowledge of the password; what evidence must the applicant have about the contents of the encrypted drive; and is the production of a password a self-authenticating act?

---

33 *All Writs Act 1789* 28 USC § 1651.

34 See, eg, *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013); *United States v Apple Mac Pro Computer* 851 F 3d 238 (3rd Cir, 2017). Note, however, that some applications have relied upon grand jury subpoena powers: see, eg, *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335 (11th Cir, 2012) (which relied upon the powers in 18 USC § 6003).

35 851 F 3d 238 (3rd Cir, 2017) ('*Apple Mac Pro*').

36 Ibid 246.

Knowledge of the contents of the encrypted drive is a contentious issue, one that has given rise to two competing interpretations of the foregone conclusion doctrine. This thesis will describe those competing approaches as the control test and the contents test. Under the control test, all that the applicant is required to show to satisfy the doctrine is evidence that the suspect has possession or control of the electronic device and that he or she knows what the password is. To those requirements the alternative contents test adds a further requirement: that the applicant provide evidence that it knows with reasonable particularity what is contained on the encrypted drive.[37] What the reasonable particularity test demands is that '[a]lthough the State need not have "perfect knowledge" of the requested evidence, it "must know, and not merely infer," that the evidence exists, is under the control of the defendant, and is authentic'.[38] Judicial support and justification for each of those tests is discussed in Part 3.3.2. The subsequent Part 3.3.3 argues that the control test is the preferable of the two tests, for reasons that include that it more faithfully applies the foregone conclusion doctrine as it has been described by the Supreme Court. If that argument is correct, it suggests that the control test is more likely to be adopted by the Supreme Court should it address the matter.

---

37 The reasonable particularity standard has been adopted by most courts hearing compelled production orders: *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1344 (11th Cir, 2012); *Re Grand Jury Subpoena to Sebastian Boucher* (D Vt, No 2:06-mj-91, 19 February 2009), 3; *United States v Pearson* (ND NY, No 1:04-CR-340, 24 May 2006); *Commonwealth v Gelfgatt* 11 NE 3d 605, 621 (Mass, 2014) (Lenk J, dissent); *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013) slip op 8; *Apple Mac Pro* 851 F 3d 238, 247 (3rd Cir, 2017); *State v Stahl* 206 So 3d 124, 135 (Fla Ct App, 2016); *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015); *Seo v State* 109 NE 3d 418, 436 (Ind Ct App, 2018); *Commonwealth v Jones* 34 Mass L Rptr 287 (Mass Super Ct, 2017); *GAQL v Florida* 257 So 3d 1058 (Fla App 4 Dist, 2018). Note, however, that the standard is not universally adopted, nor has it been accepted by the Supreme Court: Vivek Mohan and John Villasenor, 'Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era' (2012) 15 *University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny* 11, 20 where the authors note that the Supreme Court was 'specifically presented with the "reasonable particularity" standard in *Hubbell* and chose not to accept it'. See also Orin Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination' (2019) 97 *Texas Law Review* 767, 775 where the author discusses the application of the reasonable particularity standard.

38 *State v Stahl* 206 So 3d 124 (Fla Ct App, 2016), 135 citing *United States v Greenfield* 831 F 3d 106 (2nd Cir, 2016). In *In re Grand Jury Subpoena Duces Tecum*, the Court spoke of the need for the government to be able to demonstrate that the files were present on the encrypted drive: *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1348-49 (11th Cir, 2012).

Before considering the application of the foregone conclusion doctrine, however, Part 3.3.1 will consider a preliminary question: does the form of the order play a role in determining whether the privilege applies to that order?

3.3.1 The form of the compelled production order

The United States' cases show that compelled production orders initially took one of three forms: they required the suspect to enter the password into the encrypted device; they required the suspect to provide the unencrypted contents of the encrypted drive; or they required the suspect to give the password to law enforcement officials. Is the privilege infringed by each of these orders, and if so how?

The most common form of order is to require the suspect to enter the password into the encrypted device.[39] When faced with this form of order, courts have held that any testimony that may arise does so through the operation of the act of production doctrine. This is because although the contents of the laptop are not testimonial as they have been voluntarily created, the act of producing the password (by entering it into the computer) will reveal that the suspect knows the encryption key and has control over the files on the computer.[40] The act of producing a password is, it is said, not merely a physical act, but one that 'probes into the contents of an individual's mind'.[41] Therefore, entering the encryption key into the encrypted drive is a testimonial act that engages the act of production doctrine.[42] This is significant, as the foregone conclusion doctrine provides an exception to the act of production doctrine that can exclude the operation of the privilege. The result is that where a compelled production order seeks production through compelled decryption of the unencrypted documents, the applicability of the privilege depends on whether the foregone conclusion doctrine is enlivened on the particular facts of the case.

---

39 Orin Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 *Georgetown Law Journal* 989, 1002. Note, however, that in some cases it is not entirely clear whether the password or the act of decryption is sought: see, eg, *State v Stahl* 206 So 3d 124 (Fla Ct App, 2016), 133–34.

40 *Re Grand Jury Subpoena to Sebastian Boucher* (D Vt, No 2:06-mj-91, 29 November 2007).

41 *GAQL v Florida* 257 So 3d 1058, 1061 (Fla App 4 Dist, 2018). See also *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335 (11th Cir, 2012); *Apple Mac Pro* 851 F 3d 238, 247-8 (3rd Cir, 2017).

42 See also *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015); *Apple Mac Pro* 851 F 3d 238 (3rd Cir, 2017); *Commonwealth v Gelfgatt* 11 NE 3d 605 (Mass, 2014).

The same outcome arises under the second form of order, where what is sought is production of the unencrypted documents. In *In re Grand Jury Subpoena Duces Tecum*,[43] the government sought production of the unencrypted documents. The court held on the facts that the act of decrypting and producing the hard drives would 'be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files'.[44] The act of production was therefore enlivened.[45]

The third form of order requires the suspect to give the password to the law enforcement officials. This form of order is likely to constitute a testimonial act without the need to rely on the act of production doctrine.[46] In *United States v Kirschner,*[47] the government sought to compel Kirschner to provide the encryption key to his computer to enable it to be searched for evidence of child pornography. Borman J found that providing the encryption key involved compelled testimony that revealed a fact (the password) that might result in incriminating evidence being found on Kirschner's computer.[48] The government, Borman J held, 'is not seeking documents or objects – it is seeking testimony from the defendant', and testimony of that nature was protected by the privilege.[49] In the language of the Supreme Court, it constitutes a 'sworn

---

43 670 F 3d 1335 (11th Cir, 2012).

44 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1346 (11th Cir, 2012).

45 See also *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013).

46 See, eg, Laurent Sacharoff, 'Unlocking the Fifth Amendment: Passwords and Encrypted Devices' (2018) 87 *Fordham Law Review* 203, 223-4.

47 823 F Supp 2d 665 (ED Mich, 2010) ('*Kirschner*').

48 *Kirschner* 823 F Supp 2d 665 (ED Mich, 2010), 669. Borman J further noted that a grant of direct-use immunity was insufficient to cure the breach of the privilege.

49 *Kirschner* 823 F Supp 2d 665 (ED Mich, 2010), 669. See, too, in support of this finding: Orin Kerr, 'A Revised Approach to the Fifth Amendment and Obtaining Passwords' The Washington Post (online), 15 August 2017 <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/> where the author argues that providing a password is testimony though it may not be incriminating testimony; Susan W Brenner, 'Encryption, Smart Phones and the Fifth Amendment' (2012) 33 *Whittier Law Review* 525, 537 who argues that where a password has been memorised, orally providing that key to law enforcement officials is testimony; and Joshua A Engel, 'Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing' (2012) 33 *Whittier Law Review* 543, 555 where he argues that giving a password is a testimonial act not necessarily because the suspect is using

communication of facts which would incriminate' the maker of the statement, thereby making it a testimonial act to which the privilege applies directly.[50] Note, though, that in the earlier decision in *United States v Pearson*,[51] the Court's analysis relied on the act of production doctrine even though what was sought was the password and not the act of decryption.[52] This approach is based on the understanding that as the password itself is not incriminating, giving it to law enforcement is not an act of testimony but rather one of production (that unlocks the incriminating evidence).

If all forms of compelled production orders implicate the privilege, does it make a difference which form is sought? There are some judicial dicta suggesting it does not. In *In re Grand Jury Subpoena Duces Tecum*,[53] the Court rejected the argument that producing the unencrypted contents was distinguishable from providing the encryption key. Drawing on the analogy of a key to a safe, it noted that whether the government seeks the key or combination to a safe, what it is ultimately seeking is the contents of the safe rather than simply the key to it.[54] Furthermore, regardless of what is sought from the suspect (be it the password or unencrypted documents), he or she is required to use the contents of his or her mind to produce that which is sought, the production of which entails the making of 'implied factual statements'.[55] Once produced, that evidence will be used to incriminate him or her, thus infringing the privilege.[56]

---

the contents of his or her mind, but because the government can use that password to access further information which they could not otherwise obtain without the password.

50 *Doe II* 487 US 201, 210 (1988).

51 (ND NY, No 1:04-CR-340, 24 May 2006) ('*Pearson*').

52 See also *Securities Exchange Commission v Huang* (ED Pa, Civ No 15-269, 23 September 2015); Phillip R Reitinger, 'Compelled Production of Plaintext and Keys' [1996] *The University of Chicago Legal Forum* 171, 196 where the author states that producing an encryption key is a 'reified act of production'.

53 670 F 3d 1335 (11th Cir, 2012).

54 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1346 (11th Cir, 2012).

55 Ibid.

56 Ibid. Similar opinions were expressed in *Seo v State* 109 NE 3d 418, 431 (Ind Ct App, 2018) where the Court argued that whether one stated the password or used it to unlock an encrypted device was 'a distinction without a difference'; *GAQL v Florida* 257 So 3d 1058, 1062 (Fla App 4 Dist, 2018); *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015); *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013), slip op 9. Note, however, the argument of Nathan K McGregor, 'The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege' [2010] 12 *Vanderbilt Journal of Entertainment and Technology Law* 581, 606-609 that because producing an unencrypted copy of a file involves producing contraband, it represents a greater diminution of the scope of the privilege than does the production of a password.

While it is correct that the privilege is applicable regardless of the form of the order, the dicta above fail to adequately consider the mechanism through which the privilege is engaged. Where a compelled decryption order is sought, or where the unencrypted documents are demanded, the privilege is engaged through the act of production doctrine. As such, the exception contained in the foregone conclusion doctrine may be enlivened. Where the password is sought, however, the adoption of the *Kirschner* approach precludes reliance on the foregone conclusion doctrine as it does not rely on the act of production doctrine to engage the privilege. In this situation the privilege cannot be avoided.[57] The form of order is, therefore, significant as a request for the password will, if the *Kirschner* approach is adopted, ensure that the application fails. It may be for this reason that most compelled production orders seek delivery of the unencrypted documents or the act of decryption.

The choice between demanding the suspect perform the act of decryption him- or herself or demanding he or she produce the decrypted documents also has consequences if the control test is adopted. Where the act of decryption is compelled, the foregone conclusion doctrine can be satisfied by leading evidence that the suspect knows the password as the only testimony given by the suspect through his or her act of decryption is that he or she knows the password. By contrast, and as Kerr has noted, 'complying with an order to produce all of the files on a device in decrypted form may require knowledge beyond just [the password]'.[58] That additional knowledge may include knowledge of the contents of the encrypted drive.

As most orders seek either the act of decryption or production of the decrypted documents, it is apparent that how the foregone conclusion doctrine is applied on the particular facts of a case is likely to be the critical issue in almost any application for a

---

57 Where a court adopts the *Kirschner* approach, it may find that providing the password infringes the privilege but that the act of entering the password into the encrypted device does not: *United States v Spencer* (ND Cal, Case No. 17-cr-00259-CRB-1, 26 April 2018), slip op 3.

58 Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 784.

compelled production order.[59] A qualification to that statement concerns what might be considered a fourth form of order: decryption using a biometric feature. Is the privilege infringed by decryption using biometrics? The case law in the United States has found, with but a few exceptions, that it is not.

3.3.1.1 Decryption through biometrics: the fourth form of order

In *Commonwealth v Baust*,[60] the government sought an order requiring Baust to unlock his phone either through entering the passcode or using his fingerprint on the fingerprint scanner. Using his fingerprint, the Court held, was a purely physical act that did not require Baust to 'communicate any knowledge at all'.[61] Accordingly, unlocking the phone with a fingerprint did not infringe the privilege.[62] The same conclusion was reached by the Minnesota Court of Appeals in *State v Diamond*.[63] It held that an act is only testimonial if it relates 'a factual assertion or disclosed information'.[64] Producing a fingerprint did not require Diamond to speak his guilt, disclose any knowledge or use his mental capacity. In that way it was distinguishable from the act of providing an encryption key or the combination to a safe.[65] That the use of the fingerprint communicated the fact that Diamond had the use and control of the phone did not alter

---

59 *Kirschner* stands as the sole decision examined in this thesis which did not rely on the act of production doctrine.

60 89 Va Cir 267 (2014) ('*Baust*').

61 Ibid 271. See also *State v Stahl* 206 So 3d 124, 135 (Fla Ct App, 2016) where the Court noted that using a fingerprint to unlock a smartphone would not be protected under the privilege as it was 'an exhibition of a physical characteristic, the forced production of physical evidence'.

62 This finding has academic support. See, eg, Kerr and Schneier, above n 38, 1003 where the authors state that one method of obtaining an encryption key is to order a suspect to use his or her fingerprint (or other biometric data) to unlock the encrypted device as providing a fingerprint is not a testimonial act. But see, *contra*, Erin M. Sales, 'The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to be Free from Self-Incrimination' (2014) 63 *University of Miami Law Review* 193, 224 where the author suggests that because the use of the fingerprint may provide a link in the chain of evidence, the privilege would apply unless the foregone conclusion doctrine was enlivened. The author is wrong in her argument, however, as non-testimonial evidence does not become testimonial merely because it provides a link in the chain of evidence: *Byers* 402 US 424, 433–434 (1971).

63 890 NW 2d 143 (Minn App 2017).

64 Ibid 150 citing *Doe II* 487 US 201, 210 (1988).

65 *State v Diamond* 890 NW 2d 143 (Minn App 2017), 150-151.

that fact that the use of the fingerprint was a non-testimonial act.[66] For these reasons the Court found that the Fifth Amendment had not been infringed.[67]

More recent cases confirm the correctness of those decisions. First, in an appeal against the decision in *State v Diamond*, the Supreme Court of Minnesota upheld the District Court's decision. The Supreme Court held that as using a fingerprint 'elicited only physical evidence from Diamond's body and did not reveal the contents of his mind, no violation of the Fifth Amendment privilege occurred'.[68] The use of the fingerprint was more akin to 'exhibiting the body than producing documents'.[69] Secondly, in *In the Matter of the Search Warrant Application for [redacted text]*, the United States' District Court found that the privilege was not infringed by compelling the provision of a physical characteristic as there was no communicative element in such an action.[70] It was important, the Court held, to keep in mind the difference between an act being testimonial and one being incriminating: a non-testimonial act does not become testimonial merely because it is incriminating.[71] As the act of providing a fingerprint was not testimonial, it did not become so merely because it might incriminate the person.

The two findings that underpin these decisions – that a purely physical act does not infringe the privilege and that a non-testimonial act cannot be rendered testimonial merely because it may lead to incriminating evidence – are founded on well-established Supreme Court precedent. The former principle can be found as far back as the *Holt* decision, when the Supreme Court held that the privilege did not mean that a suspect's

---

66 Ibid 151. See also *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1344 (11th Cir, 2012) where the Court held that an act of production is not testimonial where what is compelled is a physical act, such as producing the physical key to a safe.

67 Fingerprints are not the only biometric feature that have been used to decrypt electronic devices. Orders have been made compelling decryption using Face ID: *In the Matter of the Search of Apple iPhone 8 recovered from the Residence of Grant Michalski, 221 N. Front Street, #105 Columbus, OH, and Currently Held in FBI Secure Evidence Storage, 425 W. Nationwide Blvd, Columbus, OH* (case no. 2:18-MJ-707).

68 *State v Diamond* 905 NW 2d 870, 872 (Minn, 2018).

69 Ibid 875.

70 *In the Matter of the Search Warrant Application for [redacted text]* 279 F Supp 3d 800, 803 (ND Ill, 2017). The Court noted that the fingerprints could be taken when the suspect was sleeping, a time during which a person is unable to communicate.

71 Ibid 805.

body was excluded as a source of evidence;[72] and the latter was endorsed in *Doe II* when it was held that '[i]f a compelled statement is not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence'.[73]

Though there is little judicial dissent to this line of cases, an opposing argument raised in *In re Application for a Search Warrant*[74] requires comment. In that matter Weisman J, when analysing the applicable legal principles, held that although 'the production of physical characteristics generally do not raise Fifth Amendment concerns', those concerns may be raised where the compelled act of production is itself incriminatory.[75] Drawing heavily on the decision of the Court of Appeal of the Eleventh Circuit in *In re Grand Jury Subpoena Duces Tecum*,[76] he stated that the question to be answered was 'whether the government sought testimony implicating the Fifth Amendment by requiring Doe to decrypt certain computer files'.[77] In *In re Grand Jury Subpoena Duces Tecum*, the Court found that an act of production could be testimonial where, through the use of 'the contents of his own mind', the person producing the evidence makes a 'statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic'.[78] To the argument that fingerprints are not testimonial, Weisman J held that by unlocking a phone with one's fingerprints, a person was producing the contents of the phone and 'testifying' that that person had access to, and control over, the phone.[79] This, he held, infringed the privilege.

In the matter before Weisman J there was no use of the contents of the accused's mind; placing one's finger on the home button of a phone is a purely physical act. His answer to this problem – to say that by using his fingerprint he was testifying – is simply wrong.

---

72 *Holt* 218 US 245, 252–3 (1910).

73 *Doe II* 487 US 201, 208-209 (1988).

74 (ND Ill, No 17M081, 16 February 2017).

75 *In re Application for a Search Warrant* (ND Ill, No 17M081, 16 February 2017), 4.

76 670 F 3d 1335 (11th Cir, 2012).

77 *In re Application for a Search Warrant* (ND Ill, No 17M081, 16 February 2017), 4.

78 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012) as quoted in *In re Application for a Search Warrant* (ND Ill, No 17M081, 16 February 2017), 5. Note, though, that under the control test the statement of fact is that the suspect knows how to unlock the phone.

79 *In re Application for a Search Warrant* (ND Ill, No 17M081, 16 February 2017), 6.

It constitutes the regurgitation of an argument that was rejected as far back as the decision in *Schmerber*, when the Supreme Court dismissed the notion that a person was testifying by providing a blood sample for a blood alcohol test.[80] Indeed, the dissenting judges in *Schmerber* raised, and saw rejected, the same argument that Weisman J made, namely that 'the sole purpose of this project which proved to be successful was to obtain "testimony" from some person to prove that petitioner had alcohol in his blood at the time he was arrested'.[81] For Weisman J, the dominant purpose of the fingerprint was to obtain testimony to prove that the phone in question contained incriminating evidence and that the petitioner had control of that evidence. On long-standing Supreme Court principles, a purely physical act that does not require the use of the contents of one's mind nor does it rely on the truth-telling of a person cannot constitute testimony and thus cannot engage the act of production doctrine.[82]

Finally, Weisman J makes the exact error that was identified in *In the Matter of the Search Warrant Application for [redacted text]*. When he held that although 'the production of physical characteristics generally do not raise Fifth Amendment concerns', those concerns may be raised where the compelled act of production is itself incriminatory,[83] he failed to bear in mind the distinction between a testimonial and an incriminating act and the fact that a non-testimonial act does not become testimonial merely because it is incriminating.[84]

---

80 *Schmerber* 384 US 757 (1966). Note, in particular: the Court's comments that 'his participation, except as a donor, was irrelevant to the results of the test' (at 765); its further comments that 'since the blood test evidence, although an incriminating product of compulsion, was neither petitioner's testimony nor evidence relating to some communicative act or writing by the petitioner, it was not inadmissible on privilege grounds' (at 765); and the dissenting opinion of Black J (with whom Douglas J joined) in which Black J unsuccessfully argued that 'the compulsory extraction of petitioner's blood…had both a testimonial and communicative nature' (at 774).

81 Ibid 774 (Black J in dissent).

82 The most likely cause of this error by Weisman J is that *In re Grand Jury Subpoena Duces Tecum* involved the use of the defendant's mind as he was required to reveal a password. He appears to have assumed that because the mental element was satisfied in *In re Grand Jury Subpoena Duces Tecum*, it had been satisfied on the facts before him.

83 *In re Application for a Search Warrant* (ND Ill, No 17M081, 16 February 2017), 4.

84 *In the Matter of the Search Warrant Application for [redacted text]* 279 F Supp 3d 800, 805 (ND Ill, 2017).

The case law on biometrics is thus reasonably settled. The compelled use of a biometric feature to unlock an encrypted device does not infringe the privilege, a finding that is based on earlier Supreme Court decisions in cases that include *Holt*, *Schmerber*, *Wade* and *Gilbert*, as well as *Fisher* and *Hubbell*. It is a finding entirely in accordance with the decisions that were analysed in Chapter 1.

3.3.1.2 The form of order and the safe analogy

Before moving on to consider how the act of production and foregone conclusion doctrines have been applied by the courts when faced with a compelled production order, one last comment on the form of order bears making. In *Doe II*, both the majority opinion of the Supreme Court and the dissenting opinion of Stevens J referred to the example of a safe to distinguish those situations in which a communication expressed the contents of one's mind, and those in which it did not. According to both opinions, the surrender of a key to a safe does not require the suspect to use his or her mind to assist the state in one's own prosecution, with the result that the privilege is not engaged; where, however, a person is required to give the combination to a safe, the privilege is engaged as the act of revealing a safe combination requires the use of the suspect's mind.[85] The Court once more referred to this example in the later *Hubbell* decision.[86] The Supreme Court's discussion of this issue has also been relied upon in at least one decision involving the compelled production of a dial combination lock to a safe. In *United States v Green*, evidence found by compelling the suspect to reveal the combination to a safe was suppressed by the Court following a finding that the compulsion had breached the Fifth Amendment.[87] The Court's finding was reached on the basis of *Doe II*.[88]

The analogy to decryption is immediately clear: where a suspect produces a password or decrypts encrypted material, his or her conduct is akin to revealing the combination to a safe, with the result that the privilege ought to apply; where his or her fingerprint

---

85 *Doe II* 487 US 201, 210 fn 9, 219 (1988).

86 *Hubbell* 530 US 27, 43 (2000).

87 *United States v Green* 272 F 3d 748, 750-51 (5th Cir, 2001).

88 Ibid 753.

is used, however, his or her participation is more closely related to handing over a physical key.[89] Unsurprisingly, several decisions have expressly referenced this distinction.[90] As early as 2007 in *Re Grand Jury Subpoena to Sebastian Boucher*,[91] Niedermeier J referred to the distinction between the surrender of keys and combinations to differentiate non-testimonial and testimonial acts, and to ultimately find that providing a password was a testimonial act.[92] In *Kirschner*, the privilege was found to be infringed by a requirement to decrypt documents, an outcome based in large part on the safe and combination distinction drawn by the Supreme Court.[93] Significantly, too, the Court of Appeal for the Eleventh Circuit in *In re Grand Jury Subpoena Duces Tecum* also placed weight on this analogy in finding that the compelled production of unencrypted documents infringed the privilege whereas a purely physical act not requiring the defendant to make use of the contents of his mind did not.[94] In the more recent *Baust* decision, references to this analogy continued to be made, this time to support a finding that the defendant could not be compelled to produce the passcode to his smartphone but could be compelled to produce his fingerprint to unlock it.[95]

Though too much weight should not be placed on the use of this analogy, two comments are warranted. First, the analogy is consistent with how courts have applied the privilege to compelled production orders: where the password takes the form of a biometric key, the privilege is not engaged; in all other instances, however, compelling

---

89 That the Supreme Court has not once averted to the possibility that the act of production doctrine applies to the production of the physical key confirms that the doctrine is not intended to, and does not, apply when a fingerprint is used to unlock a phone.

90 See, eg, *Seo v State* 109 NE 3d 418, 430 (Ind Ct App, 2018); *United States v Spencer* (ND Cal, Case No. 17-cr-00259-CRB-1, 26 April 2018) slip op 3; *GAQL v Florida* 257 So 3d 1058, 1062 (Fla App 4 Dist, 2018); *In the Matter of the Search Warrant Application for [redacted text]* 279 F Supp 3d 800, 807 (ND Ill, 2017). There is also limited academic support for the analogy. See, eg, Timothy A. Wiseman, 'Encryption, Forced Decryption, and the Constitution' (2015) 11 *I/S: A Journal of Law and Policy for the Information Society* 525, 555. For criticism of the analogy, however, see Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 781.

91 (D Vt, No 2:06-mj-91, 29 November 2007) ('*Boucher I*')

92 *Boucher I* (D Vt, No 2:06-mj-91, 29 November 2007), 4.

93 *Kirschner* 823 F Supp 2d 665, 669 (ED Mich, 2010).

94 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012).

95 *Baust* 89 Va Cir 267, 271 (2014). Lenk J in his dissent in *Commonwealth v Gelfgatt* 11 NE 3d 605, 622 (Mass, 2014) also refers to this analogy.

the production of the password is an infringement of the privilege. Secondly, while awaiting a Supreme Court decision on compelled production orders, this analogy may provide some guidance as to how the Court may resolve the issue of compelled production orders. Notably, however, the safe analogy only provides guidance of the broadest scope. Specifically, it is not disputed that the privilege is engaged in all instances not involving a biometric password, and the answer to that which is disputed – what is required by the foregone conclusion doctrine? – is not given by the safe analogy. To understand that dispute, Part 3.3.2 analyses how courts have applied the doctrine to compelled production orders. Thereafter, in Part 3.3.3, argument is advanced as to which of the competing interpretations should be adopted. For while the foregone conclusion doctrine plays no part in decryption using biometric features, it remains the central issue for the remaining forms of order.

3.3.2 Competing tests for the application of the foregone conclusion doctrine

As the preceding Part identifies, in almost all cases involving compelled production orders the privilege is engaged through the act of production doctrine. That, in turn, raises the question of whether the foregone conclusion doctrine is satisfied on the facts of the matter. It is this question that lies at the heart of the compelled production cases. When the foregone conclusion doctrine is applied to compelled production orders, three key issues arise: what evidence must the applicant have of the suspect's knowledge of the password; what evidence must the applicant have concerning the contents of the encrypted drive; and how is the authentication requirement satisfied?

Of those three issues, the most contentious one concerns knowledge of the contents of the encrypted drive. Despite the apparently unremarkable nature of this issue, it is one on which the case law is deeply divided. Moreover, many of the courts that have decided this issue seem unaware that there exist two competing approaches to the question of what knowledge is required.[96] Under the contents test, the foregone

[96] Writers have recognised these two competing understandings of what is required under the foregone conclusion doctrine. See, eg, Kerr and Schneier, above n 38, 1002-3 though the authors note that at the time of writing the courts have not resolved this question; Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36; Dan Terzian, 'Forced Decryption as a Foregone Conclusion' (2015) 6 *California Law Review Circuit* 27, 27.

conclusion doctrine cannot be satisfied unless the applicant presents evidence showing that it knows with reasonable particularity what is contained on the encrypted device. Under the control test, by contrast, that requirement does not exist. This is because while the contents tests is based on the understanding that what is produced are the contents of the encrypted drive (and thus knowledge of those contents is required), the control test takes the approach that what is produced is the password (and therefore all that is required is to show that the suspect knows the password).

It is important to note, however, that even under the control test the applicant still needs to satisfy an evidentiary burden concerning the contents of the encrypted drive. This is because in order to search and seize the electronic device in question, a warrant must first be issued. For that warrant to be issued, the Fourth Amendment requires an applicant to show probable cause to believe something will be on the electronic device.[97] If a warrant includes the search of an electronic device, any such device that is found during the search may be searched and seized. If, however, the device is protected by encryption, the matter moves on to an assessment of whether the act of production doctrine is enlivened. It is at this stage that the contest test imposes its further evidentiary burden, but the control test does not. This process is amply demonstrated by the compelled production cases. In *In re Grand Jury Subpoena Duces Tecum*, for instance, various electronic devices were seized pursuant to a warrant. Those devices, or parts of devices, which were unencrypted were searched under the powers contained in the warrant.[98] To search the encrypted devices, however, a compelled production order was required. On the facts of *In re Grand Jury Subpoena Duces Tecum*, that order was not issued partly because the applicant failed to satisfy the knowledge requirement concerning the contents of the encrypted devices.[99] Thus, the burden imposed under the control test differs from that imposed under the contents

---

See also Jamil N Jaffer and Daniel J Rosenthal, 'Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge' (2014) *Catholic University Journal of Law and Technology* 273, 300 where the authors argue that the contents test has the effect of narrowing the scope of the foregone conclusion doctrine.

97 Note, however, that the probable cause requirement will ordinarily be satisfied without difficulty: Sacharoff, 'Unlocking the Fifth Amendment', above n 45, 214.

98 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1339 (11th Cir, 2012).

99 See also *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015); *State v Stahl* 206 So 3d 124 (Fla Ct App, 2016); *State v Diamond* 905 NW 2d 870 (Minn, 2018).

test in two ways: first, it is a lesser burden, requiring only probable cause to believe that evidence will be found as opposed to the more exacting standard of knowing with reasonable particularity what is contained on the encrypted drive; and, secondly, it is imposed at the time the subpoena to search and seize the electronic device is issued (rather than at the stage that the compelled production order is sought).

Part 3.3.2.1 below will consider how courts have dealt with the requirement that the applicant provide evidence showing the suspect's knowledge of the password. The dispute concerning knowledge of the contents of the encrypted device is then dealt with in Part 3.3.2.2. Finally, Part 3.3.2.3 addresses the authentication requirement.

3.3.2.1 Knowledge of the password

While this element of the foregone conclusion test is not subject to competing tests in the same manner as the knowledge of the contents is, judicial decisions on the level of evidence required to satisfy it vary considerably. In some cases, regardless of whether the court adopts a more or less demanding understanding of what this element requires, the facts are sufficient to satisfy the requirement. For example, in *Apple Mac Pro*, as part of a child pornography investigation, a search warrant was executed at the appellant's residence during which a computer, two external hard drives and two iPhones were seized. All the devices were encrypted. The appellant provided the password for one of the phones but none of the other devices for the purported reason that he could not remember them. The Court rejected his assertion as the government had established that the suspect possessed and owned the devices;[100] the suspect's sister had given evidence that she had seen the suspect decrypt at least one of the devices in question; and the assertion by the suspect that he did not know the password was made relatively late in the proceedings.[101]

---

100 *Apple Mac Pro* 851 F 3d 238, 248 (3rd Cir, 2017).

101 Ibid 249. See also *People v Johnson* 90 NE 3d 634, 637 (IL, 2017) in which the court rejected the suspect's submission that she had forgotten the password as the phone had been found in her car, it matched a description given of the suspect's phone and witnesses testified that they had seen the suspect unlock the phone; *United States v Fricosu* 841 F Supp 2d 1232, 1235 (2012) where the defendant was heard admitting to a fellow suspect that she was storing the information sought by the FBI on her computer, and that it was protected through encryption.

In other circumstances the facts will be insufficient regardless of the evidentiary burden imposed. In *Commonwealth v Jones*,[102] the Court found the foregone conclusion doctrine had not been satisfied as the phone in question – despite being found in the suspect's possession – was not registered in the suspect's name nor at the suspect's residence; the answering machine on the phone used a female voice (and the suspect was a male); no evidence was led to show that the suspect had ever used the phone; and the suspect denied owning the phone.[103]

In most cases, however, the facts fall between the above cases. Often, law enforcement officials will only be able to establish control, possession or ownership of the device in question. From that evidence the court is required to determine whether knowledge of the password has been established. Unsurprisingly, courts have differed in the conclusions they have reached on whether that constitutes sufficient evidence. At the less demanding end of the spectrum exist decisions that accept that where the electronic device in question belongs to the suspect and is in that person's possession or control, this knowledge requirement will be satisfied.[104] Other cases, however, have taken a more demanding approach.

Arguably the high point of this approach is found in *Boucher I*.[105] Boucher was stopped by a Custom and Border Protection Officer as he entered the United States from Canada. A laptop was found in his motor vehicle, which he admitted was his. The officer opened and searched the laptop (no password being required in order for him to do so) and found child pornography on drive Z. On arresting Boucher and turning off the laptop, drive Z became encrypted so that the investigating officers could no longer view its

---

102 *Commonwealth v Jones* 34 Mass L Rptr 287 (Mass Super Ct, 2017).

103 Ibid slip op 4.

104 See, eg, *State v Andrews* 197 A 3d 200, 205 (NJ Super App Div, 2018) where the Court noted that the password requirement was satisfied as 'the State has established and the defendant has not disputed that he exercised possession, custody or control over these devices'; *United States v Gavegnano* 305 Fed Appx 954, 956 (4th Cir, 2009) where is was sufficient that Gavegnano was 'the sole user and possessor of the computer'; *State v Stahl* 206 So 3d 124, 134 (Fla Ct App, 2016) where it was sufficient to establish that the phone in question belonged to Stahl, who had possession and control of it; *In the Matter of the Search of a Residence in Aptos, California 95003* (ND Cal, Case no. 17-mj-70656-JSC-1, 20 March 2018) where it was sufficient that the phone was found in the suspect's possession.

105 (D Vt, No 2:06-mj-91, 29 November 2007).

contents.[106] Notwithstanding that evidence, Neidermeier J found that it was 'not without question' that Boucher knew the encryption key, and therefore any act of decryption would constitute testimonial evidence.[107]

In *In the Matter of the Decryption of a Seized Data Storage System*,[108] law enforcement officials, acting pursuant to a valid search warrant, searched the suspect's house for child pornography.[109] The suspect, an experienced computer scientist, was the sole occupant of the house and had resided there for the past fifteen years. Sixteen storage devices were seized during the raid, nine of which were encrypted. In response to the suspect's refusal to admit access to and control of the devices in question, the Court held that the government had not established that the suspect had access to and control of the encrypted devices and the files on them.[110] In respect of smartphones, *State v Trant*[111] supports the position that possession and control of the electronic device is not on its own sufficient to demonstrate knowledge of the password.

Finally, *In re Grand Jury Subpoena Duces Tecum* adopted a similarly strict approach. As part of a child pornography investigation, law enforcement officials had identified a YouTube account that was used to share child pornography. They further identified several internet protocol (IP) addresses from which the account was accessed. Three of those IP addresses were from hotels at which Doe stayed on each of the nights in question. He was the only common hotel guest at the relevant times.[112] While he was staying at another hotel, and pursuant to a valid search warrant, officers searched his room and seized his laptop and several external hard drives. The electronic data was encrypted and a forensic review of the encrypted drives was unable to determine whether the drives contained any data. Despite the circumstances in which that

106 Ibid 1–2.

107 Ibid 3. Neidermeier J noted that requiring him to provide the encryption key placed him in the cruel trilemma.

108 (ED Wis, No 13-M-449, 19 April 2013).

109 The judgment does not provide the facts upon which the subpoena was granted.

110 *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013) slip op 8.

111 (Me Super Ct, No 15-2389, 22 October 2015).

112 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1339 (11th Cir, 2012).

electronic equipment was found in Doe's possession, the Court held that the government had not been able to show that Doe knew the password.[113]

What findings have these cases revealed? First, it is arguable that the stricter approach adopted in cases such as *Boucher I* imposes too high a standard. While many users of electronic devices may struggle to remember all the passwords that they hold, certain passwords are not readily forgotten: the password to one's computer or phone is such an example. In *Boucher I*, the laptop was found in the suspect's possession; when it was found it was unencrypted; and Boucher admitted it was his. It is difficult to understand the court's decision on this issue when it has the effect of saying that finding an electronic device in the possession of its owner at the time that it is being used is insufficient to establish that the owner knows the password. Particularly where the device in question is a person's smartphone, finding that device in a person's possession ought to be sufficient to satisfy this element.[114]

Secondly, there may be instances in which further investigations could aid in resolving this issue. For instance, in respect of smartphones, records from the telecommunications service provider could show if the smartphone was used in the immediate period prior to the suspect being searched and his or her smartphone seized. If there is evidence of such use, which would require knowledge of the password, the evidence arguably becomes overwhelming that the suspect knows the password. In other cases, such as *Commonwealth v Jones*, the suspect's argument that the phone is not his could be rebutted if it could be shown that the only, or predominant, fingerprints found on the phone belong to the suspect. Though no cases reveal the use of this sort of evidence, it is readily accessible evidence that could substantially aid the resolution of this issue.

---

113 Ibid 1346.

114 The only way to avoid that finding is to hold that it is possible that people are in the habit of owning expensive electronic devices which they carry around with them while being unable to use them. That finding, this thesis suggests, is not open to being made. See also Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 783 where he argues that evidence of regular use of an electronic device would ordinarily satisfy the requisite knowledge requirement.

Finally, as will be discussed in Chapter 4, both the English and Australian position on the evidential burden regarding the suspect's knowledge of the password conform with the more lenient approach evident in *United States v Gavegnano*,[115] *State v Stahl*[116] and *In the Matter of the Search of a Residence in Aptos, California 95003*.[117] In those two jurisdictions, courts have consistently found that where the electronic device in issue is found in the possession or under the control of the suspect, that is ordinarily sufficient to satisfy the password knowledge requirement.

Notwithstanding the differences in application, there is relatively broad agreement in the United State's case law on the password knowledge requirement. In Part 3.3.2.2 below, however, the evidentiary requirements concerning knowledge of the contents of the encrypted drive are analysed. On that, there is substantially less agreement.

3.3.2.2 Knowledge of the contents of the encrypted drive

As noted in Part 3.3, the courts of the United States have adopted two competing understandings of whether the foregone conclusion doctrine requires the applicant for a compelled production order to know with reasonable particularity what is contained on the encrypted drive. The contents test requires that knowledge; the control test does not. This Part commences by considering those decisions that support the contents test.

The leading case adopting the contents test is *In re Grand Jury Subpoena Duces Tecum*, delivered by the Court of Appeal for the Eleventh Circuit. In considering whether the privilege had been infringed, the Court noted that while the files themselves were not testimonial evidence, the critical question was whether the act of decrypting and producing those drives conveyed a statement of fact – namely, that the documents exist, are in the defendant's control or possession and are authentic – with the result that it constituted a testimonial act.[118] For the foregone conclusion doctrine to be satisfied, the government needed to know that information with reasonable particularity,[119]

115 *United States v Gavegnano* 305 Fed Appx 954 (4th Cir, 2009).
116 206 So 3d 124, 134 (Fla Ct App, 2016).
117 (ND Cal, Case no. 17-mj-70656-JSC-1, 20 March 2018) ('*Aptos Residence*').
118 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1342 (11th Cir, 2012).
119 Ibid 1343.

which required more than a mere suspicion that the documents existed.[120] After reviewing *Fisher*[121] and *Hubbell*,[122] the Court identified two key principles concerning the act of production doctrine. First, the privilege is not engaged through the compulsion of a merely physical act that does not require the defendant to use the contents of his mind.[123] Such an act, which might include providing a bodily sample or responding to a subpoena that does not require the use of the contents of one's mind, does not fall within the scope of the act of production doctrine.[124] Secondly, where the act of production doctrine is enlivened, the act of producing a document the contents of which are a foregone conclusion does not constitute a testimonial act, with the consequence that the privilege is not infringed.[125]

On the facts the Court held that the act of decrypting and producing the hard drives would 'be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files'.[126] As for the foregone conclusion doctrine, the Court held that it had not been enlivened. The government, it found, did not know what, if anything, was contained on the hard drives, and could not demonstrate that Doe could access the drives.[127] The Court contrasted this finding with the appeal decision in *Re Grand Jury Subpoena to Sebastian Boucher*,[128] in which the government knew of the existence of file names indicative of child

120 Ibid 1344.

121 *Fisher* 425 US 391 (1976).

122 *Hubbell* 530 US 27 (2000).

123 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012). The Court noted the 'famous' example of the key to the lock of a safe as an example of such compulsion.

124 See what is said in Part 1.2.1.1 of Chapter 1.

125 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012).

126 Ibid 1346. Most cases that adopt the contents test use similar language. See, eg, *United States v Fricosu* 841 F Supp 2d 1232, 1236 (D Colo, 2012); *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013); *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015).

127 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1346 (11th Cir, 2012). One aspect of this decision is unclear, however. The judgment speaks variously of the subpoena requiring Doe to 'produce the unencrypted drives' (at 1352) or to 'decrypt the hard drives' (at 1338). Where the contents test is applied, either form of order requires law enforcement to know with reasonable particularity what is contained on the encrypted drive. However, as already noted in Part 3.3.1, if the control test is applied knowledge of the contents of the encrypted drive may only be required if production of the unencrypted documents is sought; where decryption is sought, however, no such knowledge is required.

128 (D Vt, No 2:06-mj-91, 19 February 2009) ('*Boucher II*').

pornography.[129] Underlying the contents test, then, is a belief that 'what the State seeks to compel is not merely the password, but the entire contents of [the electronic device]'.[130] In this way proponents of this test appear to ignore what the subject of the order is – being the production of the password – to focus instead on what may ultimately be obtained as a result of the order.

Early decisions applying this test evidenced some inconsistencies and errors. In *Pearson*, the Court held that 'compliance with the subpoena does not tacitly concede the existence or location of the computer files because the files are already in the government's possession. Their existence is a foregone conclusion.'[131] This is an unfortunate statement as possession of the encrypted drive does not mean the contents of that drive are a foregone conclusion – a point noted by later cases. In *Boucher I*, the Court found that there was insufficient evidence regarding the contents of the encrypted drive despite some of the offending files on that drive being viewed by a law enforcement official. The basis for this finding was that to compel decryption would result in the compelled production of files 'both known and unknown' and that 'the files the government has not seen could add much to the sum total of the government's information'.[132]

Subsequent decisions have provided further guidance on what level of evidence is required to satisfy the reasonable particularity test. In *United States v Fricosu*,[133]

---

129 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1349 (11th Cir, 2012). The Court further noted that the government's knowledge of a file name would be an 'easy way' to satisfy its burden under the foregone conclusion doctrine, although it was not necessary to know the specific content of a file.

130 *Seo v State* 109 NE 3d 418, 434 (Ind Ct App, 2018). See also *GAQL v Florida* 257 So 3d 1058, 1063 (Fla App 4 Dist, 2018). The Court in *GAQL* suggested a further reason for adopting the contents test: if knowledge of the contents was not required, the foregone conclusion doctrine would always be satisfied which would 'contravene the protections of the Fifth Amendment': slip op 6-7. The case law shows this argument to be false.

131 *Pearson* (ND NY, No 1:04-CR-340, 24 May 2006) slip op 17.

132 *Boucher I* (D Vt, No 2:06-mj-91, 29 November 2007), 6. On appeal, however, it was held that it was not necessary for the government to know the exact content of the documents it sought access to for the foregone conclusion doctrine to apply; it was sufficient for the government to be able to show 'with reasonable particularity' that it knew of the existence and location of the documents in question: *Boucher II* (D Vt, No 2:06-mj-91, 19 February 2009), 3. On that basis the government had sufficient knowledge of the existence and location of the subpoenaed documents.

133 841 F Supp 2d 1232 (D Colo, 2012).

evidence that the defendant had (in a covertly recorded telephone conversation) admitted storing the information sought on the encrypted drive was sufficient evidence as the court was not required to know the precise content of any specific document.[134] Other courts have found that where files with filenames indicative of child pornography, or hash values that correspond with known child pornography,[135] are found to have been received, distributed or stored on an electronic device, that will satisfy the knowledge requirement.[136]

In *In re Grand Jury Subpoena Duces Tecum*, the government failed to satisfy the reasonable particularity standard in respect of a laptop and a number of external hard drives that were found with the accused in his hotel room despite the accused being known to be the only common guest who had stayed at three separate hotels at the same time that the IP addresses of those hotels had been used to share child pornography through one specific YouTube account.[137] The Court held that the government needed to know with reasonable particularity that the encrypted drives contained the documents sought,[138] which required more than a mere suspicion that the documents existed.[139] On the facts that standard was not met as the government did not know what, if anything, was contained on the hard drives.[140]

---

134 *United States v Fricosu* 841 F Supp 2d 1232, 1237 (D Colo, 2012).

135 Hash values are created by file sharing software. On file sharing, or peer-to-peer, networks, files are not located in one central place. Rather, the file sharing software creates a shared folder on each user's computer into which downloaded files are sent and stored. That shared folder and its contents are visible to all other users on the file sharing network. When a user wants to download a specific file, rather than downloading the complete document from a central depository, it is downloaded in multiple 'packets' from several different shared folders on the file sharing network. Those packets are joined together to form a complete file. To ensure that the packets are all from the exact same file, the software uses a hashing algorithm to create a unique hashtag for each file. This means that any files containing the same hashtag are identical. If there is any amendment to the file it will be given a new, unique hashtag. The police have a database of hashtags that have been identified as containing child pornography.

136 *Apple Mac Pro* 851 F 3d 238 (3rd Cir, 2017) (In this matter there was also evidence from a witness that she had seen child pornography on the computer in question); *In the Matter of the Decryption of a Seized Data Storage System* (ED Wis, No 13-M-449, 19 April 2013).

137 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1339 (11th Cir, 2012).

138 Ibid 1343.

139 Ibid 1344.

140 Ibid 1346.

The strict standard demonstrated in *In re Grand Jury Subpoena Duces Tecum* is found in other cases. In *Securities Exchange Commission v Huang*,[141] former bank employees who were being investigated by the Securities Exchange Commission ('*SEC*') for trading irregularities refused to provide the password to their bank issued smartphones, which were believed to contain evidence supporting the allegations. The Court held that the SEC was unable to establish that any of the documents it sought were on the smartphone. In *State v Trant*,[142] the defendant was arrested for drug trafficking. Two phones were found on the defendant upon arrest, one of which belonged to his mother. Despite evidence that the defendant had used a smartphone to send text messages to a police informant to arrange the sale of cocaine, and even though the defendant had possession and control of the devices at the time they were seized, the Court found that the State did not know that it was one of those phones that had been used to send the text messages.[143] The foregone conclusion doctrine was not satisfied.[144]

Notwithstanding the divergence apparent in the case law, there is relatively consistent support for an understanding that the knowledge requirement, when applied to the contents of an encrypted device, is not satisfied by possession or control of the device, even where there is additional evidence that the device in question has recently been used to communicate with another party about the subject matter of the investigation. As will be discussed in Chapter 4, in adopting this approach the courts of the United States have imposed a far stricter requirement than that applied by the courts in England and Wales and Australia. This is because while the contents test requires the state to know with reasonable particularity what is contained on the electronic device, the knowledge requirement in England and Wales is that of reasonable grounds for believing that relevant material will be found, while in Australia the state only needs to show

---

141 *Securities Exchange Commission v Huang* (ED Pa, Civ No 15-269, 23 September 2015).

142 (Me Super Ct, No 15-2389, 22 October 2015).

143 *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015).

144 See also *GAQL v Florida* 257 So 3d 1058 (Fla App 4 Dist, 2018) where the Court held that the State could not establish with reasonable particularly that specific Snapchat messages were on the suspect's phone even though the State had a witness who testified that she had been a party to the relevant Snapchat messages with the suspect a few days prior to the seizure of the suspect's phone. Cf *Commonwealth v Jones* 34 Mass L Rptr 287 (Mass Super Ct, 2017) in which the standard was satisfied where the State had evidence that the smartphone had been used to send text messages relevant to the sex trafficking charges.

reasonable grounds for suspecting such evidence will be present on the electronic device.

While the use of the contents test separates the United States from Australia and England and Wales, under the control test the knowledge requirement regarding the contents of the encrypted device is relatively closely aligned with those jurisdictions. This is because, as noted in Part 3.3.2 above, even though the control test rejects the requirement that the applicant for a compelled production order know with reasonable particularity what is contained on the encrypted device, it still requires probable cause to believe something will be on the electronic device. This requirement, however, is imposed at the stage that the search warrant is issued, in much the same way as similar requirements operate in England and Wales and Australia.

The case law reveals that a fundamental distinction between the control and contents test is that the latter holds that what is important is not what is produced – namely, a password – but what is sought to be accessed with what is produced. It is this understanding that is rejected by the control test. In *Commonwealth v Gelfgatt*,[145] the Court stated that

> the facts that would be conveyed by the defendant through his act of decryption – his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key – already are known to the government and, thus, are a "forgone conclusion".[146]

In other words, the testimony that is given by the act of decryption includes knowledge of the password but does not include testimony about knowledge of the contents of the encrypted device. In that circumstance, knowledge of the encrypted material is not necessary to satisfy the foregone conclusion doctrine.[147]

---

145 11 NE 3d 605 (Mass, 2014).

146 *Commonwealth v Gelfgatt* 11 NE 3d 605, 615 (Mass, 2014). See also *United States v Blatney* (A F Ct Crim App, No 2016-16, 22 May 2017).

147 Orin Kerr made this same argument in a recent article: Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 782-3. See also *United States v Spencer* (ND Cal, Case No. 17-cr-00259-CRB-1, 26 April 2018), slip op 3 where the Court stated that decrypting the devices does not entail an admission that specific files are on that device; *Commonwealth v Davis* 176 A 3d 869, 876 (Pa, 2018); *Aptos Residence* (ND Cal, Case no. 17-mj-70656-JSC-1, 20 March 2018) slip op 10 where the Court held 'that the testimony inhering to

The control test, then, stands for the proposition that the act of decryption provides no testimony about what is contained on the encrypted drive; the contents are divorced from the password. The only testimony that is given is that the suspect knows what the encryption key is. In *Apple Mac Pro*, the Court stated that 'the fact known to the government that is implied in the act of providing the password for the devices is "*I, John Doe, know the password for these devices*"'.[148] As the foregone conclusion doctrine only requires knowledge of the testimony that is given by the act of production, that knowledge is limited to knowledge of the password. As noted earlier in Part 3.3.1, however, additional knowledge may be required under the control test where the order demands the production of the decrypted documents.

Given the nature of the control test, there is less variation in how it is applied by the courts than there is with the contents test. This is so because there are less issues over which courts can disagree when applying the control test as knowledge of the contents of the device does not arise for consideration. The consequence of this is that when the control test is adopted, whether the foregone conclusion has been satisfied is determined by whether the government has led sufficient evidence regarding the suspect's knowledge of the password. Any variation that exists in the application of the control test is therefore the same variation that exists in the application of the foregone conclusion doctrine in respect of knowledge of the password. The variation that has arisen in the assessment of that element was discussed in Part 3.3.2.1.

Having identified and outlined the competing control and contents tests in the passages above, a more thorough analysis of which of those tests has the greater merit is deferred for now. That deferral is required because there is one remaining element of the foregone conclusion doctrine that needs to be discussed, and it too is affected by the

---

the act of decryption is that Mr Spencer knows the encryption password. The act of decryption requires nothing more'. One further case make the same point, though it is unclear from that decision whether the order sought the act of decryption or some other form of order: *State v Stahl* 206 So 3d 124, 134 (Fla Ct App, 2016) (producing the password does not involve an acknowledgement that one knows the contents of the device).

148 *Apple Mac Pro* 851 F 3d 238, 248 (3rd Cir, 2017).

choice between the control and contents tests. That remaining element, of authentication of the evidence produced by a compelled production order, is analysed in Part 3.3.2.3 below. Once that is complete, further analysis of the respective merits of the control and contents tests will take place in Part 3.3.3.

3.3.2.3 Authentication and the foregone conclusion doctrine

In almost every case in which the foregone conclusion is discussed, the courts have stated that an element of the doctrine is a requirement that the act of production cannot be relied upon to authenticate the evidence. However, as the Court in *Aptos Residence* noted, 'the authenticity element is routinely cited but only loosely applied if at all'.[149] What, then, does this element require, and why is it so little discussed?

The authenticity element requires the government to demonstrate that the documents produced are what they purport to be.[150] As the foregone conclusion doctrine requires the government to be able to authenticate the documents without resort to the suspect's act of production, the government needs someone other than the suspect to testify as to the authenticity and accuracy of the documents produced.[151] In the context of the compelled production of a password, however, this element is problematic – and the most likely reason that, save for perfunctory references to it, it is never properly analysed by the courts. Consider leading Supreme Court precedent on the foregone conclusion doctrine. In *Fisher*, financial documents prepared by an accountant were subpoenaed;[152] in *Doe II*, bank documents were sought;[153] and in *Hubbell*, documents relating to fraud and tax evasion were subpoenaed.[154] In each of those instances, it was a matter of vital importance that the document that was produced was authentic; phrased differently, that it was what it purported to be.

149 *Aptos Residence* (ND Cal, Case no. 17-mj-70656-JSC-1, 20 March 2018), slip op 19.
150 Ibid slip op 19. See also *United States v Gavegnano* 305 Fed Appx 954, 957 (4th Cir, 2009).
151 *Fisher* 425 US 391, 412 (1976).
152 Ibid 412.
153 *Doe II* 487 US 201 (1988).
154 *Hubbell* 530 US 27 (2000).

In almost all the compelled production cases considered in this thesis, however, the ability to independently authenticate the documents or password is irrelevant. Assume the contents test is applied to a matter involving child pornography, a common occurrence in the case law. A concept of authenticity cannot be applied in that instance. Whether an image satisfies the definition of child pornography depends on what is in the image: it either is or it is not child pornography. While a bank document may be forged, and a tax document may be altered to reflect a false financial position, the offence of child pornography simply requires possession of an image satisfying the definition of child pornography. It does not matter where the image came from; who created it; or how many hands it has passed through. It only matters whether it satisfies the definition of child pornography. It is irrelevant whether the image on the computer has been altered from the image originally obtained by the suspect. It only matters that the image still satisfies the requirement of child pornography. The same is true of terrorism material.

In some instances, authenticity may be relevant. In *State v Stahl*,[155] for example, access was sought to the suspect's phone to look for a video which would show the suspect filming up a woman's skirt. While the authenticity of such a video may be a relevant consideration, it could be authenticated through other means, most notably by the woman who was the victim of the offending. It is unsurprising, then, that the element of authenticity is little discussed in the cases. In the overwhelming majority of them it has no role to play; and in those cases in which it might arise, a factual determination will need to be made as to whether authentication can occur through other means.

How does the authentication requirement operate if the control test is adopted? That test requires the government to know as a foregone conclusion that the password exists, that the suspect knows what it is, and that it is authentic.[156] In this situation it is the authenticity of the password that is in issue. As the password is likely to be retained only in the suspect's mind (or reduced to writing in a location known only to the suspect), it is highly unlikely that another person will know the password, the more so if

155 206 So 3d 124 (Fla Ct App, 2016).
156 Ibid 136.

that password is used to secure incriminating evidence. That being so, authentication is only likely to be possible either through the act of using the password to unencrypt the drive or through the defendant's testimony. As the latter option is unlikely to ever occur,[157] self-authentication stands as arguably the only means of authenticating a password.

Self-authentication has judicial support. In *State v Stahl*, the Court noted that:

> The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established, with reasonable particularity based upon cellphone carrier records and Stahl's identification of the phone and the corresponding phone number, that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. <u>If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating – no other means of authentication may exist</u> (emphasis added).[158]

Similar sentiments have been expressed in the recent decisions in *Commonwealth v Davis*[159] and *State v Andrews*.[160]

A refusal to accept self-authentication would render the foregone conclusion all but inoperative in this area of the law when the control test is applied. This is because the only way in which to authenticate the password would be to show that the government knows what it is through other means, yet if it could show that knowledge it would have no need to compel the act of decryption as it could decrypt the device with its existing knowledge. At the time of writing no court had adopted the view that the foregone conclusion doctrine was doctrinally incompatible with the compelled production of a password. The opposite is true: all courts that have dealt with the compelled production

---

157 While it is possible that a suspect could authenticate the password by testifying that it is the correct password, since the need to compel a suspect to reveal a password only arises in circumstances where the suspect refuses to provide the password voluntarily, it is hard to envisage a circumstance in which a suspect refuses to provide the password in the absence of compulsion but once so compelled voluntarily authenticates that password, particularly if that password is inadmissible without his or her testimony authenticating it – which would be the case if self-authentication is not accepted.

158 *State v Stahl* 206 So 3d 124, 136 (Fla Ct App, 2016). Agreement was expressed with this argument in *Commonwealth v Davis* 176 A 3d 869, 876 (Pa, 2018).

159 176 A 3d 869 (Pa, 2018).

160 197 A 3d 200 (NJ Super App Div, 2018).

of a password have considered the role of the foregone conclusion doctrine in their analysis. If courts accept the role of the foregone conclusion doctrine, if they frequently find the foregone conclusion doctrine to have been satisfied, rejecting self-authentication would constitute a radical departure from that position given the largely inevitable consequence of its rejection.

In practice, then, and as is tacitly accepted by the cases, the authentication requirement is largely inapplicable to compelled production cases. On those few occasions when it may be relevant, a circumstance that only occurs if the contents test is applied, whether it can be satisfied will depend on the facts of that particular case.

3.3.2.4 Summary of the position in the United States

Two main conclusions can be drawn from the analysis above. First, it is relatively settled that in the United States, the use of a biometric feature to decrypt an encrypted device does not infringe the privilege. That is because the use of a biometric feature does not require the suspect to use the contents of his or her mind – an essential element of the privilege which, if lacking, means that the evidence produced is not testimonial evidence. Treating decryption through biometrics in this way is also consistent with the analogy drawn by the Supreme Court between producing a physical key to a safe and using a combination key to a safe: the former is a non-testimonial act; the latter a testimonial one.

Secondly, any compliance with a compelled production order that does not involve the use of a biometric features is, initially at least, an infringement of the privilege. In most instances, the privilege will be engaged as a result of the act of production doctrine, though there is some support in the case law for holding that the act of giving the password to a law enforcement official (as opposed to using it to decrypt the encrypted material) may itself be testimony falling under the privilege without the need to resort to the act of production doctrine. If the privilege is engaged through the act of production doctrine, the foregone conclusion doctrine may in turn be enlivened depending on the facts. It is in the application of the foregone conclusion doctrine that the major split in the case law arises. If the control test is adopted, the state is not

required to have any knowledge of the contents of the encrypted drive beyond that which is required to obtain a search warrant. That is the same approach which, as shall be discussed in Chapter 4, is adopted in England and Wales and Australia. By contrast, the contents test does impose a knowledge requirement concerning the contents of the encrypted drive, a requirement that distinguishes the approach in the United States from that in the remaining jurisdictions.

Though harmony between the jurisdictions may be one reason for favouring the control test over the contents test, there exist other, compelling reasons for believing the control test to be preferable to the contents test. Those reasons are explored in Part 3.3.3 below.

3.3.3 The control test is preferable to the contents test

In Parts 3.3.3.1, 3.3.3.2 and 3.3.3.3 below it is argued that the control test is preferable to the contents tests. Which of the competing tests prevails is significant for at least two reasons. First, and as already noted above, the control test is closely related to the test adopted in England and Wales and Australia concerning knowledge of the contents of the encrypted device. The adoption by England and Wales and the United States of a broadly similar test on this issue would provide a strong endorsement of the approach adopted in Australia. Secondly, at present the decisions of the courts of the United States – which are largely found in the lower courts – are in conflict. In time, the Supreme Court may be called upon to determine this issue. As the two tests lead to different outcomes, which of those tests is ultimately adopted will affect the scope of the privilege in the United States when applied to compelled production orders. In the sections below, it is argued that the control test more faithfully applies established Supreme Court principles concerning the act of production and foregone conclusion doctrines. If that argument is correct, it is to be expected that the control test – with the more limited scope that it grants to the privilege than the contents test – is more likely to be adopted by the Supreme Court. Furthermore, the reasons relied upon by courts in support of the contents test should therefore be treated with more caution than those advanced in support of the control test.

Though this thesis argues below that the control test is more faithful to established principles than the contents test, as Part 3.3.2.2 above has shown, there is substantial judicial support for the opposing contents test. Moreover, the contents test has academic support.[161] That support, however, adds little to what the courts have said, and fails to address the criticisms of the contents test that are raised below. Those criticisms, which include both theoretical and practical objections to the contents test, argue strongly for the adoption of the control test.

3.3.3.1 The contents test incorrectly applies the act of production doctrine

One of the fundamental problems with the contents approach is revealed by the Supreme Court decisions – *Fisher* and *Hubbell* – relied on in *In re Grand Jury Subpoena Duces Tecum*. *Fisher* concerned a summons served on Fisher's solicitor requiring the accountant to produce documents he possessed which had originally been prepared by Fisher's accountant. It was not disputed that if the service of that subpoena on Fisher would have engaged the privilege, then Fisher's attorney to whom the subpoena had been served would be immune from having to comply with it.[162] The Supreme Court held that the privilege was not engaged as Fisher was not required to give oral testimony, nor was he required to 'restate, repeat, or affirm the truth of the contents of the documents'.[163] The documents had been voluntarily prepared by someone other than Fisher and therefore they did not fall under the privilege.[164] In *Hubbell*, a subpoena was served on Hubbell requiring production of 11 different categories of documents. The breadth of that request resulted in Hubbell producing more than 13,000 documents.

---

161 Laurent Sacharoff, 'What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr' (2019) 97 *Texas Law Review* 63; Sacharoff, 'Unlocking the Fifth Amendment', above n 45, 208; Jaffer and Rosenthal, above n 95, 301 fn 124; Jody Goodman, 'Forced Data Decryption: Does it Violate the Fifth Amendment?' (2013, Winter) 27 *Criminal Justice* 43, 43-44; Adam M Gershowitz, Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest? (2011) 96 *Iowa Law Review* 1125, 1173. See also Minerva Pinto, The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing (2016) 25 *Temple Political and Civil Rights Law Review* 223, 231; Wiseman, above n 89, 551-52; Aaron M Clemens, No Computer Exception to the Constitution: The Fifth Amendment Protects against Compelled Production of an Encrypted Document or Private Key (2004) *University of California Los Angeles Journal of Law and Technology* 2, 11.

162 *Fisher* 425 US 391, 396 (1976)

163 Ibid 409.

164 Ibid 409. See also at 397 where it was said that '[t]he Court has held repeatedly that the Fifth Amendment is limited to prohibiting the use of "physical or moral compulsion" exerted on the person asserting the privilege'.

The Court found the act of production had been enlivened in this case as Hubbell was required to use the contents of his mind to collate and review the documents.

Thus, in *Fisher*, in *Hubbell*, what was to be produced by the defendants were the very document said to incriminate them. Such is not the case with a password. The password itself is not incriminating,[165] though it may lead to incriminating evidence. In *Fisher* and *Hubbell* it followed as a matter of logic that the government needed to know of the existence and location of the documents it sought by way of subpoena – of the incriminating evidence itself – in order for the foregone conclusion doctrine to apply as it was those documents that added to the government's knowledge of the offending. Put simply, as it was documents that were to be produced, knowledge of them was required. However, when a password is compelled what is produced is the password, not the documents.

This argument has academic support. Orin Kerr has written that 'the foregone conclusion doctrine asks if the testimony inherent in the act was already known to the government'.[166] To answer that it is necessary to determine what the person is required to do and 'what testimony is implicit in [that] act'.[167] In the context of compelled decryption, the implied testimony is that the person knows the password exists, that it has been asked for and that he or she knows what the password is.[168] That is the knowledge that the government needs to know as a foregone conclusion.[169] Furthermore, it has been noted that the act of decryption makes no communications

---

165 This is readily evident. If a person provides a password and no incriminating evidence is found on the encrypted device (and assuming there is no other incriminating evidence), no conviction will follow for the simple reason that there is no evidence against the accused. Thus, the password itself is not incriminating.

166 Orin Kerr, 'The Fifth Amendment Limits on Forced Decryption and Applying the Foregone Conclusion Doctrine', The Washington Post (online), 7 June 2016 <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/>.

167 Ibid.

168 Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 783. See also Orin Kerr, 'Fifth Amendment Protects Passcode on Smartphone, Court Holds', The Washington Post (online), 24 September 2015 <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds/>.

169 Kerr, 'The Fifth Amendment Limits on Forced Decryption', above n 165.

about the content of the device that has been decrypted.[170] If one accepts that the act of decryption does not make a statement about the content of the decrypted device, there should be no need for the government to have knowledge of the contents before the foregone conclusion doctrine can apply.[171]

Drawing on that understanding, Kerr has further argued that '[t]he details of what records are on the phone should be irrelevant to whether the foregone conclusion doctrine applies because access to the phone is independent of what records are stored inside it'.[172] Phrased differently, the testimonial aspect does not change depending on the content of the phone.[173] While the act of decryption does communicate the suspect's control of the device, where access and control are foregone conclusions that communication lacks a testimonial element.[174]

So understood, the Court in *In re Grand Jury Subpoena Duces Tecum* erred. The cases on which *In re Grand Jury Subpoena Duces Tecum* relied, *Hubbell* and *Fisher*, were concerned with the production of physical documents. When those documents are produced, the person impliedly testifies that the documents he or she has handed over fall within the scope of the order and are believed to show evidence of the alleged crime. In that context, it makes sense that the foregone conclusion doctrine can only apply if the government knows that the files exist, where they are and that they are in the accused's possession or control. By contrast, providing a password provides no

---

170 Kerr, 'Compelled Decryption and the Privilege Against Self-Incrimination', above n 36, 779; Joseph Jarone, 'An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption' (2015) *Florida International University Law Review* 767, 791-792.

171 Jarone, above n 169, 793.

172 Kerr, 'Fifth Amendment Protects Passcode on Smartphone', above n 167.

173 It is for this reason that the focus of the test should be on the password and not the encrypted documents. Focusing on the documents has the further consequence that any compelled evidence not otherwise infringing the privilege may retrospectively be deemed an infringement of the privilege if it leads to incriminating evidence. Such a view finds no support in the case law and contradicts statements by the Supreme Court that a compelled statement that is not testimonial does not become testimonial because it leads to incriminating evidence: *Doe II* 487 US 201, 208-9 (1988). See also *Byers* 402 US 424, 433–434 (1971) (non-testimonial evidence does not become testimonial merely because it provides a link in the chain of evidence).

174 Jarone, above n 169, 795.

testimony about what documents, if any, exist and whether the person providing the password has possession or control of them.

3.3.3.2 The contents test cannot adequately respond to the time gap problem

With some limited exceptions, in most decisions in which the state can show some level of evidence regarding the contents of the electronic device there is a gap in time between the point at which the state gains possession of the electronic device and the moment at which the electronic device was known to hold the material in question. In *Pearson*, for example, that the defendant received emails containing child pornography did not mean that he retained that material on his computer by the time it was seized by the police. Likewise, though there was evidence in *Apple Mac Pro* that child pornography had been on the defendant's computer, there was no evidence that it remained on the computer at the time it was seized. The same story is evident in several other cases,[175] and it is a problem that has been identified in the literature on compelled decryption.[176]

For the Court in *Pearson* to have been satisfied that the material in question was on the defendant's computer at the time the subpoena was issued (and would remain on it until it was executed) it must, arguably, have either ignored the gap in time problem or, more likely, have tacitly accepted that the requirements of the doctrine will be met if evidence is led that the documents in question had been on the computer in the recent past. In many respects such an approach is a practical necessity. Save for rare cases like the *Boucher* cases and *United States v Fricosu*, the best evidence that can usually be put forward is that the offending material has recently been on the electronic device and is believed to still be there. To demand more would in all but a few cases foreclose the availability of the doctrine. Nevertheless, the manner in which the time gap problem has been resolved by courts appears inconsistent with the reasonable particularity test.

---

175 See, eg, *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335 (11th Cir, 2012); *Commonwealth v Gelfgatt* 11 NE 3d 605 (Mass, 2014); *State v Stahl* 206 So 3d 124 (Fla Ct App, 2016); *Securities Exchange Commission v Huang* (ED Pa, Civ No 15-269, 23 September 2015); *Baust* 89 Va Cir 267 (2014).

176 Mohan and Villasenor, above n 36, 23.

This issue has been considered in the Canadian decision of *R v Cusick*.[177] In a matter in which the defendant challenged the police's delay in obtaining and executing a search warrant after first becoming aware of the defendant having uploaded potentially illegal material from his computer to a Microsoft cloud account, Ricchetti J said the following:

> A search warrant for a computer will inevitably be issued after the fact, at the earliest days after the reasonable and probable grounds for belief have come to the attention of the police. Within the time period for the police to seek and execute a search warrant, it could not possibly be known what the "chances" are that the files in question remain or were deleted permanently or whether any electronic artifact of the file continues to exist. Unfortunately, that is the nature of computer evidence in the digital age. This difficulty as to the likelihood of evidence being found on computers has now been compounded by the ability to use cloud storage so that very little may actually be on a computer's hard drive or other computer equipment in the user's home. Much of what used to be on a person's computer is now on large servers somewhere in the world. As we see from the evidence in this case, what may be the only thing left on the computer equipment are electronic artifacts of the computer's use of the cloud or evidence of use of the same user account.
>
> The police will never know what the "chances" are that the electronic artifacts or use of the same user account after the police receive the information, let alone months later. Does the fact the police cannot specify what the "chances" are that artifacts or the user account on the computer used might no longer be there mean that search warrants cannot be issued to search computers? Of course not. The trial judge erroneously disregards that what the police must show is "reasonable and probable" grounds to believe that the search will provide evidence of the offence. The test is "credibly based probability" that there would be evidence of the offence found at the location. The circumstances and the amount of time since the alleged use are relevant to the "credible based probability" that the computer will continue to have evidence such as the use of the email address or computer artifacts.[178]

While the *Cusick* decision demonstrates how the time gap problem need not be insurmountable, it is notable that the test for the issue of the search warrant in *Cusick* (reasonable and probable grounds to believe) differs from the reasonable particularity standard applied in *In re Grand Jury Subpoena Duces Tecum*. In fact, the *Cusick* test shares broad similarities with that required for the issue of a search warrant under the control test, as well as in Australia and England and Wales. In other words: while the control test and English and Australian standards are sufficiently accommodating to account for the time gap problem, the standard imposed by the contents test is too

---

177 2015 ONSC 6739, 126 WCB (2d) 270. Note that an appeal from this decision was dismissed by the Ontario Court of Appeal in June 2019: *R v Cusick* 2019 ONCA 524.

178 *R v Cusick* 2015 ONSC 6739, 126 WCB (2d) 270, [141]-[142].

demanding to do so, particularly in as much as it requires the applicant to know that the evidence is on the computer. The result is that under current doctrine and in the absence of a Supreme Court decision lowering the standard required to be met to show knowledge of the contents of an encrypted drive, the time gap problem either remains largely unsolvable under the contents test or it gets tacitly ignored. Under the control test, by contrast, this problem does not arise.

3.3.3.3 The contents test leads to the wrong focus

When courts have applied the contents test, they have frequently done so by asking whether the state knew with reasonable particularity that the evidence existed in a specific location, that it was possessed by the accused and that it was authentic.[179] Vivek Mohan and John Villasenor have argued that reference to the location of the evidence is misplaced, ill-suited to modern demands (which include storage of documents on the cloud),[180] and inconsistent with *Hubbell* and *Fisher*. In *Hubbell*, they argue, the Court did not require the government to know the location of the evidence; rather, the Court spoke of how the foregone conclusion doctrine was inapplicable if the government could not establish existence, possession (or control) and authenticity without the compelled act of production.[181] That standard can be achieved without needing to show the location of specific documents. They argue that if courts required knowledge of possession or control instead of location, the foregone conclusion doctrine would more accurately reflect the Supreme Court's decisions in *Fisher* and *Hubbell* and the doctrine could be satisfied more easily.[182]

There is significant force in this argument. In *Fisher*, the Court spoke of how the act of production may concede 'the existence of the papers demanded and their possession or control by the taxpayer' (emphasis added).[183] That statement was affirmed by the

179 See, eg, *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1344 (11th Cir, 2012), *United States v Fricosu* 841 F Supp 2d 1232, 1237 (D Colo, 2012); *Commonwealth v Gelfgatt* 11 NE 3d 605, 617 (Mass, 2014) (Lenk J, dissent); *Boucher II* (D Vt, No 2:06-mj-91, 19 February 2009), 3; *Pearson* (ND NY, No 1:04-CR-340, 24 May 2006).

180 Mohan and Villasenor, above n 36, 20.

181 Ibid 22.

182 Ibid 23.

183 *Fisher v United States* 425 US 391, 410 (1976).

Court in *United States v Doe*,[184] *Doe II*[185] and *Hubbell*.[186] The *Hubbell* Court also spoke repeatedly about the 'existence, authenticity and custody of items that are produced'.[187] What is common through those decisions is the understanding that for the foregone conclusion doctrine to apply, knowledge of the location of the documents is not required. Rather, it is knowledge of the existence of the documents and their possession or control by the accused that needs to be shown. Knowledge of the location of the documents will usually follow from that information, where applicable.

That the document's location is not an essential element of the act of production and foregone conclusion doctrines is further emphasised by the fact that neither *United States v Doe* nor *Doe II* refers to the location of a document when discussing those doctrines. While *Hubbell* and *Fisher* do refer to the location of the documents, those references are arguably used as an adjunct to the existence requirement.[188] Indeed, that is how it was understood in *In re Grand Jury Subpoena Duces Tecum*, where the Court, in discussing the foregone conclusion doctrine, held that 'an act of production is not testimonial – even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed material…' (emphasis added).[189]

Notably, the control test is not concerned with the location of the relevant evidence as compelling the production of a password does not involve the compelled production of a physical document. To ask where the password is located is misguided and largely nonsensical – in almost all cases it will be retained in the suspect's mind. However, when the court asks whether the government can establish the existence of the password, its authenticity and the suspect's possession or control of it, the test remains coherent, jurisprudentially consistent and well adapted to the problem of compelled decryption.

184 465 US 605, 614 (1984).
185 *Doe II* 487 US 201, 209 (1988).
186 *Hubbell* 530 US 27, 36 (2000).
187 Ibid 40-41.
188 *Fisher* 425 US 391, 411 (1976); *Hubbell* 530 US 27, 44-45 (2000).
189 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012).

3.4 LESSONS FROM THE CANADIAN AND UNITED STATES' APPROACHES TO COMPELLED PRODUCTION ORDERS

What are the key lessons that can be taken from the experiences of the courts of Canada and the United States when hearing an application for a compelled production order? The first is that there is limited benefit that can be derived from the Canadian experience. As Chapter 1 identified, Canadian courts have afforded the privilege a broader scope than the other jurisdictions considered in this thesis have, one that appears to encompass any incriminating evidence that has been obtained through the coercion of the suspect. That scope, together with the constitutional status of the privilege, has resulted in Canadian courts refusing all applications for compelled production orders, regardless of whether the password was numeric, alphabetic or biometric. In adopting so strict a position, Canada stands alone. Significantly, the reasons for the Canadian position – the constitutional status of the privilege and an understanding that it applies to any incriminating evidence that has been obtained through the coercion of the suspect – are ones that do not apply to Australia. The former, because the privilege does not hold the same status in Australia; the latter, because so broad a scope has been rejected by Australian courts.

With regard to the United States, which of the control or contents tests is ultimately endorsed by the Supreme Court may affect the utility of the cases of the United States for comparative purposes. Adoption of the control test would bring Australia, England and Wales and the United States broadly into alignment. That fact alone would provide a relatively substantial endorsement of the Australian position regarding the evidence that the state must possess about the contents of the encrypted device. The contents test, by contrast, with its test of reasonable particularity, imposes an additional obligation that far exceeds that found in the English or Australian statutes. It is, furthermore, an obligation that is arguably unjustified as it appears to rest on a misunderstanding of Supreme Court precedent on the act of production doctrine. To adopt a similar requirement in Australia would be to impose a heightened evidentiary burden not required to search for any other evidence pursuant to a search warrant. Moreover, even as some courts have endorsed the contents test in the United States, they have refused to apply it strictly, at least with regard to the time gap problem. The

contents test, then, is one apparently adrift of the moorings of the act of production doctrine, and one that cannot be implemented in accordance with its own terms due to the time gap problem.

A further objection can be had with the United States' approach: the different treatment given to the privilege depending on the manner by which the encrypted device is decrypted. Objections to this different treatment have been made by courts, often in the context of the safe analogy. In *State v Stahl*, the Court wrote that '[w]e question whether identifying the key which will open the strongbox – such that the key is surrendered – is, in fact, distinct from telling an officer the combination. More importantly, we question the continuing viability of any distinction as technology advances'.[190] It was the Court's view that the Fifth Amendment was not intended to provide different levels of protection depending on whether your smartphone was locked with a password or the fingerprint scanner, and as fingerprint scanners were not protected under the privilege neither should the use of a password.[191] In *State v Trant*, the Court observed that

> the line between testimonial and non-testimonial is very fine, and that [the] application of Fifth Amendment jurisprudence produces what may appear to many to be an absurd result, whereby suspects who use a four-digit password to protect information on their electronic devices are given full sanctuary, and suspects who use their fingerprint to protect information are given no sanctuary. Given the daunting task of reconciling Fifth Amendment case-law (and the values underlying that jurisprudence) with the enormous challenges posed for law enforcement by modem encryption technology, resolution of the issues posed by password-protected cellphones may need to await consideration by the U.S. Supreme Court.[192]

These criticisms have academic support, with several academics noting that the Supreme Court's dicta that a physical key can be compelled but a combination key cannot is seemingly arbitrary and leads to an outcome that is difficult to justify: if you lock your phone with a password it cannot be compelled, but if you use your fingerprint it can.[193]

---

190 *State v Stahl* 206 So 3d 124, 135 (Fla Ct App, 2016).

191 Ibid 135. A similar comment is made in *United States v Spencer* (ND Cal, Case No. 17-cr-00259-CRB-1, 26 April 2018) slip op 3.

192 *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015), 8-9 fn 3.

193 See, eg, Dan Terzian, The Fifth Amendment, Encryption and the Forgotten State Interest (2014) 61 *University of California Law Review Discourse* 298, 305; John E D Larkin, 'Compelled

There is much force in this criticism. While the path that the case law of the United States has taken to reach its position on compelled production orders is clear and consistent with earlier precedent, that does not mean that the outcome it has reached is desirable, and even less so that it is one that Australia should seek to replicate. If the question that is asked is whether the state can compel a suspect to provide a password to lawfully seized but encrypted electronic data, the answer to that question should not depend on the form that the password takes.

Finally, in one respect the United States appears to have departed from previous decisions on the scope of the privilege. In *Breithaupt* and *Byers*, the scope of the privilege was determined after weighing the competing interests of the public and of the suspect. In both those interests, the balance fell in favour of the public interest. To date, no court has engaged in a similar balancing exercise when considering compelled production orders. Despite that, the analysis undertaken in Chapter 1 suggests that an argument can be made that the scope of the privilege does not encompass the giving of a password. As has been made clear on several occasions, the privilege is not an absolute right but rather is one the contours of which are determined by balancing the public and the private interests.[194] There are reasons for believing that balancing could favour the exclusion of the privilege. Like motor vehicle reporting obligations, the information requested of the suspect is limited and not of itself incriminating; the information revealed would provide substantial assistance to law enforcement officials; there is no risk of false information being provided; and no new evidence is created through the act of compulsion. As will be seen in the next Chapter, the use of a balancing test that considered those very factors is a feature of both the English and Australian positions. It is not immediately clear why the courts of the United States did not consider a similar approach.

Production of Encrypted Data' (2012) 14 *Vanderbilt Journal of Entertainment and Technological Law* 253, 270; Carin Myers Morrison, 'Passwords, Profiles, and the Privilege against Self-Incrimination: Facebook and the Fifth Amendment' (2012) 65 *Arkansas Law Review* 133, 148; David Colarusso, 'Heads in the Cloud, a Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination' [2011] 17 *Boston University Journal of Science and Technology Law* 69, 85.

194 See, eg, *Byers* 402 US 424, 427 (1971).

CHAPTER 4

ENGLAND AND AUSTRALIA

4.1 INTRODUCTION

Chapter 3 analysed how the United States and Canada have responded to the issue of compelled production orders. That analysis showed that in Canada, under the current statutory regime, compelled production orders – regardless of the form they take – infringe the privilege and are therefore unlawful. In the United States, such orders have also been found to fall within the scope of the privilege, ordinarily through the operation of the act of production doctrine. It is the act of production doctrine, however, that also provides the means by which the privilege can be disengaged. If the applicant can show that the knowledge revealed by the act of production is a foregone conclusion (which requires the applicant to show that it knows of the existence of the evidence, the suspect's possession of the evidence and it can authenticate the evidence without the assistance of the suspect), then that act of production is taken to be a non-testimonial act to which the privilege will no longer apply. It is the foregone conclusion doctrine that lies at the heart of the United States case law, with the courts struggling to apply it consistently to compelled production orders. Specifically, under the contents test the government must know with reasonable particularity what is contained on the encrypted drive; under the control test, that requirement does not exist. As will be shown in this Chapter, the adoption of the control test would result in the United States adopting a broadly similar approach to that applied in England and Wales and Australia.

The reason for the separate treatment of England and Wales and Australia in this Chapter is as follows: while Canada and the United States seek to deal with applications for compelled production orders under existing statutory powers, England and Wales and Australia have enacted legislation that authorises the granting of a compelled production order in certain circumstances. In England and Wales, the *Regulation of Investigatory Powers Act 2000*[1] ('*RIPA*') provides for such orders; in Australia, legislation

[1] 2000 c 23, Part III.

has been enacted at the federal level,[2] as well as in Queensland,[3] Victoria[4] and Western Australia.[5] This Chapter considers how that legislation operates, how the privilege interacts with it and what comparisons can be drawn to the approaches already identified in Canada and the United States.

Before considering the terms of those statutes and how they have been applied by the courts, Part 4.2 describes the principles of interpretation relevant to the English and Australian legislation. At the heart of the interpretative exercise is the principle of legality, which relevantly holds that parliament does not discard fundamental rights or principles except by a clearly expressed intention or necessary implication. That principle is discussed both in Part 4.2 and Part 4.4. Part 4.2 also considers the role played by the *Human Rights Act 1998* and the *Victorian Charter* in the interpretation of the English and Victorian statutes. As will there be discussed, the *Human Rights Act 1998* has been interpreted as granting courts broad scope to read into, or read down, English statutes.

Part 4.3 addresses a further preliminary issue by considering whether compelled production orders infringe the privilege in England and Wales and Australia. The importance of this question relates to the issue of abrogation: if the privilege is not implicated by such orders, there is no need for a statutory provision that abrogates the privilege. If, however, the privilege is engaged by a compelled production order, statutory abrogation is required. As discussed in Chapter 2, both England and Wales and Australia have previously abrogated the privilege to enable certain related orders to be made, as for example when imposing motor vehicle reporting obligations on the registered owner of a motor vehicle.

Part 4.4 is concerned with how relevant aspects of the statutory provisions providing for compelled production orders operate. That includes a discussion of how the privilege is

---

2 *Crimes Act 1914* (Cth) s 3LA.
3 *Police Powers and Responsibilities Act 2000* (Qld) s 154.
4 *Criminal Investigations Act 2006* (WA) s 59.
5 *Crimes Act 1958* (Vic) ss 465AA and 465AAA.

abrogated in the respective jurisdictions, whether different forms of order affect the privilege in different ways and the evidentiary burdens imposed by the legislation. The latter two issues were important aspects of the decisions of the courts of the United States.

Lastly, Part 4.5 considers the recent decision in *Luppino (2)* before Part 4.6 concludes the Chapter.

4.2 RELEVANT PRINCIPLES OF STATUTORY INTERPRETATION

At the heart of compelled production orders in England and Wales and Australia lies the issue of statutory interpretation: how have the courts of those jurisdictions interpreted the relevant statutory provisions? In this Part the thesis briefly outlines relevant principles that are utilised by Australian and English courts when interpreting the compelled production order provisions.

In *Project Blue Sky Inc v Australian Broadcasting Authority*, the Australian High Court said of the interpretative exercise:

> The primary objective of statutory interpretation is to construe the relevant provision so that it is consistent with the language and purpose of all the provisions of the statute. The meaning of the provision must be determined 'by reference to the language of the instrument viewed as a whole'. … Thus, the process of construction must always begin by examining the context of the provision that is being interpreted.[6]

The Court later went on to hold that:

> the duty of a court is to give the words of a statutory provision the meaning that the legislature is taken to have intended them to have. Ordinarily, that meaning (the legal meaning) will correspond with the grammatical meaning of the provision. But not always. The context of the words, the consequences of a literal or grammatical construction, the purpose of the statute or the canons of construction may require the words of a legislative provision to be read in a way that does not correspond with the literal or grammatical meaning.[7]

---

6 *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355, 381 [69].

7 Ibid 384 [78].

This approach is consistent with that required by the *Acts Interpretation Act 1901* (Cth), which requires the adoption of 'the interpretation that would best achieve the purpose or object of the Act'.[8] Notably, even where there is no ambiguity in the language of the statute, the court is still empowered to consider the purpose of the legislation so as to determine whether there is more than one permissible interpretation that is consistent with the purpose of the legislation, and which of those interpretations best gives effect to the purpose of the legislation.[9] While the rules above provide a starting point for a court faced with an application for a compelled production order, additional rules and principles further guide that process, including the principle of legality.

The principle of legality requires a court, when interpreting a statute, to engage in that act of interpretation with the understanding that the legislation is 'founded on the principles and traditions of the common law'.[10] In the words of the Australian High Court, 'judicial findings as to legislative intention are an expression of the constitutional relationship between the arms of government with respect to the making, interpretation and application of laws'.[11] A central aspect of that relationship is the understanding that fundamental human rights – such as the privilege – are not abrogated other than by the clearly expressed intention of parliament or necessary implication.[12] Furthermore, where a provision has the effect of abrogating the privilege, that provision is to be interpreted narrowly.[13] As recently noted by the High Court, 'the principle of legality favours a construction, if one be available, which avoids or minimises the statute's encroachment upon fundamental principles, rights and freedoms at

---

8 *Acts Interpretation Act 1901* (Cth) s 15AA.

9 *Mills v Meeking* (1990) 169 CLR 214, 235. See also *R (Westminster City Council) v National Asylum Support Service* [2002] UKHL 38, [5] where Lord Steyn stated that statutes are to be interpreted in light of their context even where there is no ambiguity in the language of the statute. Importantly, the context of a statute includes its purpose: David Lowe and Charlie Potter, *Understanding Legislation: A Practical Guide to Statutory Interpretation* (Hart Publishing, 2018) 49.

10 *R v Home Secretary; Ex parte Pierson* [1998] AC 539, 587.

11 *Zheng v Cai* (2009) 239 CLR 446, [28] as quoted in Dennis Pearce and Robert Geddes, *Statutory Interpretation in Australia* (LexisNexis Butterworths, 8th ed, 2014) 4.

12 See, eg, *Pyneboard Pty Ltd v Trade Practices Commission* (1993) 152 CLR 328, 341; *Electrolux Home Products Pty Ltd v Australian Workers' Union* (2004) 221 CLR 309, [19]-[21]; *Beghal* [2016] AC 88, 117 [61]; *R v Home Secretary; Ex parte Pierson* [1998] AC 539, 589.

13 Pearce and Geddes, above n 9, 378 and the authorities there cited.

common law'.[14] As the abrogation of the privilege is necessary for a compelled production order to be made in England and Wales or Australia, this presumption is of some importance in the interpretation of the relevant statutes.[15]

For England and Wales and Victoria, a further important interpretative question arises.[16] What effect do the *Human Rights Act 1998* and *Victorian Charter* have on the interpretation of the respective provisions authorising compelled production orders? Section 3 of the former statute provides that 'so far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way that is compatible with the Convention rights'; s 32 of the latter states that 'so far as it is possible to do so consistently with their purpose, all statutory provisions must be interpreted in a way that is compatible with human rights' (emphasis added). Do those provisions merely codify existing interpretative presumptions, or do they authorise courts to go further to protect rights such as the privilege?

The *Human Rights Act 1998* has been found to grant English courts new powers to interpret legislation in a manner consistent with the rights it protects. Importantly, the words 'so far as is possible to do so' have been interpreted by the House of Lords to impose a duty to ensure that the provision in question is read consistently with the *ECHR* 'unless it is plainly impossible' to do so.[17] That means that when it is necessary to give effect to a right, the duty imposed under s 3, which requires that legislation must be read compatibly with the *ECHR*, allows a court to read in or read down words in the relevant provision in a manner that departs from the legislature's intention when

---

14 *North Australian Aboriginal Justice Agency Limited v Northern Territory* (2015) 256 CLR 569, 581 [11].

15 While the principle of legality gives rise to several presumptions – such as the presumptions that a law is constitutional and that it does not operate retrospectively – they will not be considered in this Part. To the extent that they arise later in this Chapter they will be considered at that time.

16 The Australian Capital Territory, too, has a human rights statute but not legislation authorising the granting of a compelled production order. In Queensland, the *Human Rights Act 2019* (Qld) is being progressively implemented at the time of writing. Once fully enacted, this issue will arise there too.

17 *R v A (No 2)* [2002] 1 AC 45, 68.

drafting the provision.[18] The result is that even provisions that are unambiguous may need to be given a 'linguistically strained interpretation' to achieve compliance with the *ECHR*.[19]

By contrast, the Australian High Court has opposed granting s 32 a similar scope to s 3, finding instead that s 32 – which 'differs textually' from s 3 and 'finds its place in a different constitutional setting'[20] – does not change the established interpretation process.[21] In Victoria, then, as with all other Australian jurisdictions, the principle of legality and the existing common law presumptions continue to guide the interpretation of provisions such as those authorising the making of compelled production orders.

The above principles describe the approach that is to be taken by English and Australian courts to the interpretation of the respective statutory provisions authorising the granting of a compelled production order. In Part 4.4, how the courts have applied these rules to the respective provisions is considered. Before then, Part 4.3 will consider if compelled production orders infringe the privilege.

4.3 DO COMPELLED PRODUCTION ORDERS IMPLICATE THE PRIVILEGE IN ENGLAND AND AUSTRALIA?

In Part 4.4 below, the statutory provisions that Australia and England and Wales have enacted to deal with the issue of compelled production orders are discussed. Before then, this Part considers why that legislation is necessary. To do that it examines whether compelled production orders are an infringement of the privilege, for if they are such orders cannot be made in the absence of the statutory abrogation of the privilege. The structure for this Part is as follows: Part 4.3.1 examines the position in England and Wales in respect of alphabetic and numeric passwords; Part 4.3.2 considers

---

18 See, eg, *Ghaidan v Godin-Mendoza* [2004] 2 AC 557; *Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264; *R v A (No 2)* [2002] 1 AC 45.

19 John Wadham et al, *Blackstone's Guide to the Human Rights Act 1998* (Oxford University Press, 2nd ed, 2015) 3.38.

20 *Momcilovic v The Queen* [2011] 245 CLR 1, 38 [20] (French CJ).

21 Ibid 50 [50] (French CJ). See also Michelle Sanson, *Statutory Interpretation* (Oxford University Press, 2nd ed, 2016) 279 where the author argues that the High Court found that 's 32(1) applies in the same way as the principle of legality, just with a wider field of application'.

that same question in Australia; and Part 4.3.3 considers whether compelled production orders requiring the use of a biometric feature in either jurisdiction infringe the privilege.

4.3.1 Alphabetic or numeric passwords in England and Wales

In England and Wales, it is understood that the privilege does not apply to evidence having an existence independent of the will of the accused. This understanding is present in early decisions of the European Court of Human Rights – whose decisions are required to be taken into account by English courts – though the decisions of that Court are conflicting and open to criticism.[22] Initially, in *Saunders* the European Court of Human Rights found that

> The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing...[23] (emphasis added).

That understanding, however, appears to have since evolved into one that now focuses primarily on the will of the accused with limited regard being had to whether the evidence has an independent existence. It is through that evolution that the Court has been able to find that pre-existing documents[24] and narcotics retrieved from a suspect's stomach[25] fall within the scope of the privilege even though both are forms of evidence having an existence independent of the will of the accused.

Notwithstanding the difficulties in the European position, the English courts have more clearly accepted that evidence having an independent existence does not fall within the scope of the privilege. Thus, in *Attorney General's Reference (no 7 of 2000)*,[26] the Court of Appeal expressly adopted the approach set out in *Saunders*, holding that the

---

22 See the discussion of those decisions in Part 1.2.2.1.

23 *Saunders* (1997) 23 EHRR 313, 337–338, [68]–[69]. See also *Jalloh* (2007) 44 EHRR 32, [100].

24 *Heaney & McGuinness v Ireland* (2001) 33 EHRR 12.

25 *Jalloh* (2007) 44 EHRR 32.

26 [2001] 1 WLR 1879.

distinction drawn between 'statements made and other material independent of the making of a statement, is not only one to which we should have regard, but is one which, it seems to us, is jurisprudentially sound'.[27] Subsequent cases have continued to adopt this understanding of the privilege.[28] How, though, does it apply to cases involving the compelled production of an encryption key?

In *R v S(F)*, the accused refused to comply with an order made under s 49 of *RIPA*. At first instance, Judge Stephens QC found that the privilege against self-incrimination was not engaged as the evidence had an existence 'independent of the minds of the defendants' and that, even if the privilege was engaged, the infringement occasioned by the order was 'legitimate and proportionate'.[29] The defendants took that finding on appeal. Lord Judge CJ handed down the Court of Appeal's decision. In considering the role of the privilege, his Lordship observed that both English law and the European Court of Human Rights recognise that the privilege does not apply to 'evidence existing independently of the will of the subject', such as subpoenaed documents and bodily evidence.[30] To the question of whether the encryption key had an existence independent of the suspect's will, thus rendering it outside the scope of the privilege, his Lordship held that:

> On analysis, the key which provides access to protected data, like the data itself, exists separately from each defendant's "will". Even if it is true that each created his own key, once created, the key to the data remains independent of the appellant's "will" even when it is retained only in his memory, or at any rate until it is changed. If investigating officers were able to identify the key from a different source (say, for example, from the records of the shop where the equipment was purchased) no one would argue that the key was not distinct from the equipment which was to be accessed, and indeed the individual who owned the equipment and knew the key to it. Again, if the arresting officers had arrived at the premises in Sheffield immediately after S had completed the process of accessing his own equipment enabling them to identify the key, the key itself would have been a piece of information existing, at this point, independently of S himself and would have been immediately available to the police for their use in the investigation. In this sense the key to the computer equipment is no different from the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral.[31]

---

27 Ibid 1891 [58].

28 See, eg, *R v Kearns* [2002] 1 WLR 2815, [52]; *C plc v P (Attorney General Intervening)* [2008] Ch 1, 10-11 [16].

29 *R v S(F)* [2009] 1 WLR 1489, 1494 [15].

30 Ibid [18] and the cases there cited, including *Saunders* (1997) 23 EHRR 313; *Attorney General's Reference (No 7 of 2001)* [2001] 2 Cr App R 19; *R v Kearns* [2003] 1 Cr App R 7.

31 *R v S(F)* [2009] 1 WLR 1489, 1496 [20].

Drawing a comparison to blood samples, his Lordship held that just as a blood or urine sample was a fact independent of the suspect's mind, so too was an encryption key.[32] That conclusion notwithstanding, Lord Judge CJ proceeded to note that 'the fact of the defendant's *knowledge* of the keys may itself be an incriminating fact'.[33] This, Lord Judge CJ noted, was the approach adopted in the United States in *Boucher I*. His Lordship thus adopted an approach broadly consistent with the act of production doctrine in the United States, one in which the privilege 'may' be engaged by a requirement to provide an encryption key.[34]

Three years later in *Greater Manchester Police v Andrews*,[35] the English High Court adopted the same approach. The defendant, a convicted sex offender, was arrested on suspicion of having breached a Sexual Offences Prevention Order which prohibited him from looking at photographs of children.[36] Upon his arrest, his laptop and two USB memory sticks were seized. The memory sticks were encrypted but the laptop revealed indecent images of children. An application was brought under s 49 for the defendant to provide the encryption key to the memory sticks. When that application was rejected,[37] the police appealed to the High Court. McCombe J and May P heard the appeal application. In setting out the privilege's principles, McCombe J noted the distinction between evidence having an existence independent of the will of the accused and statements made by the accused as a result of compulsion. The privilege only applied to the latter form of evidence.[38] Notably, however, McCombe J followed the approach in *R v S(F)* in finding that the privilege had been engaged by the requirement

---

32 Ibid 1497 [21].

33 Ibid.

34 Ibid 1498 [24].

35 [2011] EWHC 1966 (Admin) ('*Andrews*').

36 *Andrews* [2011] EWHC 1966 (Admin), [2]. His arrest was as a result of a member of staff at the hostel he was staying at informing the police that he had been seen looking at pictures of children.

37 On the grounds that the police could not show that the respondent knew the encryption key. HHJ Steiger held that as there was no evidence that the defendant knew the encryption key, 'for the defendant to reveal what the key was, would itself be incriminating material, there being no other independent evidence to show that he does know what the key is'.

38 *Andrews* [2011] EWHC 1966 (Admin), [13].

to provide the encryption key as doing so revealed 'the fact of the defendant's knowledge of the keys'.[39]

In England and Wales, then, the position is the same as that in the United States. While the contents of the encrypted device are not themselves privileged information, the act of producing the password to that information will engage the privilege if the contents of the encrypted drive are incriminatory. Notably, the English courts recognise the incriminating testimony to be that the suspect knows the encryption key, rather than that the suspect knows what is on the encrypted drive. In that respect the approach of the English courts has more in common with the control test than it does with the contents test.

4.3.2 Alphabetic or numeric passwords in Australia

In a recent decision, the Federal Court found that the privilege is infringed by an order to produce an alphabetic or numeric password. In *Luppino (No 1)*, a compelled production order was made using the specific powers provided under s 3LA of the *Crimes Act 1914* (Cth). The order required Luppino to provide the password to his mobile phone and to applications on that phone. Luppino refused to comply with the order and commenced judicial review proceedings to have the order declared invalid. Pending the outcome of that application, the police sought two interlocutory orders: that Luppino record the relevant passwords in writing and place them in a sealed envelope to be deposited with the Australian Government Solicitor; and that Luppino file an affidavit recording his compliance with the first order.[40] The power to make the interlocutory orders was said to reside in s 23 of the *Federal Court of Australia Act 1976* (Cth), which provides that '[t]he Court has power, in relation to matters in which it has jurisdiction, to make orders of such kinds, including interlocutory orders, and to issue, or direct the issue of, writs of such kinds, as the Court thinks appropriate'.[41] This power, then, is the equivalent of that granted to courts in the United States by the *All Writs Act*. Luppino opposed the interlocutory order on the grounds that it infringed the privilege.

---

39 Ibid [16] referring to *R v S(F)* [2009] 1 WLR 1489, 1496-7 [21].

40 *Luppino (No 1)* [2018] FCA 2106, [3]-[12].

41 Ibid [18].

White J had little hesitation in refusing the interlocutory relief. At the outset his Honour noted that unlike s 3LA of the *Crimes Act*, the provision sought to be relied upon did not abrogate the privilege.[42] The result was that, with regard to the second order, it required Luppino to depose to his knowledge of the passwords, which would be 'evidence out of the plaintiff's own mouth which could be relied upon in a prosecution for an offence pursuant to s 3LA(5)'.[43] Such action was an infringement of the privilege.[44] With regard to the first order, White J held that recording those details was 'an interim step' that may lead to the disclosure of the passwords against Luppino's wishes in circumstances where their disclosure could incriminate him.[45] 'Given the fundamental nature of the common law privilege against self-incrimination', his Honour held, 'that course would be inappropriate'.[46] Notably, White J further found that it was unnecessary to determine whether that outcome was the result of the statutory provision in question lacking the requisite authority to authorise such an order or as a result of the operation of the privilege.[47]

Luppino (*No 1)* thus establishes two things. First, that an order requiring a person to depose to his or her knowledge of a password will infringe the privilege. An inevitable consequence must follow from that: if deposing to one's knowledge infringes the privilege, taking an action that demonstrates knowledge of the password – such as by performing an act of decryption – must also infringe the privilege. Notably, this finding in *Luppino* (*No 1)* is consistent with the finding by the Court of Appeal in *R v S(F)* that the privilege is infringed where a suspect is compelled to reveal a password that protects incriminating evidence.[48] Secondly, White J's decision holds that the Federal Court does not have a subpoena power to issue a compelled production order. This is a notable distinction from the position adopted in the United States; there, the *All Writs Act*

42 Ibid [22].
43 Ibid [28].
44 Ibid [27].
45 Ibid [32].
46 Ibid.
47 Ibid [33].
48 *R v S(F)* [2009] 1 WLR 1489, 1493 [12] where the Court notes that compliance with a compelled production order 'may inculpate the individual to whom the notice is addressed'.

provides that the court may issue all writs necessary to enable it to exercise its jurisdiction, thereby enabling courts to make the sort of order sought in *Luppino (No 1)*. The result is that where a compelled production order is sought outside the terms of the specific statutory provisions authorising such orders, there does not appear to be another statutory power under which such an order can be made. This decision finds support elsewhere, both with regard to the applicability of the privilege to compelled production orders and the existence of another statutory power under which a compelled production order can be made.

Support for the finding that the privilege is infringed by a compelled production order is found in both case law and Explanatory Memoranda to the statutes that enacted the compelled production provisions. When s 3LA of the *Crimes Act 1914* (Cth) – the Commonwealth provision authorising the granting of a compelled production order – was amended in 2009, it was argued in the Replacement Explanatory Memorandum to that Bill that:

> Requiring a person to provide assistance for officers to access evidence could be considered to threaten a person's privilege against self-incrimination. However, section 3LA (as it currently stands or as repealed and replaced by this item) does not impact on this privilege. The privilege against self-incrimination arises when a person is required to provide documents or things, or answer questions that would tend to incriminate themselves. This is not the case with section 3LA which only requires a person to provide information which will enable a constable to properly conduct a search of their computer or data. The officer or constable still has to conduct the search to determine if there is evidential material on the computer. The assistance order cannot require a person to assist an officer or constable to navigate through data on a computer, or to point to evidential material. The assistance order only requires the person to provide an officer or constable with the assistance that is reasonable for them to have access to the data on a computer (emphasis added).[49]

Put simply, the compelled production of an encryption key was said not to be the production of evidence, but merely the provision of information to facilitate the conducting of an authorised search. A similar argument is present in the statement of compatibility to the Crimes Amendment (Child Pornography and Other Matters) Bill 2015 (Vic) which introduced s 465AAA into the *Crimes Act 1958* (Vic), where it is said that the legislation does not infringe the privilege because 'while the information the

[49] Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009, 92.

person provides may enable police to obtain evidence that incriminates the person, the giving of that information, such as the computer password or similar, is not itself a confession of guilt'.[50]

One substantial problem with this argument looms large. While the passage from the Explanatory Memorandum to the Bill that amended the *Crimes Act 1914* (Cth) recognises that answering questions that would tend to incriminate would constitute an infringement of the privilege, it fails to address the fact that the production of an encryption key is expected to unearth incriminating evidence.[51] As the privilege extends to derivative evidence, the basis for the Explanatory Memorandum's confidence in the inapplicability of the privilege is unclear. Inadvertently, the memorandum offers support to the position that compelled production orders infringe the privilege. Furthermore, the argument in the memorandum appears to run directly counter to the decision of the High Court in *Sorby*, in which the Court said that 'the privilege protects the witness not only from incriminating himself directly under a compulsory process, but also from making a disclosure which may lead to incrimination or to the discovery of real evidence of an incriminating character'.[52] The giving of an encryption key would appear to fall squarely within that scenario.

The opinion expressed in the statement of compatibility to the Crimes Amendment (Child Pornography and Other Matters) Bill 2015 that the privilege is not implicated by the compelled production of an encryption key also has limited support. Somewhat surprisingly, the Explanatory Memorandum and statement of compatibility to the Justice Legislation Amendment (Confiscation and other Matters) Bill 2014, which introduced the earlier s 465AA into the *Crimes Act 1958*, each respectively declare that the compulsory powers 'expressly limit the right to self-incrimination'[53] and 'arguably

---

50 Victoria, *Parliamentary Debates*, Legislative Assembly, 5 August 2015, 2417 (Martin Pakula, Attorney-General). Statements of compatibility are required by s 28 of the *Victorian Charter*.

51 In the United States, it would constitute evidence falling within the scope of the act of production doctrine.

52 *Sorby* (1983) 152 CLR 281, 310 (Mason, Wilson and Dawson JJ).

53 Explanatory Memorandum, Justice Legislation Amendment (Confiscation and other Matters) Bill 2014, 31.

limits'[54] the privilege. The only apparent reason for the change in the understanding of the privilege recorded in the statements of compatibility between 2014 and 2015 is the change of government that occurred during that time.[55]

Moreover, the Victorian Scrutiny of Acts and Regulations Committee, in commenting on the operation of s 465AAA, expressed the view that 'clause 9 may engage the suspect's Charter's rights to a fair hearing, including the right against compelled self-incrimination set out in Charter s. 25(2)(k)'.[56] The Committee's conclusion was based primarily on the decision of the Victorian Supreme Court in *Major Crime*,[57] in which the Court listed evidence found on a computer that had been obtained through use of the coercive powers under the *Major Crime (Investigatory Powers) Act 2004* (Vic) as an example of derivative evidence obtained in breach of the privilege.[58]

Notwithstanding the occasional dissenting argument, the stronger argument – and the position finding the greatest support in the case law – is that compelled production orders do implicate the privilege.

The second finding in *Luppino (No 1)* – that there is no pre-existing statutory power that authorises the granting of a compelled production order – finds support in *R v Ford*.[59] The applicant in that matter was stopped and searched by police in the early morning while they were conducting foot patrols. He was found with 14 tablets hidden in his underwear and almost $400 in his possession. He also had an iPhone 5. While asking the applicant questions, the police officers asked for the PIN to unlock his phone. At the time that they made this request the applicant had not been informed of his rights. He provided the PIN and a subsequent search of the phone uncovered messages suggesting

---

54 Victoria, *Parliamentary Debates*, Legislative Council, 17 September 2014, 3096.

55 As ss 465AA and 465AAA are relevantly identical for present purposes, any differences in those provisions cannot explain the different approaches to the privilege adopted in the two statements of compatibility.

56 Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Alert Digest*, No 9 of 2015, 18 August 2015, 9. The Committee had expressed the same opinion the previous year in respect of s 465AA: Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Alert Digest*, No 13 of 2014, 14 October 2014, 15.

57 (2009) 24 VR 415.

58 Ibid 436-7 [91]-[92].

59 [2017] QSC 205.

that the applicant was involved in drug dealing.[60] At trial the applicant was successful in having the evidence found on his phone excluded on the grounds that it had been obtained in breach of his right to silence. In finding for the applicant, Flanagan J noted that the request for the PIN was made verbally by the constables after detaining and searching Ford but before informing him of his right to remain silent.[61] Critically, his Honour found, with reference to the powers under ss 154 and 154A of the *Police Powers and Responsibilities Act 2000* (Qld), that the constables were not 'exercising a power under any Act which required the applicant to give information or answer questions'.[62] As a result, it was open to Ford to lawfully refuse to provide the PIN.[63]

There was no dispute that the stop, search and arrest of the applicant constituted a lawful exercise of the police officer's powers to perform those actions. Flanagan J's finding that the constables were not exercising a statutory power to require Ford to provide an encryption key therefore means that those powers do not include the authority to require a suspect to provide the encryption key to an encrypted electronic device. In so finding this decision adopts the same line as *Luppino*, one that holds that it is only through the use of the specific statutory provisions addressing compelled production orders that a law enforcement official can compel a suspect to provide an encryption key.[64]

---

60 Ibid [6]-[9].

61 Ibid [17].

62 Ibid [25].

63 Ibid [50].

64 The ordinary search powers granted to a law enforcement official under a search warrant do not, for example, grant the power to require assistance to access encrypted data: *Police Powers and Responsibilities Act 2012* (Qld) s 157. Note, too, that the only oral information that a police officer can ordinary require of a suspect is their name and address: *Police Powers and Responsibilities Act 2012* (Qld) s 40. See also the second reading speech to the Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA), in support of the passage of the Bill, in which it was said that 'the Bill addresses the omission in current South Australian police powers as there is no general power in South Australia, unlike Queensland, Victoria, Western Australia and the Commonwealth, to compel the provision of a password': South Australia, *Parliamentary Debates*, Legislative Council, 18 October 2017, 7970-71. As the four jurisdictions identified by the second reading speech are those jurisdictions that have enacted compelled production legislation, it follows that in the absence of such legislation there is no general power to do so.

The Australian position regarding alphabetic and numeric passwords can briefly be summarised as follows. In order to obtain a compelled production order, there needs to be a statutory provision that both authorises the making of such an order and, in so doing, abrogates the privilege which would otherwise serve as a bar to the granting of such an order. Such a power does not appear to be contained in any pre-existing statutory provisions with the result that specific statutory provisions are required to address these two requirements. As will be discussed in Part 4.4, several Australian jurisdictions have enacted such legislation.

4.3.3 Decryption using biometrics in England and Wales and Australia

While the privilege is engaged by the compelled production of a numeric or alphabetic password, does the same result follow if compelled decryption is sought using a biometric feature?

To date, no English or Australian courts have considered whether the use of a fingerprint to decrypt an encrypted device infringes the privilege. Nevertheless, both jurisdictions hold that the privilege does not apply to bodily evidence. In *Saunders*, the European Court of Human Rights – in a passage cited with approval by the English Court of Appeal[65] – held that the privilege did not apply to

> material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing.[66]

In Australia, the High Court in *Sorby* endorsed this understanding of the privilege, finding it inapplicable to evidence of the condition of a person's body.[67] As discussed in Chapter 3, in the United States the privilege is also understood to be inapplicable to evidence of a person's bodily features. There, the application of that principle to compelled

---

65 *Attorney General's Reference (No 7 of 2000)* [2001] 1 WLR 1879, [58].

66 *Saunders* (1997) 23 EHRR 313, 338 [69]. See also *Jalloh* (2007) 44 EHRR 32; *MacLeon v HM Advocate* 2012 JC 293, 306 (DNA samples do not infringe the privilege); *McFadden v HM Advocate* 2010 SCL 247 (voice samples do not infringe the privilege).

67 *Sorby* (1983) 152 CLR 281, 292 (Gibbs CJ). See also *Grollo v Bates* (1994) 53 FCR 218, 250 where the Court stated that 'body, blood and breath content, and fingerprints, are not the person's creation but are objective elements of identity' and therefore not covered by the privilege.

production orders using biometrics has resulted in courts holding that the privilege does not apply to such orders. That approach finds support in English law. In *R v S(F)*, the English Court of Appeal said of encryption keys that:

> If however, as for present purposes we are assuming, they contain incriminating material, the facts of the defendants' *knowledge* of the keys may itself become an incriminating fact. For example, to know the key to a computer in your possession which contains indecent images of children may itself tend to support the prosecution case that you were knowingly in possession of such material. This was the approach adopted in In re Boucher 2007 WL 4246473 a decision of the District Court of Vermont, where the reasoning acknowledged that some 'acts of production' such as fingerprints, blood samples or voice recordings would not attract the privilege against self-incrimination.[68]

It is to be expected that Australian courts will follow the English and United States' approach to biometrics as they have adopted the same position as those courts in respect of bodily samples more generally. Breathalyser samples have been held not to infringe the privilege for reasons that include that the privilege allows a person 'a right to refuse to answer incriminating questions' but that it does not extend beyond such testimonial disclosures.[69] Similar findings have been made in respect of the taking of fingerprints[70] and the giving of a voice sample.[71] In *Sorby*, the High Court noted that a person may be required to give a fingerprint or a voice or handwriting sample.[72] While the statements in *Sorby* relate to the use of those samples for purposes of identification, the giving of such samples does not become a testimonial act falling within the scope of the privilege merely because the giving of them reveals incriminating evidence.[73]

While the privilege is not expected to be a bar to the making of such an order in Australia, any such order still needs to be authorised by statute. Is there an existing

---

68 *R v S(F)* [2009] 1 WLR 1489, 1497 [21]. The Court also spoke of how disclosing one's knowledge of the encryption key entails a 'disclosure': [25]. No such disclosure is present, however, where biometrics are used.

69 *King v McLelland* [1974] VR 773, 776.

70 *R v Carr* [1972] 1 NSWLR 608, 612 (the privilege does not apply to the taking of a fingerprint as the privilege only applies to 'answers given to questions asked'.)

71 *Bulejcik v The Queen* (1996) 185 CLR 375.

72 *Sorby* (1983) 152 CLR 281, 292 (Gibbs CJ).

73 This conclusion is consistent with the High Court's acknowledgement that real evidence is non-testimonial and therefore outside the scope of the privilege: *Bulejcik v The Queen* (1996) 185 CLR 375, 400 (Toohey and Gaudron JJ).

statutory power in Australia that authorises the making of such orders?[74] While there is no clear answer, the stronger argument is that in the absence of specific statutory provisions providing for compelled production orders using biometrics, there is not.

Consider a police officer's search powers. What warrantless search powers are granted to police officers are limited to authorising them to search a person[75] or, in respect of a personal search, to require a person to remove certain items of clothing.[76] Those powers do not appear to encompass requiring that person to assist in the search, and, notably, none of the relevant statutes contain a provision expressly requiring such assistance to be given. Where a warrant has been obtained authorising the search, the powers authorised by those warrants do not ordinarily include a power to compel a person to assist in the execution of that search.[77] That understanding is supported by the *Luppino* decision.

While some statutes give law enforcement officials the power to take a suspect's fingerprints, that power is ordinarily given only to enable a person in custody to be identified[78] or for purposes of forensic analysis.[79] There are two reasons for believing that those statutes do not provide authority to compel the use of a fingerprint to decrypt

---

74 This question arises in Australia because not all its states and territories have enacted legislation to allow for compelled production orders. In those states and territories that have not, a compelled production order involving biometrics cannot be made unless there is an existing statutory power to do so. This question does not arise in England because, as will be seen, *RIPA* allows for the making of such orders.

75 *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) ss 21-28A; *Police Offences Act 1935* (Tas) Part VII; *Criminal Code Act* 1924 (Tas) ss 26A, 27; *Summary Offences Act 1953* (SA) s 68; *Crimes Act 1900* (ACT) s 207.

76 *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) s 30(b).

77 Ibid Part 5; *Search Warrants Act 1997* (Tas) s 6; *Summary Offences Act 1953* (SA) s 67; *Crimes Act 1900* (ACT) s 195; *Police Administration Act* (NT) Part VII Division 2. Note, however, that in South Australia at least one statute could be interpreted as providing the necessary power to compel a person to unlock an electronic device with a fingerprint. Under the *Controlled Substances Act 1984* (SA), authorised officers are granted search powers that enable them to examine electronically stored documents and to 'give such directions as are reasonably necessary for, and incidental to, the effective exercise of the officer's powers under this Act': s 52(2)(c) and (j). It is arguable that this provision is broad enough to demand a person unlock an electronic device with a fingerprint.

78 *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) s 133(1).

79 *Crimes (Forensic Procedures) Act 2000* (NSW); *Forensic Procedures Act 2000* (Tas) ss 3, 12, 17; *Criminal Law (Forensic Procedures) Act 2007* (SA) s 3; *Crimes (Forensic Procedures) Act 2000* (ACT) s 5; *Police Administration Act* (NT) s 4, Part VII, Division 7.

a device. First, while the statutory power authorises the taking of a forensic sample such as a fingerprint, when a fingerprint is used to unlock an encryption device no forensic procedure takes place and no forensic sample is obtained. Secondly, in several statutes authorising the taking of forensic samples, those statutes provide that the samples are taken for the specific purpose of analysing them as part of the investigation of an offence.[80] No analysis occurs where a fingerprint is used to unlock an electronic device. To allow those provisions to be utilised to require a person to use his or her fingerprint to decrypt an encrypted device would be to use the provisions for a purpose for which they are not intended. As identified in Part 4.2, at the heart of the interpretative exercise lies the requirement that regard must be had to the purpose of a statutory provision. Where such regard is had, it is clear that the purpose of these powers does not extend to compelling decryption using a fingerprint.

The result is therefore as follows: without a specific provision providing for the making of a compelled production order using biometrics, there does not appear to be a basis on which law enforcement officials can compel decryption with a fingerprint, notwithstanding that such an act does not infringe the privilege.

4.3.4 Comparison to United States and Canada

At this stage of the analysis, points of similarity and difference with Canada and the United States are already noticeable. The United States stands alone as the sole jurisdiction to have found that, in certain circumstances, the privilege will not be engaged by a compelled production order. In each of Canada, England and Wales and Australia, the act of compelling a person to provide a password that will reveal incriminating evidence is an infringement of the privilege.

Furthermore, the mechanism by which the United States has found the privilege engaged – the act of production doctrine – appears to have been recognised by the English and Australian courts, albeit that they do not use the same terminology. Regardless of terminology, the English Court of Appeal has accepted that where the

[80] *Crimes (Forensic Procedures) Act 2000* (NSW) Part 6 Division 6; *Criminal Law (Forensic Procedures) Act 2007* (SA) Part 4; *Crimes (Forensic Procedures) Act 2000* (ACT) Division 2.6.5.

production of a password leads to incriminating evidence, the privilege will be engaged by that act.[81] Unlike the United States, however, neither the English nor the Australian case law appears to recognise an equivalent of the foregone conclusion doctrine – though such a doctrine is not necessary in light of the jurisdictions' ability to abrogate the privilege.

In several other respects, however, components of the United States' approach have been rejected in England and Wales and Australia. In England and Wales, the Court of Appeal has rejected the analogy relied upon by some courts of the United States concerning the purported difference between using a physical key to unlock a safe and using a combination to open it. In the United States, only the latter engages the privilege. In *R v S(F)*, however, it was said that the key to a computer is no different to the physical key to a drawer: both 'exist independently of the suspect'.[82]

In Australia, a key element of the United States' approach is not endorsed. While the courts of the United States have found a power to compel the production of a password in the *All Writs Act*, in *Luppino (No 1)* a similarly worded provision in Australia was found not to include the power to compel that act of production. The *Luppino* (*No 1)* decision left open whether that outcome was a result of the wording of the provision not being sufficiently broad to capture such an order or whether it was a consequence of the operation of the privilege. Given the wording of the provision, however, which allows for the making of any orders the court deems appropriate, it is hard to understand how the scope of that wording would not encompass a compelled production order. It is likely that the determinative factor was, instead, the ability of the privilege to preclude such an order being made given the failure of that provision to abrogate the privilege.

Ultimately, though, it is the ability of England and Wales and Australia to abrogate the privilege without a commensurate grant of immunity that stands as arguably the primary distinction between them and Canada and the United States. In the United States and Canada, any act of abrogation needs to be accompanied by direct and

81 *R v S(F)* [2009] 1 WLR 1489, 1498 [24].

82 Ibid 1497 [21].

derivative-use immunity, which would preclude the use of any evidence found through the compelled production order from being used against the suspect. This outcome is a result of the constitutional protection afforded to the privilege in those jurisdictions. Consequently, in Canada and the United States a compelled production order will not be granted unless the court finds that the privilege is not engaged. In Canada, no means have been identified by which such orders may fall outside the scope of the privilege; in the United States, the foregone conclusion doctrine can perform that function.

Three different outcomes have been identified between the jurisdictions. In Canada, with its strict approach to the privilege and reluctance to abrogate it, the privilege stands as a barrier past which compelled production orders cannot pass; in the United States, though the privilege receives the same constitutional protection, the foregone conclusion doctrine provides an exception to its application, a means to limit somewhat the extent of its reach; and in England and Wales and Australia, though the courts have been willing to find that the privilege is engaged by compelled production orders, that finding has been made in circumstances where the privilege has been abrogated, rendering the finding of limited significance. It is that act of abrogation that is the subject of Part 4.4.1 below. As will there be seen, what was previously a straightforward matter has been somewhat complicated in England and Wales and Victoria by the existence in those jurisdictions of human rights statutes granting a measure of protection to the privilege.

4.4 DETERMINING COMPELLED PRODUCTION ORDER APPLICATIONS UNDER THE ENGLISH AND AUSTRALIAN STATUTES

This Part considers how the English and Australian courts have determined applications for a compelled production order brought under their respective statutes. That requires, first, an analysis of how the jurisdictions in question abrogate the privilege, which occurs in Part 4.4.1. Considered in that analysis is the impact the *Human Rights Act 1998* and the *Victorian Charter* have had on the English and Victorian decisions. Thereafter, Parts 4.4.2 and 4.4.3 consider two issues that featured prominently when the courts of the United States considered compelled production orders: the form of order and its effect on the role of the privilege, and the evidentiary burdens that were

imposed on the applicant. The former of those issues is considered in Part 4.4.2, the latter in Part 4.4.3. The focus in Part 4.4.3 is on the burdens imposed in respect of the applicant's knowledge of the contents of the encrypted drive and the recipient's knowledge of the password to the encrypted data.

Before considering those issues, however, it is necessary to introduce the statutes that allow for compelled production orders. In England and Wales, Part III of *RIPA* provides for compelled production orders. In Australia, by contrast, legislation compelling the production of an encryption key exists at the federal and state levels.[83] At the federal level, s 3LA of the *Crimes Act 1914* (Cth) provides a mechanism through which access to encrypted material can be compelled. Section 3LA applies to data storage devices that are seized pursuant to a warrant issued under s 3E. Section 3E provides for the granting of a warrant where an issuing officer is satisfied that there are reasonable grounds for believing there to be 'evidentiary material' at the premises to be searched. Evidentiary material is material relevant to an offence, which means 'an offence against a law of the Commonwealth; or … a Territory; or … a State offence that has a federal aspect'.[84] Offences with a federal aspect include those involving an electronic communication,[85] which further includes any communication of information in the form of text, data or visual images.[86]

The result is a provision that captures much of the serious offending that legislation of this nature is typically understood to be directed at, such as terrorism offences, drug trafficking offences and, where the material is distributed electronically, child pornography offences. However, less serious state offences, such as possession of child

---

83 There are several other federal and state statutory provisions granting law enforcement the power to apply for compelled production orders. As the purpose of this thesis is to consider, amongst other things, whether in principle a compelled production order can be made, there is no need to consider each of those statutes. It is enough to consider the principal statute under which compelled production orders will ordinarily be made. Provisions not considered in this Chapter but which provide for compelled production orders include: *Competition and Consumer Act 2010* (Cth) s 154RA; C*ustoms Act 1901* (Cth) s 201A; *Proceeds of Crime Act 2002* (Cth) s 246; *Telecommunications Act 1997* (Cth) s 547J; *Criminal Assets Confiscation Act 2005* (SA); *Fair Trading Act 2010* (WA) s 75(1).

84 *Crimes Act 1914* (Cth) s 3C.

85 Ibid s 3AA(3)(e).

86 Ibid s 3AA(5).

pornography, fall outside the scope of this provision. As a result, several states have implemented their own legislation compelling the production of an encryption key in respect of offending under state laws. In Queensland, ss 154 and 154A of the *Police Powers and Responsibilities Act 2000* (Qld) provide for compelled production orders, the former provision applying where an order is sought concomitantly with the application for a search warrant, the latter when the application is brought after a search warrant has been executed and an electronic device seized. Victoria adopts the same approach, with s 465AA of the *Crimes Act 1958* (Vic) governing the situation where a compelled production order is sought after an electronic device has been seized pursuant to a search warrant, and s 465AAA providing for a compelled production order to be included in a search warrant.[87] In Western Australia, s 59 of the *Criminal Investigation Act 2006* (WA) provides for the issuing of a data access order that can require a person to provide an encryption key. Lastly, in July 2019, South Australia passed the *Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019* (SA). It allows a magistrate to issue a compelled production order where there are reasonable grounds for believing data evidencing the commission of a serious offence is on an encrypted electronic device. As this statute was only enacted during the final stages of this thesis, it will only be considered where it raises an issue not considered under the other Australian statutes.

4.4.1 The abrogation of the privilege

A central feature of the English and Australian statutes is the abrogation of the privilege. As discussed in Part 4.3 above, in both jurisdictions producing a password (other than a biometric one) that reveals incriminating evidence will infringe the privilege. Any statute that purports to authorise compelled production orders must, therefore, first abrogate the privilege. This Part examines how that abrogation occurs. That examination takes place in three parts: Part 4.4.1.1 considers abrogation in those Australian jurisdictions that do not have a human rights statute; Part 4.4.1.2 examines the Victorian approach and the role performed by the *Victorian Charter*; and finally Part 4.4.1.3 analyses abrogation in England and Wales where the *Human Rights Act 1998* protects the privilege in Article 6.

[87] Both provisions, as becomes evident in the sections that follow, are materially identical.

4.4.1.1 Abrogation in jurisdictions without a human rights statute

Of the Australian jurisdictions without a human rights statute, Western Australian expressly abrogates the privilege by providing that the privilege cannot be relied upon to refuse to answer a disclosure notice.[88] Furthermore, it does so without giving any express immunity in exchange for that compliance.[89]

By contrast, at the federal level the *Crimes Act 1914* (Cth) does not expressly abrogate the privilege. That does not preclude the possibility, however, that the privilege has been abrogated by necessary implication.[90] The High Court has previously held that 'the privilege will be impliedly excluded if the obligation to answer, provide information or produce documents is expressed in general terms and it appears from the character and purpose of the provision that the obligation was not intended to be subject to any qualification'.[91] It is, therefore, a question of what purpose the statute seeks to achieve. If that purpose can only be achieved through the abrogation of the privilege, that act of abrogation will be implied. Such is likely to be the case with s 3LA. In *Loges v Martin*, in considering whether the privilege was infringed by a statutory obligation imposed on the registered owner of a motor vehicle to answer a question by a law enforcement official about who was driving the vehicle at a specified time, the Supreme Court of Victoria held that 'a purpose of this Act is to ensure the safe use of roadways. The law compels the conclusion that the identity of the drivers of registered vehicles be made available to law enforcement officers. The privilege to decline to answer has necessarily

---

88 *Criminal Investigation Act 2006* (WA) s 61(3). The recent *Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019* (SA) s 74BW(2) also abrogates the privilege.

89 No implied immunity has, to date, been identified in any of the cases involving the issuing of, or compliance with, a disclosure notice. See also *Sumption v Grant* [2013] WASC 258, [38] where the Court notes that the privilege is not a defence to a data access order.

90 The apparent reason for not including such a clause appears to be found in the Replacement Explanatory Memorandum to the 2009 amendments to the provision, in which it is said that 'section 3LA (as it currently stands or as repealed or replaced by this item) does not impact on the privilege': Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009, 92. Obviously, if the drafters' understanding was that the provision did not implicate the privilege, there would have been no need to abrogate that same privilege.

91 *Pyneboard Pty Ltd v Trade Practices Commission* (1983) 152 CLR 328, 341 (per Mason ACJ, Wilson and Dawes JJ concurring). See also *Loges v Martin* (1991) 13 MVR 405; *R v Hooper* (1995) 64 SASR 480.

been extinguished'.[92] In a similar manner, the sole purpose of s 3LA is to obtain the encryption key or other access information to encrypted electronic data so as to allow law enforcement officials to investigate criminal activity. To allow a person to refuse to provide that encryption key on the grounds that it would infringe the privilege would entirely defeat the purpose of the provision. Necessarily, therefore, the privilege must have been abrogated by s 3LA.

It is to be noted, however, that while there is no restriction on parliament's ability to abrogate the privilege through statute, such abrogation is ordinarily not undertaken lightly. The cases examined in Chapter 2 reveal the use of a balancing exercise to justify acts of abrogation. For example, in respect of motor vehicle reporting obligations, the extent of the infringement of the privilege and the public interest were both considered as part of the analysis of whether the privilege had been abrogated.[93] The reference to those factors demonstrates an understanding that while rights such as the privilege may be statutorily abrogated, such abrogation does not occur lightly and only where to do so is reasonable. That the Federal parliament argued in the Explanatory Memorandum to the 2009 amendments to s 3LA that compelled production orders do not infringe the privilege further reflects this caution in abrogating the privilege. To surmount that cautious approach, a balancing exercise may be used to demonstrate the reasonableness of the act of abrogation. This use of a balancing exercise may play a heightened role in Victoria, where the existence of the *Victorian Charter* argues for greater weight to be placed on interests of the individual.

At the federal level and in Western Australia, the statutory abrogation of the privilege is clear and compliant with common law requirements. In England and Wales, Victoria and Queensland, however, that picture is potentially complicated by the existence of human rights statutes in those jurisdictions. Victoria and Queensland are considered next.

4.4.1.2 Abrogation of the privilege in Victoria

92 *Loges v Martin* (1991) 13 MVR 405, 409,

93 *R v Hooper* (1995) 64 SASR 480, 486.

Victoria and Queensland are the only enacting jurisdictions in Australia with human rights statutes. The Queensland Act – the *Human Rights Act 2019* (Qld) – has not, however, fully commenced operation. There is, therefore, no case law interpreting its provisions. Moreover, its provisions are, for present purposes, broadly similar to those in the *Victorian Charter*. In particular, both protect the privilege and both contain broadly similar limitations clauses. As, therefore, any interpretation of the Queensland legislation will be influenced by how courts have interpreted the Victorian legislation, this Part will only consider the Victorian statute and how courts have interpreted its provisions.

The *Victorian Charter* provides, in s 25(2)(k), that a person charged with a criminal offence has the right 'not to be compelled to testify against himself or herself or to confess guilt'.[94] As already identified in Part 4.3, compelled production orders will, absent an act of abrogation, infringe the privilege. However, s 7 of the *Victorian Charter* provides that any of the rights in the *Charter* may be limited where it is reasonable to do so taking into account the factors identified in that provision.[95] Importantly, if a limitation is found to be unreasonable, that finding does not have the effect of invalidating the provision in question. Instead, the court is limited to issuing a declaration of inconsistent interpretation.

The question thus arises whether ss 465AA and 465AAA of the *Crimes Act 1958* (Vic), which expressly abrogate the privilege with no compensatory grant of direct or derivative-use immunity, comply with s 7 of the *Victorian Charter*. As identified in Part 4.2, s 32 of the *Victorian Charter* requires that all its provisions are, as far as it is possible to do so, to be interpreted in a manner consistent with that provision's purpose and in

---

94 The comparable provision in the *Human Rights Act 2004* (ACT) is s 22(2)(i).

95 Section 7(2) provides that:

> A human right may be subject under law only to such reasonable limits as can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom, taking into account all relevant factors including:
> (a) the nature of the right; and
> (b) the importance of the purpose of the limitation; and
> (c) the nature and extent of the limitation; and
> (d) the relationship between the limitation and its purpose; and
> (e) any less restrictive means reasonably available to achieve the purpose that the limitation seeks to achieve.

a way that is compatible with human rights. That obligation, however, does not impose any obligations beyond the established rules of interpretation.[96] Thus the question of whether the infringement of s 25(2)(k) of the *Victorian Charter* that is caused by ss 465AA and 465AAA complies with the limitation clause in s 7 of the *Victorian Charter* is to be determined using existing common law presumptions. Though there are no cases dealing with ss 465AA and 465AAA to aid the understanding of those provisions, their statements of compatibility offer some guidance,[97] as does the decision in *Major Crime*.[98]

The statements of compatibility for the Crimes Amendment (Child Pornography and Other Matters) Bill 2015 (Vic), which introduced s 465AAA, and the Justice Legislation Amendment (Confiscation and other Matters) Bill 2014 (Vic), which introduced s 465AA, argue that even if those provisions infringe the privilege, such infringement is 'reasonable and justified'.[99] In those statements of compatibility, the Attorney-General expressed the government's view that just as a police officer can break into and search a locked cupboard containing child pornography, so the police should be able to search electronic information that has been 'locked' by encryption. A person 'should not, simply because of their use of more sophisticated technology, now be empowered to stymie police investigations by refusing to divulge the electronic key to that evidence'.[100] Furthermore, the Attorney-General stated that information revealed through the use of that encryption key might enable the police to identify and help children that are subject to abuse. Importantly, too, the crimes being investigated are of a serious nature,[101] and the procedure to obtain a compelled production order is subject to judicial oversight.[102]

---

96 *Momcilovic v The Queen* [2011] 245 CLR 1, 50 [50] (French CJ). See also Sanson, above n 21, 279 where the author argues that the High Court found that 's 32(1) applies in the same way as the principle of legality, just with a wider field of application'.

97 Statements of compatibility are required by s 28 of the *Victorian Charter*.

98 (2009) 24 VR 415.

99 Victoria, *Parliamentary Debates*, Legislative Assembly, 5 August 2015, 2417 (Martin Pakula, Attorney-General).

100 Ibid.

101 Victoria, *Parliamentary Debates*, Legislative Council, 17 September 2014, 3096.

102 Victoria, *Parliamentary Debates*, Legislative Assembly, 5 August 2015, 2417 (Martin Pakula, Attorney-General).

All of those factors are relevant to a s 7 analysis. The privilege, though a 'right deeply engrained in the common law',[103] is one that can, and often is, abrogated by statute where necessary. In the case of an encryption key, the purpose of the limitation is to ensure that evidence that is otherwise unreadable by law enforcement officials is rendered readable. That limitation of the privilege is of considerable importance as without its abrogation there may be no other means of viewing the evidence protected by the encryption program. While those factors argue for the reasonableness of the limitation, the extent of the limitation is substantial as it may result in a suspect being compelled to provide evidence that incriminates him or her. However, there may not be any less restrictive means of obtaining the material in an unencrypted form that would still allow the provisions to achieve their intended purpose.[104] While the evidence of a person's knowledge of the encryption key could be protected by a direct-use immunity which would not undermine the purpose of the legislation, such an immunity would provide no relief for a suspect as knowledge of the encryption key is not itself ordinarily incriminating. Rather, it is the contents of the encrypted drive that may be incriminating, and they are not protected by a direct-use immunity. Though a derivative-use immunity would protect those contents, it is likely to also fatally undermine the purpose of the provisions.

The s 7 analysis performed by the Victorian Supreme Court in *Major Crime* provides further guidance to whether a court may find the limitation imposed by a compelled production order to be reasonable. The case concerned s 39 of the *Major Crime (Investigative Powers) Act 2004* (Vic), which gives a judge the power to issue a coercive powers order requiring a person to attend an investigation to answers questions. The abrogation of the privilege required by that provision is accompanied by a direct-use immunity, but not a derivative-use one. The Court, after considering the s 7 factors, read a derivative-use immunity into the provision on the grounds that such immunity was required under s 25(2)(k) of the *Victorian Charter*.[105]

---

103 *Sorby* (1983) 152 CLR 281, 309 (Mason, Wilson and Dawson JJ); *Reid v Howard* (1995) 184 CLR 1, 5 (Deane J), 11 (Toohey, Gaudron, McHugh and Gummow JJ).

104 Note that this issue of a less intrusive alternative is discussed further in Chapter 5.

105 The legislature subsequently amended the legislation to remove the derivative-use immunity that had been read in by the Court.

At the outset of her s 7 analysis, Warren CJ noted that the Court was required to balance the competing interests of society in investigating and prosecuting offending, and of the individual in ensuring he or she receives a fair trial. The standard of proof required to be met to satisfy a court that a limitation is reasonable is high.[106] With regard to the nature of the right, Warren CJ found the privilege and the right to a fair trial to be 'fundamental to the criminal justice system'.[107] The extent of the limitation was also found to be substantial, not least because derivative evidence – the use of which was permissible under the legislation – could be 'as damaging as the original, self-incriminating information'.[108] Allowing its use could 'provide a 'back-door' to prosecuting authorities to use compelled incriminating testimony against the testifier'.[109] Despite those findings, Warren CJ accepted that the offences targeted by the legislation were 'serious and significantly detrimental to society', and that the abrogation of the privilege 'better enable[d] the investigation of such offences'.[110] Her Honour also found that the purpose of the limitation was 'important enough to lead to such limitation', and that 'the limitation was rationally and purposively connected to its purpose'.[111]

It was to be the final element, the need for the limitation to adopt the least restrictive means appropriate, that Warren CJ found to be determinative in holding that the infringement of the privilege did not satisfy s 7 of the *Victorian Charter*. Her Honour found that when investigating organised crime, it was possible to identify two separate groups: those intended to be charged, and those intended to be questioned. By giving careful consideration to which of the groups the suspects fell into, it was possible to compel certain suspects to provide evidence to be used against the other suspects.[112]

---

106 *Major Crime* (2009) 24 VR 415, 448 [177].

107 Ibid 448 [146]. Note, though, that in England it is recognised that a breach of the privilege does not automatically render a trial unfair.

108 Ibid 435 [84]. Note, though, that a password itself is not ordinarily incriminating.

109 Ibid 437 [95].

110 Ibid 449-50 [151]. Tellingly, however, Warren CJ noted that the prosecution failed to properly inform the Court how the coercive powers facilitated that investigation.

111 Ibid 450 [153].

112 Ibid 450 [155].

Through the use of that approach, the rights afforded by the privilege could be protected while the aims of the legislation could still be met.[113]

It is arguable that legislation compelling the production of an encryption key has the same factors in its favour identified by Warren CJ in *Major Crime* without suffering the most significant disadvantage. Both sets of legislation target serious criminal conduct in a manner that rationally connects the limitation to the purpose of the legislation. There is also a strong public interest in providing law enforcement officials with the powers set out in the respective statutes. A shared difficulty with the statutes, however, is that they both substantially limit a long-established common law right. Importantly, however, none of those features were decisive in *Major Crime*. Rather, it was Warren CJ's finding that there were less restrictive means available to pursue the goals of the legislation that led to the finding that the limitation infringed the *Victorian Charter*.

Tellingly, there do not appear to be less restrictive means by which the encrypted material can otherwise be obtained while still enabling legislation compelling the production of an encryption key to retain its effectiveness. Organised crime is by definition criminal conduct involving more than one person.[114] There is, therefore, always at least one other offender who can be prosecuted with the information obtained from the first offender. Such is not always the case with other forms of offending; and may rarely be the case where the offending involves possession of child pornography, a common target of laws compelling the production of an encryption key. Where what is found on a computer are unlawful images and nothing more, the inability to use that evidence against the possessor of those images would preclude the prosecution of that person in circumstances where there is unlikely to be anyone else who can be prosecuted.[115] The United States' case law is replete with cases in which (as far as can be discerned from the facts of the case) the encrypted evidence was only

113 Ibid 451 [156].

114 *Major Crime (Investigative Powers) Act 2004* (Vic), s 3AA(1)(b).

115 Other forms of offending sought to be prosecuted through compelled production legislation – such as terrorism offences and drug trafficking – do not necessarily suffer from this same feature.

relevant to a prosecution against the possessor of the electronic device.[116] There being no less restrictive means by which law enforcement can obtain in plaintext the data that has been encrypted and for which law enforcement does not know the encryption key, it is likely that a s 7 *Victorian Charter* analysis performed on ss 465AA and 465AAA of the *Crimes Act 1958* (Vic) may yield an outcome different to that reached in *Major Crime*.

In a post-script to *Major Crime*, the Parliament of Victoria subsequently amended the *Major Crime (Investigative Powers) Act 2004* (Vic) to remove the derivative-use immunity. In the statement of compatibility for the Criminal Organisations Control and Other Acts Amendment Bill 2014, which amended s 39, it is stated that by granting direct use immunity, 'the central aspect of the privilege against self-incrimination is protected'.[117] Any move to extend that protection to derivative use evidence, however, 'significantly undermines the effectiveness of the coercive powers scheme' and 'effectively immunise[s]' the person who provides the evidence.[118] The statement also notes that the compulsory powers do not give rise to concerns about unreliable evidence as a result of improper questioning, and that there is no less restrictive means of obtaining the evidence without severely undermining the purpose of the legislation.[119] All of these arguments are applicable to the compelled production of an encryption key.

On balance, then, the factors identified in the statements of compatibility and other passages above for limiting the privilege are likely to be accepted by a Victorian court as sufficient for purposes of s 7 of the Charter. In particular: allowing a person to hide behind encryption would afford that person a level of protection not afforded to other forms of evidence; without the ability to compel the production of an encryption key investigations will be impeded in increasing numbers as the use of encryption grows; for

---

116 See, eg, *Boucher II* (D Vt, No 2:06-mj-91, 19 February 2009); *Apple Mac Pro* 851 F 3d 238 (3rd Cir, 2017); *United States v Gavegnano* 305 Fed Appx 954 (4th Cir, 2009); *State v Stahl* 206 So 3d 124 (Fla Ct App, 2016).

117 Victoria, *Parliamentary Debates*, Legislative Assembly, 26 June 2014, 2382 (Robert Clark, Attorney-General). The term 'central aspect' bears more than a passing relation to the 'essence of the privilege' that is spoken of in England and Europe.

118 Ibid.

119 Ibid.

some offending, the information may help to identify other perpetrators; there is no risk of unreliable evidence arising from the production of the encryption key; there are no less restrictive means to obtain the evidence in question; and the legislation has appropriate safeguards, including judicial oversight. Furthermore, even if a court found the legislation to infringe s 7, the legislature's response to the decision in *Major Crime* suggests that it would be undeterred by such a finding.

4.4.1.3 Abrogation of the privilege in England and Wales

Although *RIPA* fails to expressly address the issue of abrogation, that it has that effect has been confirmed by the courts. The leading decision on this issue is *R v S(F)*,[120] a decision of the Court of Appeal. The defendants were alleged to be party to a conspiracy to breach a control order made in respect of H, which required him to remain at his home address. In breach of that order, S collected H from his home and took him to a new address. Shortly after arriving at the new address the police entered the premises and found S alone in a room with a computer on which an encryption key had been partially entered. Following the arrest of S, his home was searched and computer material retrieved from his computer's hard drive. However, the files on the computer were encrypted and could not be accessed. On the same day that S was arrested, A was also arrested and computer material seized, though parts of it too were inaccessible as a result of an encryption program.[121] To obtain access to the encrypted data, s 49 disclosure notices were served on the defendants requiring them to produce the encryption keys. Both S and A refused to comply with the notices on the basis that they were incompatible with the privilege against self-incrimination.

To the question of the impact that the legislation would have on the privilege, the Court, per Lord Judge CJ, noted that the privilege was not an absolute right. Referring to the decision of the House of Lords in *R v Director of Serious Fraud Office, Ex parte Smith*,[122] his Lordship noted that some curtailment of the privilege was necessary and accepted

120 [2009] 1 WLR 1489.

121 *R v S(F)* [2009] 1 WLR 1489, 1491-2 [2]–[4]. The judgment does not explain the relationship between A and S, or why A was arrested and computer material seized.

122 [1993] AC 1.

as being 'indispensable to the stability of society'.[123] The privilege was, accordingly, subject to 'numerous statutory exceptions which limit, amend or abrogate [it] in specified circumstances' provided that limitation did not compromise the fairness of the trial under Article 6 of the *ECHR*.[124] To ensure compatibility with Article 6, the limitation needed to be 'reasonably directed by national authorities towards a clear and proper public objective and if representing no greater qualification than the situation calls for'.[125]

After finding that a requirement to provide an encryption key implicated the privilege where the data discovered using that encryption key was incriminating,[126] his Lordship stated that the determinative question was whether any interference with the privilege imposed by a disclosure notice was 'proportionate and permissible'.[127] In an extended passage, Lord Judge CJ identified the key facts of the matter as follows:

> A number of issues are clear and stark. The material which really matters is lawfully in the hands of the police. Without the key it is unreadable. That is all. The process of making it readable should not alter it other than putting it into an unencrypted and intelligible form that it was in prior to encryption; the material in the possession of the police will simply be revealed for what it is. To enable the otherwise unreadable to be read is a legitimate objective which deals with a recognised problem of encryption. The key or password is, as we have explained, a fact. It does not constitute an admission of guilt. Only knowledge of it may be incriminating. The purpose of the statute is to regulate the use of encrypted material, and to impose limitations on the circumstances in which it may be used. The requirement for information is based on the interests of national security and the prevention and detection of crime, and is expressly subject to a proportionality test and judicial oversight. In the end the requirement to disclose extends no further than the provision of the key or password or access to the information. No further questions arise. The notice is in very simple form. Procedural safeguards and limitations on the circumstances in which this notice may be served are addressed in a comprehensive structure, and in relation to any subsequent trial, the powers under s.78 of the 1984 Act to exclude evidence in relation, first, to the underlying material, second, the key or means of access to it, and third, an individual

123 *R v S(F)* [2009] 1 WLR 1489, 1494-5 [17] citing *R v Director of Serious Fraud Office, Ex parte Smith* [1993] AC 1.

124 *R v S(F)* [2009] 1 WLR 1489, 1494-5 [17].

125 Ibid. His Lordship proceeded to quote a passage from Lord Bingham in *Brown* [2003] 1 AC 681 in which Lord Bingham held that the limitation of the privilege and other rights protected under Article 6 'is acceptable if reasonably directed by national authorities towards a clear and proper public objective and if representing no greater qualification than the situation calls for'.

126 *R v S(F)* [2009] 1 WLR 1489, 1498 [24].

127 Ibid 1498 [25].

> defendant's knowledge of the key or means of access, remain. Neither the process, nor any subsequent trial can realistically be stigmatised as unfair.[128]

Article 6 did not, therefore, preclude the abrogation of the privilege provided that act of abrogation was proportionate and reasonable – requirements that *RIPA* satisfied. Importantly, however, Lord Judge CJ further noted that if that abrogation affected the right to a fair trial under Article 6, any evidence found as a result of the compelled production order could be excluded from trial through s 78 of *PACE*.[129]

In so holding, Lord Judge CJ drew from a large body of jurisprudence. In *Brown*, a case in which the owner of a motor vehicle that had been involved in an accident was required to state who the driver of the vehicle was at the time of the accident, the Privy Council found that the limitation of the privilege was proportionate and that there had, accordingly, been no infringement of Article 6. The privilege, Lord Bingham held, could be subject to limited qualification where there was a 'proper public objective' for that limitation and the limitation was proportionate.[130] The approach identified in *Brown* subsequently gained acceptance in the European Court of Human Rights: in *Jalloh*, the European Court of Human Rights accepted that the privilege could be limited provided the 'essence' of the privilege remained intact;[131] and in *O'Halloran and Francis* a requirement on the owner of a motor vehicle to identify who had been driving the vehicle at the time that it was caught speeding was found not to breach the essence of the privilege, with the result that the right to a fair trial had not been breached.[132]

The role of s 78 in ensuring the fairness of the trial was reiterated by the Supreme Court in *Beghal*.[133] The case concerned the use of powers granted to nominated officers to compulsorily question a person under the *Terrorism Act 2000*. Beghal, on returning to

---

128 Ibid. This passage was cited with approval by McCombe J in *Andrews* [2011] EWHC 1966 (Admin), [16].

129 Section 78 of *PACE* requires the exclusion of evidence where 'the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it'.

130 *Brown* [2003] 1 AC 681, 704-5.

131 *Jalloh* (2007) 44 EHRR 32, [97].

132 *O'Halloran and Francis* (2008) 46 EHRR 21, [62]-[63]. For a fuller discussion of those cases and the development of the law in this area, see the discussion in Part 1.3.2.

133 [2016] AC 88.

the United Kingdom from France, was stopped and questioned under those powers.[134] She refused to answer the questions on the grounds that to do so would infringe the privilege. In finding that the privilege was not intended to apply to the compulsory questioning powers, Lord Hughes, delivering the leading judgment of the Court, stated that the risk of prosecution was low, that allowing the use of the privilege would render the powers provided by the Act 'very largely nugatory' and that s 78 would exclude from trial any evidence derived from the answers given by Beghal.[135] It is Lord Hughes' comments on the role of s 78 that are presently relevant. In particular, his Lordship held that the application of s 78 to the evidence provided under the compulsory questioning powers 'is effectively inevitable'.[136] Lord Hughes went on to note that

> once article 6, directly binding on a court under s 6(3) of the Human Rights Act 1998, is brought into the equation, there is simply no room for any contrary conclusion, for…article 6 has the effect that any use in a criminal prosecution of answers obtained under compulsion of law will be a breach of the right to a fair trial.[137]

What do Lord Hughes' comments mean for evidence obtained through a disclosure notice issued under s 49 of *RIPA*? It is unlikely that *Beghal* automatically requires the exclusion of any evidence obtained through the use of the compulsory disclosure powers. Notwithstanding the firm line apparently drawn by *Beghal*, both the Supreme Court and the European Court of Human Rights have accepted that trial fairness is only implicated if the essence of the privilege has been destroyed. There is no discussion of this element in *Beghal*, and consequently no evidence that *Beghal* intended to overturn that line of authority. Indeed, on closer examination there is nothing inconsistent between *Beghal* and existing authority including *Brown*, *Jalloh* and *O'Halloran and Francis*. This is so because if one asks whether the essence of the privilege had been extinguished by the questioning in *Beghal*, the only answer that could have been given was that it had been as the evidence showed that Beghal was subject to more than a dozen broad questions without legal representation.[138] It is likely that the unequivocal

---

134 Beghal was questioned for approximately half an hour and asked more than a dozen questions: *Beghal* [2013] EWHC 2573 (Admin), [10].

135 *Beghal* [2016] AC 88, 118-9 [64]-[65].

136 Ibid 119 [66]. Lord Hughes further noted that because s 78 would inevitably be used, there was no appreciable risk that by answering the questions Beghal was exposing herself to the risk of self-incrimination.

137 Ibid.

138 See *Beghal* [2013] EWHC 2573 (Admin), [10] where some of those questions are listed.

response given by Lord Hughes to the future use of information obtained through the compulsory questioning powers was not the introduction of a new, more stringent test concerning the role of the privilege, but rather the application of existing doctrine to facts that could only give rise to one conclusion.[139]

The question that remains unresolved, however, is whether the giving of an encryption key in response to a s 49 notice constitutes the destruction of the essence of the privilege. The Court of Appeal in *R v S(F)* did not resolve this issue, instead merely noting that it would be for the trial judge to decide whether to exclude any evidence – be it direct, derivative or both – obtained from the s 49 notice.[140] While the decision of Lord Hughes in *Beghal* may suggest that the use of evidence obtained through a s 49 notice will render a trial unfair, the stronger argument is that it does not have that effect. A s 49 notice has a far more limited scope than that which existed in *Beghal*, being restricted to the asking of a solitary question the answer to which is not in itself incriminating, though it may lead to incriminating evidence. In this respect, a s 49 notice bears a closer relationship to the circumstances that arose in *O'Halloran and Francis* than they do to the *Beghal* facts. As with the requirement to state who was driving a motor vehicle at the time it was involved in a traffic infringement, the encryption key on its own cannot result in a conviction for an offence; there is no risk that the evidence given under a s 49 notice will be unreliable; the legislation only provides for the asking of a solitary question; and there is a strong public interest in ensuring that law enforcement have access to potentially incriminating evidence that is stored in an encrypted state.[141] In *Brown* Lord Bingham reached a similar conclusion, holding that the fact that the answer given by the suspect was in itself not incriminating, and that the legislation only allowed

---

139 See also Andrew L-T Choo, *The Privilege against Self-Incrimination and Criminal Justice* (Hart Publishing, 2013), 115-116 where the author argues that English courts have not adopted the view that the admission of evidence obtained as a result of the abrogation of the privilege automatically renders the trial unfair. Instead, whether the evidence is to be excluded is determined following the use of a balancing exercise between the rights of the accused and those of society in having the information made available at trial

140 *R v S(F)* [2009] 1 WLR 1489, 1498 [25].

141 *O'Halloran and Francis* (2008) 46 EHRR 21, [52]-[53], [57]-[60].

for the asking of a solitary question, were both relevant factors in finding that the use of that answer at trial did not render the trial unfair.[142]

In summary, it is uncontentious that *RIPA* abrogates the privilege in respect of compelled production orders, an outcome that has not been altered by the existence of the *Human Rights Act 1998*. That is not the end of the issue, however, as the protection afforded to the privilege by Article 6 prohibits any limitation imposed on the privilege by its abrogation from destroying the essence of the privilege. To date no court decision has found that compelled production orders under *RIPA* destroy the essence of the privilege, a result that accords with how the privilege has previously been treated in related orders. Thus, while the existence of Article 6 imposes challenges on the use of *RIPA*, those challenges have not been found to be insurmountable. A similar outcome was identified in Victoria, the other jurisdiction with a human rights statute.

In all English and Australian jurisdictions, then, the statutory provisions that provide for compelled production orders have also abrogated the privilege. With that preliminary issue addressed, Part 4.4.2 considers other aspects of how the provisions operate, including what they require in respect of the form of orders sought as well as the evidentiary burdens they impose. It starts with an assessment of the form of compliance that may be required by a compelled production order.

4.4.2 Forms of order

It was seen in Chapter 3 when examining the United States that the form the order takes affects how and whether the privilege is engaged by a compelled production order. In particular, where the order seeks the act of decryption or the production of the decrypted documents the privilege is engaged through the act of production doctrine, which opens up the possibility that the foregone conclusion doctrine may be enlivened. Furthermore, where the form of the order requires decryption through biometrics, the privilege is not engaged. In Part 4.3 it was shown that in Australia and England and

142 *Brown* [2003] 1 AC 681, 705 (Lord Bingham). Notably, however, a further factor relied on by Lord Bingham was that the consequences of non-compliance were 'non-custodial'. Such is not the case, however, with a s 49 notice.

Wales, too, decryption using biometrics does not engage the privilege. What though of the difference between orders requiring production of the password, the act of decryption or production of the unencrypted documents? The answer to that question depends on whether each of those forms of order are provided for under the respective statutes. If those orders fall within the scope of the legislation the privilege will be inapplicable to them as a result of the abrogation of the privilege; if they do not, there will be no alternative mechanism through which to compel the particular form of order without infringing the privilege.

In England and Wales, a disclosure notice 'must set out the disclosure that is required by the notice and the form and manner in which it is to be made'.[143] Where a suspect possesses 'both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form', that person can use the key to obtain access to the material or to put it in an intelligible form before disclosing it in an intelligible form.[144] The recipient of a disclosure notice can also comply with the obligation to produce the information in an intelligible form by disclosing the encryption key.[145] The wording of that provision is tolerably clear: compliance can occur by providing the encryption key, performing the act of decryption or producing the unencrypted documents.[146] Regardless of the form of compliance, the privilege is not engaged under *RIPA*.

In Australia, the Commonwealth and Victorian statutory provisions provide that a magistrate may order a person to 'provide any information or assistance that is reasonable and necessary to allow a constable to'[147] access data or to convert it into a

---

143 *RIPA* s 49(4)(g). Disclosure notice is the term *RIPA* uses for what this thesis has termed a compelled production order.

144 Ibid s 50(1).

145 Ibid s 50(2).

146 Note though that it is ordinarily the decision of the recipient of the notice as to how to comply with the order. In the event that the applicant wishes to have the encryption key produced, he or she will need to comply with additional evidentiary burdens that include demonstrating a belief that such an order is necessary to prevent the purpose of the disclosure notice being defeated: *RIPA* s 51(4).

147 Near identical wording is found in the *Criminal Investigation Act 2006* (WA) s 59(2)(d), where it states that a data access order must contain 'an order that the person provide information or

form intelligible to the constable.[148] At first blush, that wording includes ordering the specified person to perform the act of decryption him- or herself. This possibility, though, appears to be rejected by the Explanatory Memorandum to the *Crimes Act 1914* (Cth), in which it is stated that the section does not infringe the privilege as the privilege only

> arises when a person is required to provide documents or things, or answer questions that would tend to incriminate themselves. This is not the case with section 3LA which only requires a person to provide information which will enable a constable to properly conduct a search of their computer or data (emphasis added).[149]

Whether those statements in the Explanatory Memorandum accurately reflect the terms of the provision is, however, debateable. If the powers provided are limited to compelling a specified person to provide information that would allow a constable to access or convert encrypted data, there would be no need to refer to an obligation to provide assistance. There is an interpretative presumption that all words in a statute have a particular meaning and that none are superfluous.[150] Applying that presumption, the words 'providing assistance' must mean more than simply 'providing information'. For if assistance is given the same meaning as information then its role is otiose and a contravention of the presumption That being so, the use of the words 'or assistance' strongly suggests that the assistance it envisages is something other than simply the provision of information, and that the specified person may be required to decrypt any encrypted data. The same outcome arises under the *Police Powers and Responsibilities Act 2000* (Qld), which provides that an issuing magistrate may order the recipient of the disclosure notice to 'give a police officer access to the storage device and the access information'. Since a separate obligation to give the access information would be redundant if an obligation to give access to the device could be satisfied by providing the encryption key (or other relevant information), the obligation to give access to the

---

assistance that is reasonable and necessary to allow the applicant to' gain access to, copy or reproduce the data on the data storage device.

148 *Crimes Act 1914* (Cth) s 3LA(1)(a) and (c); *Crimes Act 1958* (Vic) ss 465AAA(2) and 465AA(2) and (3). The *Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019* (SA) adopts similar wording: s 74BR(1).

149 Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009, 92.

150 See, eg, *Project Blue Sky Inc v Australian Broadcasting Authority* (1998) 194 CLR 355, 382 [71].

storage device must mean something other than producing the encryption key. That something other can only be entering the encryption key into the device him- or herself.

While both England and Wales and the Australian jurisdictions recognise that there are different methods by which access to the encrypted documents can be obtained, the manner in which a suspect is required to comply with a compelled production order has no bearing on whether the order will infringe the privilege. In this respect the statutory responses in England and Wales and Australia contrast sharply with the case-based development that has occurred in the United States, where the form of the order does affect the applicability of the privilege.[151] Given the criticisms that have been made regarding the position in the United States and the fact that the form of the order may determine whether the privilege is implicated, the English and Australian position is to be preferred.

4.4.3 Evidence required to be satisfied before an order is made

Chapter 3 revealed that two evidentiary burdens lie at the heart of the decisions of the courts of the United States when confronted with an application for a compelled production order. First, could the applicant establish that the suspect knew the password to the encrypted device; and, secondly, was the applicant required to establish that it knew with reasonable particularity what was contained on the encrypted drive? Whether this latter burden arose depended on which of two competing tests the court adopted. Under the contents test, that element needed to be satisfied; under the control test, it did not arise. This Part considers how the English and Australian statutes address those two issues and compares their approach to that of the United States.

Addressed first is the obligation to establish the suspect's knowledge of the password.

---

151 Note, too, that in the United States if the control test is adopted the form of order may also affect the evidentiary requirements. In that situation different evidentiary requirements arise when the unencrypted contents are compelled compared to when the act of decryption is required. No such differences are present in the English and Australian statutes.

4.4.3.1 The applicant's knowledge about the contents of the encrypted drive

Before a disclosure notice can be issued under *RIPA*, the appropriate permission to do so must first be granted to the person who will issue the disclosure notice. Ordinarily, that permission will be granted concomitantly with the issuing of a search warrant or, if the warrant has already been issued and executed, upon the written permission of a person holding judicial office.[152] In order for the appropriate permission to be granted, the person granting that permission must, amongst other requirements, be satisfied that there are reasonable grounds for believing that relevant evidentiary material of substantial value will be found.[153] Once the appropriate permission has been granted, the person to whom that permission has been given may issue a disclosure notice pursuant to s 49(2) of *RIPA*. Notably, s 49(2) does not contain a further requirement regarding the state's knowledge of the contents of the encrypted drive. Thus, the requirement ordinarily imposed on the state is to adduce enough evidence to satisfy the judicial decision maker that there are reasonable grounds <u>for believing</u> evidentiary material to be contained on the encrypted drive. In Australia, a less onerous standard is adopted, with the state only needing to adduce sufficient evidence for the issuing magistrate to be satisfied that there are reasonable grounds <u>for suspecting</u> the encrypted device contains evidential material.[154]

What do reasonable grounds for believing and reasonable grounds for suspecting require? Suspicion and belief are 'different states of mind',[155] there being 'a clear distinction between things that are "suspected" of having a certain quality or characteristic…and things which are believed to have this peculiarity'.[156] Both, however,

---

152 *RIPA* sch 2, para 2(a).

153 Note that Schedule 2 of *RIPA* itself is silent on the evidentiary burden to be satisfied before the appropriate permission may be granted. Instead, that burden (which requires there to be reasonable grounds for believing evidentiary material will be found) is contained in the requirements imposed on an applicant for a warrant: *PACE* s 8. As such, the appropriate permission cannot be granted unless this requirement is satisfied.

154 *Crimes Act 1914* (Cth) s 3LA(2)(a); *Crimes Act 1958* (Vic) ss 465AA(5)(a), 465AAA(3)(a); *Criminal Investigation Act 2006* (WA) s 59(1)(b) read with s 58(3)(f); *Police Powers and Responsibilities Act 2000* (Qld) s 151.

155 *George v Rockett* (1990) 170 CLR 104, 115. See also *Ruddock v Taylor* (2005) 222 CLR 612, 633 [73] (per McHugh J in dissent).

156 *Ruddock v Taylor* (2005) 222 CLR 612, 633 [75] (per McHugh J in dissent) quoting *Homes v Thorpe* [1925] SASR 286 at 291.

are assessed by means of an objective test: '[w]hen a statute prescribes that there must be "reasonable grounds" for a state of mind – including suspicion and belief – it requires the existence of facts which are sufficient to induce that state of mind in a reasonable person'.[157]

Of those two states of mind, 'reasonable suspicion is something less than a belief'.[158] It refers to 'a state of conjecture or surmise where proof is lacking: "I suspect but I cannot prove"'.[159] In *Queensland Bacon Pty Ltd v Rees*, the Australian High Court said that '[a] suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to "a slight opinion, but without sufficient evidence"'.[160] It is, the Privy Council has held, 'a very limited requirement'.[161] For that reason, though 'a factual basis for the suspicion must be shown', the facts giving rise to a reasonable suspicion need not be sufficient to give rise to a reasonable belief.[162] However, while reasonable belief requires a factual basis in excess of that required for a reasonable suspicion, the factual basis for a reasonable belief need not rise as high as the balance of probabilities.[163]

---

157 *George v Rockett* (1990) 170 CLR 104, 112. See also *Ali v Jayaratne* [1951] AC 66, 71; *Inland Revenue Commissioners v Rossminster* [1980] All ER 80, 92 (per Lord Diplock); *Mohammed v The Secretary of State for the Home Department* [2014] EWHC 4317 (Admin), [96]; *Bradley v Commonwealth* (1973) 128 CLR 557, 574-575; *W.A. Pines Pty Ltd v Bannerman* [1980] 30 ALR 559, 571 (per Lockhart J); *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 429 [10] per Gleeson CJ and Kirby J; *Ruddock v Taylor* [2005] HCA 48, [40].

158 *R v Zotti* (2002) 82 SASR 554.

159 *Hussein v Chong Fook Kam* (1970) AC 942, 948. See also *George v Rockett* (1990) 170 CLR 104, 115.

160 (1966) 115 CLR 266, 303 (per Kitto J). See also *Mohammed v The Secretary of State for the Home Department* [2014] EWHC 4317 (Admin), [96]: 'suspicion suggests a temporary and provisional view, suggests the existence of doubt, and that matters may become clearer in the future'.

161 *Hussein v Chong Fook Kam* (1970) AC 942, 949.

162 *George v Rockett* (1990) 170 CLR 104, 115. See also *Ruddock v Taylor* (2005) 222 CLR 612, [75] (McHugh J in dissent) where his Honour, citing *Homes v Thorpe* [1925] SASR 286, 291, states that '[t]he gradation in mental assent is "suspicion" which falls short of belief'. Note, too, the decision in *Mohammed v The Secretary of State for the Home Department* [2014] EWHC 4317 (Admin), [96] in which the judgment of McHugh J was said to accord with the English position.

163 *George v Rockett* (1990) 170 CLR 104, 116. It was further noted that '[b]elief is an inclination of the mind towards assenting to, rather than rejecting, a proposition and the grounds which can reasonably induce that inclination of the mind may, depending on the circumstances, leave something to surmise or conjecture'.

How have the courts interpreted these evidentiary burdens? With limited discussion and a seeming willingness not to be unduly burdened by them. In *R v S(F)* three computers were seized. On one, belonging to S and found at his apartment in London, documents were retrieved which appeared to satisfy the requirement for a document of the kind likely to be useful to a terrorist; on another, in Sheffield, at which S was found having partially entered an encryption key, the use of encryption prevented the police from searching the computer; and the third computer, also protected by encryption, belonged to the second defendant who was also arrested. Thus, the only evidence discussed in the judgment relating to the belief that evidence would be found on all the encrypted computers was the evidence that was found on S's computer in London. That evidence was, nevertheless, found to be sufficient to satisfy the evidentiary requirements regarding the contents of all of the encrypted drives, even the two found at different locations.

In Australia, courts have held the standard to be met in circumstances where: encrypted files were found on a computer that had been used to view terrorist propaganda and websites;[164] an order for access to email accounts was sought after child pornography had been found in the accused's possession;[165] a hard drive was found in the possession of a person who was a customer of a child pornography website;[166] an iPhone was found in the possession of a person at the same time as drugs were found hidden on him;[167] and an iPad and mobile phone were found in a suspect's house during a search that found drugs.[168]

---

164 *K v Children's Court of Victoria* [2015] VSC 645, [9]-[10].

165 *R v SW* [2008] NSWDC 148, [2]-[4]. Compare this to *Securities Exchange Commission v Huang* (ED Pa, Civ No 15-269, 23 September 2015) where a compelled production order for the password to a suspect's mobile phone was refused as part of a corporate fraud investigation.

166 *R v Monaghan* [2014] ACTSC 278, [28]-[29].

167 *R v Ford* [2017] QSC 205, [6]-[8]. See also *Lenton v Western Australia* [2017] WASCA 224, [11]-[18] (drugs and mobile phones found in person's backpack).

168 *Garbellini v The State of Western Australia* [2017] WASC 93, [9]; *The State of Western Australia v Doyle* [2017] WASCA 207, [7]. See also *Dias v The State of Western Australia* [2017] WASCA 49, [3]-[9], *Chadburne v The State of Western Australia* [2017] WASCA 216, [15]-[18] and *Sumption v Grant* [2013] WASC 258, [7]-[8], all of which involved drugs and mobile phones found in the suspect's motor vehicle while the suspect was in the vehicle.

The primary lesson to be taken from the English and Australian positions on this evidentiary requirement is how similar it is to the control test in the United States, and consequently how far removed it is from the contents test. To know with reasonable particularity what will be found on an encrypted device, as is demanded by the contents test, is to require far more than to have a reasonable belief or reasonable suspicion that material evidence will be found. That much is clear from the United States' decisions that have applied the contents test, as *In re Grand Jury Subpoena Duces Tecum* amply demonstrates. In that matter, the Court found that the reasonable particularity standard had not been satisfied despite: an encrypted laptop and encrypted hard drives being found in the hotel room with the accused; and the accused having been the only common guest who had stayed at three other hotels from which child pornography had been shared through one specific YouTube account. That decision sits at odds with the decision in *R v S(F)*, and is one that is unlikely to have been occurred under the English or Australian requirements.

A similar divergence is apparent in *GAQL v Florida*, a matter in which the defendant was involved in a motor vehicle accident while driving with an illegal blood-alcohol content. A passenger gave evidence that the defendant had been drinking and that he had shared messages with the survivor by phone that day while drinking. The State sought a compelled production order to view any messages on the defendant's phone. Despite that evidence, the Court held that the reasonable particularity standard had not been satisfied as the State could not identify 'any specific file locations or even particular file names' that it believed to be on the defendant's phone.[169] This outcome, once more, is unlikely to have arisen under the English or Australian statutes.

The position adopted by England and Wales and Australia, as well as by the control test, has much to recommend it. The evidentiary burdens imposed in those jurisdictions require a factual basis to give rise to a reasonable belief (in England and Wales) or suspicion (in Australia) that evidentiary material is contained on the encrypted drive. Under the control test, probable cause for believing there to be evidence on the

[169] *GAQL v Florida* 257 So 3d 1058, 1064 (Fla App 4 Dist, 2018).

electronic device must be shown.[170] Those thresholds are sufficient to prevent the state from engaging in baseless fishing expeditions, but they are not so onerous as to undermine the efficacy of the compelled production order legislation. By comparison, the burden imposed by the contents test would see compelled production orders subject to an evidentiary standard that no other search warrant faces, a burden for which there is no obvious justification. The burden is not there to protect a suspect' privacy, as the ordinary warrant requirements perform that function; nor is it there to protect the privilege, for, as Chapter 3 argued, the control test arguably more faithfully applies the elements of the act of production and foregone conclusion doctrines than does the contents test. The contents test stands alone among the three jurisdictions in imposing so onerous a burden,[171] and it is one that appears to be imposed in error.

It is the existence of that potential error which may provide the strongest reason for concluding that there is little that Australian courts can learn from the approach of the United States. The courts of the United States that have imposed the contents test have done so on the understanding that it is required by the foregone conclusion doctrine. There is no broader argument for why the state would need to know the contents of the encrypted drive with 'reasonable particularity'. Having that level of knowledge does not lessen the infringement of the privilege and the risk of a miscarriage of justice does not rise or fall depending on the state's knowledge of the contents of that drive. It is only because of the contents test that such a demanding standard is imposed by some courts, and as the contents test arguably misapplies the foregone conclusion doctrine, the heightened requirements imposed by it are inappropriate for Australia.

Having in this Part considered the evidentiary burden regarding the state's knowledge of the contents of the encrypted drive, in Part 4.4.3.2 the evidentiary burden concerning the suspect's knowledge of the password is examined.

4.4.3.2 The suspect's knowledge of the password

---

170 See Part 3.3.2.

171 The burden imposes a higher burden than that imposed in Canada to obtain a search warrant: see *R v Cusick* 2015 ONSC 6739, [141]–[142].

In England and Wales, the same standard is applied to knowledge of the password as is applied to knowledge of the contents of the encrypted drive. That is, the person issuing the disclosure notice must be satisfied that there are reasonable grounds to believe that the suspect possesses the password.[172] In Australia, by contrast, a higher standard is imposed: the issuing judicial officer must be satisfied that the suspect knows the password.[173] To be so satisfied, the magistrate must believe that those conditions have been met on a balance of probabilities.[174]

In their application these provisions have, as with the requirement concerning knowledge of the contents of the encrypted device, proven to be more easily satisfied than is the case in the United States. In England and Wales, in *Andrews*, McCombe J of the High Court, in overturning the decision of the Court below, held that it was 'a perfectly legitimate inference to draw'[175] that the respondent knew the encryption keys to his laptop and two USB memory sticks that were found with it at the hostel at which he lived.[176] May P, agreeing with and adopting the reasons of McCombe J, reiterated that the decision of the Court below was 'unsustainable' and that 'the facts of the present case falls so far in favour of a disclosure requirement that the judge's decision must be wrong'.[177] That decision appears to be based solely on the respondent's ownership of the laptop and the location at which it and the USB memory sticks were found.

---

172 *RIPA* s 49(2)(a).

173 *Crimes Act 1914* (Cth) s 3LA(2)(c); *Crimes Act 1958* (Vic) s 465AA(5)(a), 465AAA(3)(a); *Criminal Investigation Act 2006* (WA) s 59(1)(c). Note that s 154 of the *Police Powers and Responsibilities Act 2000* (Qld) is silent on the evidentiary burden that must be met. However, as all of the Australian jurisdictions speak of relevant knowledge when referring to the suspect's knowledge of the password, and as each of the Commonwealth, Victoria and Western Australia require the issuing officer to be *satisfied* that the specified person has the relevant knowledge, that same standard is likely to be adopted by a Queensland court hearing an application under s 154.

174 See, for example, *Commissioner of the Australian Federal Police v Hart* (2018) 351 ALR 1, [10]-[11].

175 Andrews [2011] EWHC 1966 (Admin) [20].

176 Ibid [3]-[4].

177 Ibid [27]. This decision is to be preferred to that in *In re Grand Jury Subpoena Duces Tecum*. There is no evidence in *In re Grand Jury Subpoena Duces Tecum* judgment that the accused provided a satisfactory explanation for why he was travelling with several electronic devices for which he did not know the encryption keys. In the absence of any such reasonable explanation there is every reason to expect a magistrate to be satisfied that the person knows the encryption key to electronic devices found in that person's possession.

Under *RIPA*, however, this is not necessarily the end of the process. If a person refuses to comply with a s 49 notice, s 53 addresses that non-compliance. Section 53(1) provides that the knowing failure to comply with a s 49 notice constitutes an offence. Section 53(2) proceeds to provide that where it is shown that a person possessed the encryption key at any time prior to the granting of the s 49 notice, 'that person shall be taken' to continue to possess that key 'unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it'. If, therefore, the recipient of a s 49 notice can show that he or she is not in possession of the encryption key at the time that compliance with the notice is sought, compliance is not required. In order for the recipient of a s 49 notice to rely on this provision, it is necessary for him or her to adduce 'sufficient evidence of that fact…to raise an issue with respect to it' provided that 'the contrary is not proved beyond a reasonable doubt'.[178] To date, however, no cases have been identified that consider what constitutes sufficient evidence for this purpose.

Though no Australian courts have expressly discussed this requirement, several decisions of the Supreme Court and Court of Appeal of Western Australia indicate that the approach adopted in *Andrews* has found favour in Australia, notwithstanding the use of the more demanding standard of being satisfied. In *Garbelline v The State of Western Australia*,[179] a magistrate granted a data access order against the appellant for an iPad and mobile phone which were found during a search of her home, a home she shared with her adult daughter and 14 year old nephew; and in *The State of Western Australia v Doyle*,[180] mobile phones found at the appellant's house were made subject to a data access order. Similar outcomes have been reached in circumstances where the electronic device was found in the suspect's possession. In *Lenton v Western Australia*,[181] at the time of the appellant's arrest he was carrying a backpack which contained illegal drugs as well as several mobile phones and a laptop computer, all of

178 *RIPA* s 53(3).
179 [2017] WASC 93.
180 [2017] WASCA 207.
181 [2017] WASCA 224.

which were password protected.[182] A data access order was granted in respect of those devices. In *Dias v The State of Western Australia*,[183] a data access order was granted in respect of mobile phones found in a backpack that was in the appellant's car which was stopped and searched while he was driving; and in *Chadburne v The State of Western Australia*,[184] a mobile phone found in the appellant's vehicle was made the subject of a data access order.[185]

That Australia and England and Wales have adopted a more lenient standard than that applied in the United States is clear. In *In re Grand Jury Subpoena Duces Tecum*, the defendant was found with the laptop and hard drives in the hotel room in which he was staying (on his own). The Court, nevertheless, found those facts to be insufficient to establish that the suspect was able to access the electronic devices.[186] Similarly, in *In the Matter of Decryption of a Seized Data Storage System*, law enforcement officials, during a lawful search of the suspect's home, of which he was the sole resident, found several computers and storage devices. Regardless of the fact that the suspect was the only occupier of the premises, the Court held that the State had not established that the suspect knew the passwords to the encrypted devices.[187] Neither of those decisions would have been made by an English or Australian court.

The English and Australian position is to be preferred to that of the United States. While modern life may require the use of more passwords than the ordinary person can remember, it is also true that there is a hierarchy of passwords. While the ordinary person may not remember the password to a little used online service, they do remember their phone and computer passwords – passwords for devices that are used every day. For USB drives, too, we either remember them or reduce them to writing because once they are forgotten there is no other means of accessing the data on those

182 *Lenton v Western Australia* [2017] WASCA 224, [10]-[18].

183 [2017] WASCA 49.

184 [2017] WASCA 216.

185 Notably, however, in none of those decisions does it state whether the suspects denied knowledge of the encryption key.

186 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1346 (11th Cir, 2012).

187 *In the Matter of Decryption of a Seized Data Storage System* (Ed Wis, No 13-M-449, 19 April 2013), slip op 8.

devices. As passwords reduced to writing still fall within the scope of the English and Australian statutes, it is strongly arguable that if the state can show that the suspect owns the devices that are found in his or her possession, that evidence is sufficient to satisfy the evidentiary burden. For in that circumstance the owner of the electronic device would have been found in possession (or control) of the electronic device in question, a device owned by him or her and the type of device the password to which is either remembered because of the frequency with which it is used or reduced to writing due to the risk of forgetting that password. It is therefore, as the English Court of Appeal held, a perfectly legitimate conclusion to draw that the suspect will know the password (or have reduced it to writing somewhere).

To the extent that it is necessary, some assistance in dealing with this issue could be obtained through a thorough examination of the electronic device. For example, fingerprint analysis of an electronic device found in a house shared by several people may demonstrate that the device is only, or is overwhelmingly, used by one individual. In similar fashion, if the electronic devices in *In re Grand Jury Subpoena Duces Tecum* held only or overwhelmingly the fingerprints of the accused, that evidence would make the conclusion that the accused knows the encryption key irresistible. In other circumstances, it may be possible to establish that the electronic device in question had recently been used – something that can easily be established in respect of a smartphone that had recently made a phone call, accessed the internet or sent a message. Where a computer has been seized, a subpoena to the relevant internet service provider will be able to establish if the computer has been in recent use. If it has, then finding that device in the possession of its owner would render any assertion by that same owner that he or she does not know the password unsustainable.

The case law of the United States does not provide any reasons for favouring its strict approach over that of England and Wales. Those decisions simply hold that the evidentiary burden has not been satisfied. English courts, however, have weighed similar evidence differently, doing so in a manner consistent with how Australian courts have resolved this issue. It is possible, though, that the primary lesson to be taken from the analysis in this Part concerns not how courts have weighed the evidentiary burden

thus far, but what additional evidence can be led by the state to meet that evidentiary burden. As the paragraph above notes, there are several potential sources of further evidence that, if pursued, would satisfy any evidentiary burden. The lesson from this Part, then, is directed less at the Australian courts and legislatures who, in drafting and interpreting the Australian statutes, have walked the same path as one of its closest fellow common law jurisdictions. Rather, it is a lesson for those applying to Australian courts for a compelled production order – a lesson to perform relatively minor investigations that could ensure the satisfaction of the evidentiary burden regarding the suspect's knowledge of the password.

4.4.3.3 Other evidentiary requirements

Both *RIPA* and the Australian statutes impose further evidentiary burdens that have not arisen in the case law of the United States. In the case of *RIPA*, it requires that the imposition of a disclosure notice is both proportionate and the only reasonably practicable means by which the information sought can be obtained;[188] in Australia, compelled production orders can only require a person to 'provide information or assistance that is reasonable and necessary'.[189] What these requirements are directed to, therefore, is the need for the issuing of a compelled production order to be the only, or only proportionate, means of accessing the encrypted data. That question of whether a compelled production order is the only proportionate means to obtain access to encrypted material is the subject of Chapter 5. As will there be seen, that question involves the consideration of what is required by proportionality and an assessment of what other means exist to gain access to encrypted data.

4.5 LUPPINO V FISHER

Shortly before the submission of this thesis, White J of the Federal Court handed down his decision in *Luppino (No 2)* concerning the granting of a compelled production order under s 3LA of the *Crimes Act 1914* (Cth).[190] The order was made in respect of an

188 *RIPA* s 49(2)(c) and (d).

189 *Crimes Act 1914* (Cth) s 3LA(1); *Crimes Act 1958* (Vic) ss 465AA(2) and 465AAA(2); *Police Powers and Responsibilities Act 2000* (Qld) ss 154(1)(a) (which imposes a requirement of necessity); *Criminal Investigation Act 2006* (WA) s 59(2)(d).

190 *Luppino (No 2)* [2019] FCA 1100.

encrypted Samsung smartphone that was found in Luppino's motor vehicle during the performance of a lawful search that occurred while Luppino was driving the car. The phone was one of three found in his possession at the time and the only one that was encrypted. Though a substantial part of his Honour's judgment concerns procedural requirements for the granting of a compelled production order which are not germane to this thesis, several issues raised by White J warrant noting.

First, his Honour found that the information and assistance that could be required under a compelled production order included 'the provision of a username, password, digital fingerprint or private encryption key'.[191] Importantly, though, the order needs to contain a level of specificity about the form of the assistance and the device to which it applies. That is, it is insufficient for the order to merely require assistance to be provided; the order must state what the particular type of assistance is, such as the provision of the password, and identify the relevant device.[192]

Secondly, with regard to the abrogation of the privilege, White J found that although the abrogation was only 'indirect' – as it only required the giving of access to the material rather than the disclosure of the material itself – the consequences of its abrogation were indistinguishable from those that would follow from directly disclosing incriminating material.[193] His Honour's finding on this issue confirms what this thesis argued in Part 4.3.2: that the privilege is engaged by the compelled production of a password. That decision therefore rejects the argument in the Explanatory Memorandum to the 2009 amendments to s 3LA that the privilege was not infringed as the section only required the provision of information which enables the search to be conducted.[194] As this thesis there argued, the contents of the encrypted drive are derivative-use evidence and as such fall within the scope of the privilege.

191 Ibid [27].
192 Ibid [122], [167].
193 Ibid [33].
194 Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009, 92.

Thirdly, and as a result of it being raised by Luppino as one of his grounds of review, White J was required to consider the evidentiary burdens imposed by s 3LA regarding Luppino's knowledge of the password to the smartphone. White J noted that the smartphone was found in the possession of Luppino while he was alone in his motor vehicle; that all of the items in the vehicle appeared to belong to Luppino; and that Luppino had said 'no comment' when asked if the smartphone was password protected. That evidence, his Honour held, 'was rationally capable of supporting' the state of satisfaction required of the magistrate regarding Luppino's use of the smartphone and his knowledge of the password.[195] His Honour's findings on this issue are consistent with the decisions in the cases discussed in Part 4.4.3.2 above.

Lastly, Luppino challenged the applicability of s 3LA to smartphones on the basis that a smartphone was not a computer or data storage device, as required by the statute. White J, while expressing the view that this argument had 'some force', refused to express a concluded view on this issue.[196] It is important to note that his Honour's comment on this issue does not mean that compelled production orders cannot be made in respect of smartphones *because of* the privilege. Rather, White J simply questioned whether the power to perform a search that is granted by s 3LA, as drafted at the time the order was made, was intended to apply to smartphones. Furthermore, his Honour's comments have little relevance for future cases. With the passage of the *Assistance and Access Act* in December 2018, s 3LA has been amended to insert a new sub-s (1)(a)(ia), which provides that a compelled production order can be made in respect of a device found during a search of a person. This amendment is directed at ensuring that s 3LA applies to smartphones. As is made clear in the Explanatory Memorandum to the *Assistance and Access Act*, because s 3LA prior to amendment did 'not envision people carrying smartphones in their pockets…[t]he Bill will resolve this gap'.[197]

---

195 *Luppino (No 2)* [2019] FCA 1100, [196].

196 Ibid [184]

197 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 22.

4.6 CONCLUSION

The previous chapters have considered how the privilege was applied in the four jurisdictions to related orders; whether the privilege could be abrogated in those jurisdictions, and if so on what terms; how Canada and the United States dealt with compelled production orders; and, in this Chapter, how England and Wales and Australia dealt with those applications. How do the findings in this Chapter relate to those Chapters that preceded it?

First, as a result of the analysis in Part 4.3, it is apparent that both the English and Australian responses to the question of whether the privilege is infringed by a compelled production order are consistent with how they have determined the scope of the privilege in related orders. In both jurisdictions, the privilege has been found to be inapplicable to the compelled production of bodily features, such as fingerprints, blood samples and breath samples. While the use of a biometric feature such as a fingerprint to unlock an electronic device is distinguishable from using one's fingerprint for identification purposes, the similarities between those actions are arguably greater than the differences. In particular, in both instances the fingerprint is used to obtain evidence against the suspect. With compelled production orders, the incriminating evidence is that which is found on the now decrypted device; as an identification tool, that fingerprint can be matched to a fingerprint at a crime scene. Without the use of that fingerprint, potentially incriminating evidence – a fingerprint at the crime scene, encrypted electronic data – could not be used against the suspect. Furthermore, the compelled use of one's fingerprint, in either scenario, is a physical act involving a physical item that exists independently of the suspect's will and which involves no testimony on the suspect's behalf. That is why, as the English Court of Appeal noted, 'some "acts of production" such as fingerprints, blood samples or voice recordings would not attract the privilege against self-incrimination'.[198]

Consistency with existing precedent is evident too in respect of alphabetic and numeric passwords. In Australia, for example, motor vehicle reporting obligations, though an

[198] *R v S(F)* 1 WLR 1489, 1497 [21].

infringement of the privilege, were permitted due to the abrogation of the privilege by the statute that imposed the reporting obligation. It is precisely that same circumstance that arises with compelled production orders: they implicate the privilege but avoid the consequence of that by abrogating the privilege. In England and Wales, motor vehicle reporting obligations infringed the privilege but did not destroy its essence – the same outcome as occurred with compelled production orders.

Though each of the jurisdictions found that the privilege was infringed by compelled production orders, three separate outcomes resulted from that finding. In Canada, it was the end of the matter, the infringement too severe to be excused; in the United States, that finding could be avoided if the foregone conclusion doctrine was enlivened; and in England and Wales and Australia, it resulted in the abrogation of the privilege to ensure such orders could be made. These differing outcomes are the result of the constitutional status of the privilege in Canada and the United States. That status precludes their abrogation without commensurate immunity, with the result that the finding that the privilege has been infringed either precludes the use of such orders (as in Canada) or requires further development of the privilege to remove the order from its scope (as occurs with the foregone conclusion doctrine in the United States). As both England and Wales and Australia can abrogate the privilege without such grants of immunity, there is no need for either to rely on an equivalent to the foregone conclusion doctrine or to resign themselves to being unable to compel the production of a password.

Secondly, this thesis has found that in England and Wales and Australia the applicability of the privilege is not affected by whether the order seeks the unencrypted documents, the password or the entry of the password into the encrypted device. This marks a notable change from the position in the United States, where the form of order is of substantial importance to the role of the act of production doctrine. It is also the more defensible approach. In *State v Stahl*, the Court stated that 'we are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals

who use their fingerprint as the passcode'.[199] That statement rings equally true when recast to hold that the privilege could not have been intended to provide different levels of protection to alphabetic and numeric passcode depending on the form of order that was sought.

While the manner in which the privilege is applied to compelled production orders in the United States is consistent with the contortions that have previously occurred in Fifth Amendment jurisprudence, it is only through examining the history of the privilege in the United States that the current position can be explained. In England and Wales and Australia, by contrast, the ability to abrogate the privilege allows those legislatures to focus on the purpose sought to be achieved by legislation that allows for compelled production orders, unencumbered by the tortuous developments of the privilege that plague the courts of the United States. And the purpose of that legislation is to gain access to encrypted data, regardless of the form that compliance with that order takes. As for the compelled production of biometric passwords, each of England and Wales, Australia and the United States hold that such order does not implicate the privilege.

Lastly, this Chapter has revealed how England and Wales and Australia have adopted a different approach to the United States when evaluating the evidentiary burdens. In respect of both knowledge of the password and, where the contents test is adopted, knowledge of the contents of the encrypted device, the courts of the United States imposed a greater burden. As discussed in Part 4.4.3.2, the courts of the United States have failed to articulate the reasons for the standard they have imposed in respect of the suspect's knowledge of the password. It is out of step with the approach taken in England and Wales and Australia and appears to place too much weight on the suspect's averment that he or she cannot recall the password.

As already argued in this Chapter, where a device that is ordinarily used daily is found in the possession or control of the suspect and is owned by the suspect, that evidence should satisfy the evidentiary burden concerning knowledge of the password. Such is

199 *State v Stahl* 206 So 3d 124, 135 (Fla Ct App, 2016).

the position adopted in England and Wales and Australia. It is to be expected, however, that in most circumstances that is not the only evidence that will be available to law enforcement officials: evidence from internet and telecommunication services providers will be able to show how recently most electronic devices were used. Evidence of recent usage will make the conclusion that the suspect knows the password irresistible. As for knowledge of the contents of the encrypted device, this Chapter has argued that the English and Australian legislation imposes an appropriate evidentiary burden on the applicant, one that is consistent with not only the control test in the United States but also the evidentiary burden imposed for other searches pursuant to a search warrant.

While to this point many of the issues identified in the Introduction to this thesis have been addressed, one issue remains outstanding. The previous Chapters have shown how the application of the privilege has often been driven by matters of pragmatism. In England and Wales, the Court of Appeal has noted that it is often necessary and accepted that the privilege may need to be curtailed to ensure 'the stability of society'.[200] In the United States, Brennan J noted in *Schmerber* that 'the privilege has never been given the full scope which the values it helps to protect suggest'.[201] That it has not is a result of an understanding that pragmatic considerations preclude such an outcome. Such considerations are evident in the works of English writers too.

In writing about the decision of the European Court of Human Rights in *O'Halloran and Francis*,[202] Ashworth argued that instead of courts adopting an approach that balances the public interest against that of the individual, the privilege should only be limited where a 'considered exception' is found to exist.[203] An example of a considered exception is the exception identified in *O'Halloran and Francis*, in which a requirement imposed on a motor vehicle owner to identify who was driving his motor vehicle when

---

200 *R v S(F)* [2009] 1 WLR 1489, 1494-5 [17] citing *R v Director of Serious Fraud Office, Ex parte Smith* [1993] AC 1.

201 *Schmerber* 384 US 757, 761 (1966).

202 (2008) 46 EHRR 21.

203 Andrew Ashworth, 'Self-Incrimination in European Human Rights Law – A Pregnant Pragmatism?' [2008] 30 *Cardoza Law Review* 751, 764.

the vehicle was caught breaking a road rule was not an infringement of the privilege as the exception was a pragmatic necessity on which there was a European consensus. If Ashworth is correct that *O'Halloran and Francis* constitutes a considered exception, it is arguable that compelled decryption, too, ought to be a considered exception.

Some of the reasons for identifying compelled decryption as a considered exception can be found in the following passage from Redmayne on the privilege. He writes that:

> It is therefore worth underlining the point that the positive reasons for doing away with the privilege may not be that great either. It was noted above that the creation of a duty to cooperate will not do very much to help the state prosecute and convict offenders: offenders are likely to respond by lying, rather than by self-incriminating. We can sharpen this insight by asking what positive reasons there are for sanctioning non-cooperation. Where the criminal law is concerned, we frequently look to the harm principle to justify the use of sanctions against particular forms of conduct. We can therefore ask: just what harm does a defendant do by refusing to cooperate in his prosecution? This question is not as easy to answer as it might appear. Any harm done by a noncooperative defendant is not as obvious as the harm inflicted by assault or theft. It is if anything a type of public harm: like the person who does not pay his taxes, the defendant is undermining the smooth operation of institutions essential to government. But is he? Even in a system with the privilege against self-incrimination, our conviction rate is reasonably high. The majority of defendants admit guilt, doubtless because they realize that their chances of escaping conviction are slim. Removing the privilege is not likely significantly to increase the conviction rate.[204]

That statement, directed not specifically at the abrogation of the privilege in the context of compelled decryption but rather the elimination of the privilege in its entirety, reveals why the role of the privilege in the context of compelled decryption is different to many other circumstances. In the first place, compelling decryption is unlikely to lead to false answers, as the accuracy of any answers given can be definitively tested by using the encryption key provided by a defendant to try and decrypt the relevant data. Secondly, the harm suffered by refusing to compel production of a password can more readily be identified: law enforcement is unable to view the contents of lawfully seized evidence, without which a conviction may be unobtainable. In this respect the evidence contained on an encrypted device is different to, for example, the murder weapon that is hidden and cannot be found. The encrypted evidence has been found, has been seized, but cannot be viewed. The harm in being unable to view that evidence is more tangible than

---

[204] Mike Redmayne, 'Rethinking the Privilege Against Self-Incrimination' (2007) 27 *Oxford Journal of Legal Studies* 209, 226.

the harm of not being able to extract a confession from an accused. Finally, it is not clear that defendants, in the absence of an obligation to do so, will be willing to effectively admit guilt by providing an encryption key where the refusal to do so leaves law enforcement with insufficient evidence to obtain a conviction.

Commenting on the decisions in *Brown* and *Saunders*, Redmayne acknowledges that those category of cases – which would include compelled decryption cases – are cases in which the defendant has 'little ability to produce misleading information'.[205] This, he proceeds to note, means that '[i]t is arguable, then, that there is something to be gained by abrogating the privilege in these situations'.[206] Redmayne concludes that we should not 'over-value the privilege', but should 'recognise a deep vein of pragmatism in our respect for the principles underlying it. While the privilege is valuable, it is not so valuable that we should not be prepared to recognize exceptions to it'.[207]

Both Ashworth and Redmayne recognise that which is relatively clear: in certain limited circumstances the scope of the privilege is required to give way to pragmatism. Compelled decryption may be one such instance, and it is one in which many of the concerns that arise when the privilege is abrogated – the risk of false statements, the absence of an identifiable benefit – are absent. It thus arguably stands as an example of the considered exception identified by Ashworth.

In Chapter 5 the adoption of a pragmatic approach is considered further in the context of encryption workarounds. As will there be discussed, whether there are viable and proportionate alternatives to compelled production orders is an important question, and one that influences the application of the privilege to compelled production orders.

205 Ibid 230.
206 Ibid.
207 Ibid 232.

CHAPTER 5

ENCRYPTION WORKAROUNDS

5.1 INTRODUCTION

Over the previous four Chapters this thesis has considered how the courts of the four jurisdictions have determined the scope of the privilege in respect of related orders; how those courts have assessed whether compelled production orders fall within that scope, which included an examination of the exclusionary rules in those jurisdictions and the role that abrogation of the privilege has played in England and Wales and Australia; how the various jurisdictions have weighed the competing interests of the public and the suspect when determining an application for a compelled production order; and whether the decisions of those courts when applying the privilege to compelled production orders have been consistent with how they applied the privilege to the related orders. That analysis found that in England and Wales, Australia and the United States, a compelled production order may fall outside the scope of the privilege. Remaining for consideration, however, is the role of alternative encryption workarounds and their impact on the scope of the privilege when a compelled production order is sought. That is the subject of this Chapter, in which it will be argued that where an encryption workaround is available that imposes a lesser infringement on the rights of a suspect than a compelled production order would, that alternative workaround should be used in preference to the compelled production order. This, it will further be argued, has consequences for the scope of the privilege when a compelled production order is sought.

Alternative encryption workarounds are means other than compelled production orders through which law enforcement officials can obtain access to plaintext versions of otherwise encrypted data. In recent years they have received increasing attention. While some of those workarounds may be as simple as guessing the password to the encryption program, others, such as hacking into the encrypted device, are more complicated and may require statutory authority. In England and Wales and Australia, recent statutory developments have authorised the use of the more intrusive of these

workarounds, such as hacking. Part 5.2 will discuss what encryption workarounds exist and how those recent statutory amendments have facilitated their use.

Having identified the existence and availability of the alternative workarounds, Part 5.3 considers why this is significant. In England and Wales, *RIPA* requires a compelled production order to be a necessary and proportionate response to the problem of encrypted data.[1] In Australia, the respective statutes require that a compelled production order be 'reasonable and necessary'.[2] Part 5.3.1 will explain the content of those requirements and where they are drawn from. It will show how they both serve the same purpose, that of ensuring that a compelled production order can only be granted if there is no equally effective alternative means of obtaining plaintext versions of the encrypted material that imposes less of a burden on the rights of the suspect. Thereafter, Parts 5.3.2 and 5.3.3 consider whether the alternative encryption workarounds satisfy the proportionality requirement set out in the statutes: the former Part asks whether the alternative workarounds are equally effective; the latter if they impose less of a burden than compelled production orders. It will be concluded that in certain circumstances, compelled production orders may be more intrusive than some of the alternative encryption workarounds. In those instances, the statutory requirement that the compelled production order be proportionate will not be satisfied. What that means for the scope of the privilege is the subject of Part 5.4.

Part 5.4 will argue that the alternative workarounds have the effect of varying the scope of the privilege depending on whether a less intrusive but equally effective workaround is available. This outcome arises because the statutory demands of proportionality and necessity require that if an alternative workaround is less intrusive, that workaround is to be used in preference to the compelled production order. Where, however, the workaround is more intrusive, a compelled production order may be made. Two outcomes follow from this. First, the least intrusive mechanism is always utilised and

---

1 *RIPA* ss 49(2)(b) and (c).

2 *Crimes Act 1914* (Cth) 3LA(1); *Crimes Act 1958* (Vic) s 465AA(2), 465AAA(2); *Police Powers and Responsibilities Act 2000* (Qld) s 154(1)(a) (which has the necessary though not the reasonable requirement); *Criminal Investigation Act 2006* (WA) s 59(2)(d).

either the privilege (where a compelled production order is granted) or the right to privacy (where an alternative workaround is used) will regulate the search. Secondly, where a less intrusive workaround exists, the privilege is given its full scope to prevent the use of a compelled production order (the workaround is used instead); where, however, no such workaround exists, the operation of the privilege is limited to enable the compelled production order to be made. The scope of the privilege, therefore, varies according to the existence of a viable alternative workaround. The use of the proportionality assessment in this manner is, it will lastly be argued, a pragmatic response to the infringement that the privilege experiences when compelled production orders are made, a response that seeks to ensure that the privilege is preserved as far as possible in the circumstances of each case. This pragmatic approach is, it will be further argued, consistent with the pragmatic manner in which courts in each of the four jurisdictions have dealt with the privilege over many years.

First, in Part 5.2, the issue of alternative workarounds is considered.

5.2 ENCRYPTION WORKAROUNDS IN ENGLAND AND AUSTRALIA

5.2.1 Types of encryption workarounds

In a recent article, Kerr and Schneier suggest six ways, what they term workarounds, by which law enforcement officials can obtain access to data that has been encrypted.[3] They are: finding the key; guessing the key; compelling the key; exploiting a flaw in the encryption software; accessing the unencrypted data while it is being used; and finding an alternative, unencrypted record of the data.[4] Of the alternatives to compelling the key, finding the key and guessing the key are arguably the least controversial, though there are limits to how successful they are. Finding a key, though it may be as simple as finding a copy of it reduced to writing or obtaining it from a friend or family member of the suspect, is made more difficult by software programs such as password managers that enable a computer user to encrypt all of his or her passwords through the use of a

3 Orin Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 *Georgetown Law Journal* 989.

4 Ibid 991.

single master key.[5] More intrusive means of finding the key may involve legal issues of their own. For example, the use of keylogging software (that records each key that is typed into the electronic device) to discover the password to the encrypted material requires there to be lawful authority to place such software on a person's device.[6]

Guessing the key poses different challenges. While encryption keys themselves are too long to be able to guess with modern computing power, those encryption keys are often protected by shorter passcodes (which the user can remember) that unlock the encryption key, thereby decrypting the electronic data.[7] Although Kerr and Schneier note that experts are relatively successful at guessing passwords, that success, they further note, is largely dependent on the strength of the passcode and the power of the machine guessing it.[8] Exploiting a flaw in the encryption software relies not only on the existence of a flaw that can be exploited, but also on having the knowledge and resources to exploit it.[9] Nevertheless, if sufficient financial resources are available, there is evidence that encryption on mobile phones can be hacked by third parties.[10] In respect of the San Bernardino shooting, for example, it has been claimed that a $1 million fee was paid by the FBI to a third party to gain access to the deceased shooter's iPhone.[11]

---

5 Ibid 997.

6 See, eg, *United States v Scarfo* 180 F Supp 2d 572 (2001).

7 Kerr and Schneier, above n 3, 997-98.

8 Ibid 998-99.

9 See also Manhattan District Attorney's Office, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (November 2017), 8-9 <https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf>. where they give several examples of successful exploits they have managed to achieve.

10 See, eg, Thomas Brewster, 'The Feds Can Now (Probably) Unlock Every iPhone Model in Existence', on *Forbes*, 26 February 2018 <https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#4c280c9e667a>; Thomas Brewster, 'Mysterious $15,000 "GrayKey" Promises to Unlock iPhone X for the Feds' on Forbes, 5 March 2018 < https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#4c7ef5362950>. The precise means by which the devices are hacked is not disclosed. See also Australian Government Department of Home Affairs, Submission No 18 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, 6 [23].

11 Kerr and Schneier, above n 3, 1007.

The fifth workaround is to gain access to the material while it is in an unencrypted form. This can occur either through physically obtaining the device while it is in use – as occurred during the capture and arrest of the prime suspect in the Silk Road website investigation[12] – or by remotely gaining access to the device. Remote access, as the authors note, raises both technical and legal challenges.[13] There is, though, one instance in which this workaround is relatively effective. For several years law enforcement officials in jurisdictions that include the United States and Canada have investigated child pornography offences on file sharing networks. File sharing networks operate by creating a shared folder on the personal computer of each member of the network. That folder is then accessible by all members of the network whenever that computer is connected to the internet. Therefore, once law enforcement officials gain access to the file sharing network, they can access the incriminating material without needing to decrypt any encryption software that may be on the computer in question.[14]

The final workaround (obtaining an unencrypted copy of the data) does not involve decryption of the encrypted material but instead relies on the existence of an unencrypted copy of the encrypted material.[15] A relatively well-known example of this occurred in the San Bernardino case, in which the FBI was able to find an old, partially outdated unencrypted copy of the shooter's iPhone from an iCloud backup.[16] There are obvious difficulties in relying on this workaround, however, including the need for a

---

12 Ibid 1008.

13 Ibid 1009. This may pose a particular problem in the United States. As discussed in Chapter 3, in several cases involving child exploitation material, law enforcement officials were able to view files containing child exploitation material on a suspect's computer over a peer-to-peer file sharing network. When the suspect's computer was later subjected to a physical search, the contents of it were protected by encryption. The decisions in those cases suggest a reluctance by the courts of the United States (though not the Canadian ones) to base a conviction on evidence obtained or viewed over the file sharing network.

14 See, eg, *R v Pratchett* 2016 SKPC 19, [4]-[14]; *R v Spencer* [2014] 2 SCR 212, [7]-[11]; *R v Capancioni* 2016 ONSC 4615; *Apple Mac Pro* 851 F 3d 238 (3rd Cir, 2017). See also *Aguilar v State* 2015 Tenn Crim App LEXIS 1055 (No. M2015-00430-CCA-R3-PC); *State v Cooley* 165 So 3d 1237 (2015); *United States v Ortega* 2015 US Dist LEXIS 147638 (No. CR415-134); *Pachas-Luna v State* 2015 Tex App LEXIS 10653 (No. 01-14-00516-CR) (Tex, 2015); *State v Landrum* 2015 Ariz App Unpub LEXIS 840 (No. 1 CA-CR 14-0203) (Ariz, 2015); *Phillips v United States* 2014 US Dist LEXIS 111042 (Cr Act No. 08-031-LPS) (Del, 2014); *United States v Dennis* 2014 US Dist LEXIS 65694 (No. 3:13-cr-00010-TCB-RGV) (ND GA, 2014); *United States v Cunningham* 694 F 3d 372 (2012); *United States v Schimley* 2009 US Dist LEXIS 118595 (No. 1:08 CR 510).

15 Kerr and Schneier, above n 3, 1010.

16 Ibid.

backup to exist, for it to be known to law enforcement and for law enforcement to have a means of obtaining that backup.[17]

Recent legislative enactments in England and Wales and Australia seek to give law enforcement officials in those jurisdictions the statutory authority to utilise the more intrusive encryption workarounds identified above. They do so by authorising hacking by law enforcement, as well as giving law enforcement the power to compel telecommunications operators to remove encryption. In Part 5.2.2.1 below the former of those powers is considered; in Part 5.2.2.2, the latter.

5.2.2 Statutory measures authorising encryption workarounds

5.2.2.1 Statutorily authorised hacking

In England and Wales, Part 5 of the *Investigatory Powers Act 2016* ('*IPA*') concerns what is termed equipment interference. It operates in the following manner. Section 99 of the *IPA* grants law enforcement officials the power to obtain a targeted equipment interference warrant that authorises the recipient of the warrant 'to secure interference with' any equipment so as to obtain from the equipment communications (which is defined to include 'anything comprising speech, music, sounds, visual images or data of any description'),[18] equipment data[19] or other information.[20] The definition of equipment captures computers, smartphones and storage devices.[21] The powers granted by an equipment interference warrant are broad and, importantly for present purposes, include the exploitation of software vulnerabilities and other hacking

---

17 Ibid 1011. Note, however, that as more and more metadata is produced by electronic devices, that metadata may provide the link to cloud storage servers used by a suspect: Stephanie K. Pell, 'You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?' (2016) 17 *North Carolina Journal of Law and Technology* 599, 630-31.

18 *IPA* s 135(1).

19 Equipment data includes information about the system (such as the operating system or firewall configurations) and information that can assist in identifying a person or system: *RIPA* ss 100, 263(2), (3) and (4).

20 *IPA* s 99(2). Bulk equipment interference warrants, which are concerned with obtaining overseas-related communications, equipment data and other information are provided for in Chapter 3 of Part 6 of the Act. They are not discussed in this Chapter as they are not relevant to this thesis.

21 Home Office, *Equipment Interference: Code of Practice* (March 2018), 2.2; *IPA* s 135(1).

measures such as the use of keylogging software to record each keystroke entered by the user of the equipment in question.[22]

There are restrictions on the granting of interference warrants. For all warrants, approval cannot be given unless the warrant is necessary and proportionate.[23] The proportionality assessment requires a weighing of the infringement of the suspect's privacy against the need for the order to be granted. That includes considering whether there are less intrusive means of obtaining the information;[24] 'the public interest in the integrity and security of telecommunications systems';[25] and the public interest in detecting serious crime.[26] Importantly, interference will never be proportionate if the information could be obtained by less intrusive means, a requirement that highlights the importance of determining whether compelling a password is more or less intrusive than the alternative workarounds.[27] That question is considered in Part 5.3.

In Australia, the *Assistance and Access Act* grants similar hacking powers to law enforcement officials. Schedule 2 gives law enforcement bodies the ability to apply for a computer access warrant.[28] That warrant enables the successful applicant to use the target computer or other equipment to, amongst other things, gain access to data held on the target computer,[29] to remove the computer for the purpose of executing the warrant before returning it,[30] and to take steps to conceal the fact that they have accessed the computer.[31] The computer access can occur remotely or physically.[32]

---

22 Key logging software has been used in the United States to try and circumvent encryption: *United States v Scarfo* 180 F Supp 2d 572 (2001).

23 *IPA* s 106(1)(a) and (b).

24 *IPA* s 2(2)(b).

25 *IPA* s 2(2)(c).

26 *IPA* s 2(4)(b).

27 Home Office, *Equipment Interference: Code of Practice* (March 2018), 4.19.

28 *Surveillance Devices Act 2004* (Cth) s 27A(1) as amended by the *Assistance and Access Act* sch 2 pt 1 item 49.

29 *Surveillance Devices Act 2004* (Cth) s 27E(2)(c) as amended by the *Assistance and Access Act* sch 2 pt 1 item 49.

30 *Surveillance Devices Act 2004* (Cth) s 27E(2)(f) as amended by the *Assistance and Access Act* sch 1 pt 1 item 49.

31 *Surveillance Devices Act 2004* (Cth) s 27E(7) as amended by the *Assistance and Access Act* sch 1 pt 1 item 49.

32 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 17 [70].

Those powers are supplemented by a further power enabling law enforcement officials to obtain an order compelling a person to provide assistance to gain access to data that is the subject of a computer access warrant.[33] The purpose of these powers is, amongst other things, to enable law enforcement to access material in an unencrypted state.[34]

5.2.2.2 Statutory authority to compel a telecommunications operator to remove encryption

Both the English and Australian statutes provide a further power: that of requiring telecommunications operators to remove encryption. Under the *IPA*, telecommunication operators may be given technical capability notices.[35] Technical capability notices are intended to ensure that telecommunications operators have the capability to quickly respond to requests for assistance under the *IPA*.[36] The obligations that may be imposed on telecommunications operators are set out in the *Investigatory Powers (Technical Capability) Regulations 2018* and include the power to require operators to put in place a capability that will enable the operator to remove encryption (that it applied) when required to do so by a warrant issued under the *IPA*.[37] The exercise of this power is subject to various safeguards, including that an operator can only be required to remove encryption where it is reasonably practicable to do so and where the notice is necessary and proportionate.[38] Furthermore, before the Secretary of State can approve the giving of a technical capacity notice, he or she needs to consider, amongst other things, what effect the removal of encryption has upon the integrity and security of the telecommunications system.[39]

As with the *IPA*, the *Assistance and Access Act* provides mechanisms through which assistance can be required from designated communications providers. Three separate

---

33 *Surveillance Devices Act 2004* (Cth) s 64A(1) as amended by the *Assistance and Access Act* sch 2 pt 1 item 114.

34 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 17 [71].

35 *IPA* s 253.

36 It is, therefore, intended for companies that are regularly required to provide assistance under the Act: Home Office, *Equipment Interference: Code of Practice* (March 2018), 8.1–8.2.

37 Ibid 8.7; *The Investigatory Powers (Technical Capability) Regulations 2018* sch 3, part 6.

38 *IPA* s 254(2).

39 Home Office, *Equipment Interference: Code of Practice* (March 2018), 8.15.

mechanisms have been created for Australian security agencies and interception agencies (which include police forces):[40] technical assistance requests, technical assistance notices and technical capability notices. These three mechanisms apply in respect of specified listed acts or things, which include removing electronic protection,[41] installing software[42] and facilitating access to customer equipment and electronic devices.[43] Decryption of encrypted communications is intended to be captured by that list of permissible acts.[44]

Under a technical assistance request, assistance is voluntarily given by a communications provider to a security agency upon request. A technical assistance notice has the same scope as a technical assistance request, but assistance, previously voluntary, is now mandatory.[45] Lastly, a technical capability notice, which needs ministerial approval before it can be issued,[46] requires a communications provider to take steps – such as building a new capability into their system – to ensure that the provider is able to comply with a technical assistance notice and give assistance to the Australian Security Intelligence Organisation or an interception agency.[47]

None of the three measures described above can be implemented unless the issuer of the notice or request is satisfied that the notice or request is reasonable and

---

40 Those agencies are the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Australian Signals Directorate and interception agencies. The interception agencies are the Australian Federal Police, the Australian Crime Commission and the police force of each state and the Northern Territory: *Telecommunications Act 1997* (Cth) s 317B as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

41 *Telecommunications Act 1997* (Cth) s 317E(1)(a) as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

42 *Telecommunications Act 1997* (Cth) s 317E(1)(c) as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

43 *Telecommunications Act 1997* (Cth) s 317E(1)(e) as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

44 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 39 [57].

45 *Telecommunications Act 1997* (Cth) s 317L as amended by the *Assistance and Access Act* sch 1 pt 1 item 7. It may also only be given by the Australian Security Intelligence Organisation or an interception agency.

46 *Telecommunications Act 1997* (Cth) s 317TAAA(1) as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

47 *Telecommunications Act 1997* (Cth) s 317T as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

proportionate and compliance with it is practicable and technically feasible.[48] Determining whether any such notice or request is reasonable and proportionate requires having regard to, amongst other things, the interests of law enforcement and national security; alternative means of acquiring the data sought; whether there are less intrusive forms of assistance; whether the request is necessary; and community expectations regarding privacy and cybersecurity.[49]

A further limitation imposed on what a communications provider can be required to do is a prohibition on requiring them to introduce a systemic weakness or systemic vulnerability into their system (which includes measures that make encryption less effective).[50] A systemic vulnerability or weakness is one that 'affects a whole class of technology' but excludes a vulnerability that selectively impacts a target technology connected with a particular person.[51] Target technologies include specific electronic services and software on a particular computer or smartphone. The distinction between classes of technology and target technologies is not entirely clear, however, and creates a potential source of future dispute. The Explanatory Memorandum expresses the legislature's view that technological classes include, as one example, 'an iOS operating system within a particular class, or classes, of mobile devices'.[52] It is further noted that where requirements in a notice make the whole set of these items more vulnerable, it will be prohibited'.[53] Notwithstanding that, and after noting that a systemic vulnerability does not include actions that weaken protections contained in a target technology, the Explanatory Memorandum proceeds to note that technical assistance notices can require 'the selective introduction of a weakness or vulnerability in a particular service, device or item or software on a case-by-case basis'.[54]

---

48 *Telecommunications Act 1997* (Cth) ss 317JAA, 317P and 317V as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

49 *Telecommunications Act 1997* (Cth) ss 317JC, 317RA and 317ZAA as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

50 *Telecommunications Act 1997* (Cth) s 317ZG as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

51 *Telecommunications Act 1997* (Cth) s 317B as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

52 Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 15 [51].

53 Ibid 16 [51].

54 Ibid 17 [55].

5.3 COMPELLED PRODUCTION ORDERS, ALTERNATIVE WORKAROUNDS AND THE PRINCIPLE OF PROPORTIONALITY

Part 5.2 above examined the alternative encryption workarounds that may be available for law enforcement officials to use to gain access to plaintext versions of otherwise encrypted data. That examination found that recent statutory measures in England and Wales and Australia have made those workarounds available to law enforcement bodies in those jurisdictions. This Part 5.3 analyses what effect those workarounds have on the requirement that compelled production orders be the least intrusive means of accessing the encrypted data. Part 5.3.1 begins by discussing the relevant provisions of the Australian and English statutes that impose this requirement. Thereafter, Part 5.3.2 considers whether the workarounds are capable of replacing compelled production orders, before Part 5.3.3 analyses the question of proportionality and which of compelled production orders or the alternative workarounds imposes the smallest rights infringement.

5.3.1 The statutory proportionality requirement

As noted in Part 5.1, in England and Wales, *RIPA* requires a compelled production order to be a necessary and proportionate response to the problem of encrypted data.[55] The proportionality requirement there referred to is the requirement imposed by Article 8 of the *ECHR*, which protects the right to privacy – a right implicated by compelled production orders.[56] Article 8(2) imposes this proportionality test by providing that any infringement of the right to privacy must be in accordance with the law, necessary and 'in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Those requirements, which courts must interpret narrowly,[57] are captured in ss 49(2)(b), (c) and (d) of *RIPA*.[58]

---

55 *RIPA* ss 49(2)(b) and (c).

56 Home Office, *Protected Electronic Information: Revised Code of Conduct* (August 2018), 3.36.

57 *Funke* (1993) 16 EHRR 297.

58 Home Office, *Protected Electronic Information: Revised Code of Conduct* (August 2018), 3.37.

Applied to Part III of *RIPA*, proportionality mandates, as the starting point, that the disclosure

> is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right to respect for their private life against the benefit to the investigation or operation being undertaken by a relevant public authority in the public interest'.[59]

With regard to the extent of the intrusion, a stricter standard is applied to an act that intrudes into the 'most intimate aspect of private life'.[60] Elements to be considered in that balancing exercise include why the compelled production order is the least intrusive of the available means of obtaining the information and what other methods have not been employed or have been determined to be insufficient.[61] Importantly, proportionality will never be satisfied if the information could reasonably be obtained through other less intrusive means.[62] This reflects the necessity requirement which demands that the action taken (in this case the issuing of a compelled production order) is 'strictly necessary' to achieve the purpose of the action, which purposes can include the obtaining of vital intelligence.[63]

The importance of alternative means was also identified by the Court of Appeal in *R v S(F)*. In upholding the granting of a compelled production order, the Court noted that the legislation was based on the understanding that 'no alternative, reasonable method of gaining access to [the encrypted data] or making it intelligible is available'.[64] In England and Wales, then, satisfying the demands of proportionality – and therefore by extension the requirements of *RIPA* – depends on whether there are less intrusive alternative means available.

---

59 Ibid 3.39.

60 *Dudgeon v United Kingdom* (1981) 4 EHRR 149, 165.

61 Home Office, *Protected Electronic Information: Revised Code of Conduct* (August 2018), 3.41.

62 Ibid 3.43.

63 *Szabo and Vissy v Hungary* (2016) 63 EHRR 3, [73].

64 *R v S(F)* [2009] 1 WLR 1489, 1493 [12].

In Australia, the respective statutes require that a compelled production order be 'reasonable and necessary'.[65] That requirement broadly matches the proportionality requirement in *RIPA* and is consistent with the statement in *R v S(F)* that no 'alternative, reasonable' workaround should be available. As no Australian decision on compelled production orders has expressly discussed the reasonable and necessary requirement, guidance on what is reasonable and necessary can be obtained from the English approach to proportionality (as drawn from the *ECHR*). Further guidance is also available from the High Court, which has – albeit it in a different context – identified necessity as one of the elements of a proportionality test. In *McCloy v New South Wales*, the High Court noted that the proportionality question has three stages: is the measure (in this case the ability to obtain a compelled production order) 'suitable, necessary, and adequate in its balance'.[66] Suitability is concerned with whether the measure has a rational connection to the purpose that it seeks to achieve;[67] necessity asks if there are alternative means of equal efficacy that impose a lesser burden on the right in question while being obvious and compelling;[68] and the final stage requires a consideration of whether the statutory measure imposes an undue burden on the right in question in light of the importance of the purpose it seeks to achieve.[69] If those conditions are not satisfied, the statutory provision may be disproportionate and therefore invalid.[70] The first and third of those elements have already been addressed in Chapter 4. There, it was found that compelled production orders have been upheld by Australian courts. That requires those courts to have concluded that the compelled production order in question was suitable, necessary and adequate in balance. It is only as a result of recent statutory amendments that facilitate the use of the alternative workarounds, including the *Assistance and Access Act*, that the necessity element is required to be

---

65 *Crimes Act 1914* (Cth) 3LA(1); *Crimes Act 1958* (Vic) s 465AA(2), 465AAA(2); *Police Powers and Responsibilities Act 2000* (Qld) s 154(1)(a) (which has the necessary though not the reasonable requirement); *Criminal Investigation Act 2006* (WA) s 59(2)(d).

66 *McCloy v New South Wales* (2015) 257 CLR 178, 217 [79].

67 Ibid 217 [80].

68 Ibid 217 [81].

69 Ibid 218 [86].

70 Ibid 210 [57] referring to *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 568.

reconsidered.[71] The first and third elements, which are less dependent on the facts of each case, appear to be settled.

Thus far the following has been found. Both the English and Australian statutes provide that a compelled production order can only be granted where there is no alternative, less intrusive means of obtaining plaintext versions of the encrypted data. That obligation is expressed in the requirement that the compelled production order be a proportionate measure to the problem it seeks to resolve. To date, no decisions in England and Wales or Australia have been identified in which a court has held that compelled production orders are a disproportionate measure. Those decisions, however, have assumed the absence (or failed to consider the existence) of an effective, less intrusive alternative workaround. As a result of recent statutory measures in England and Wales and Australia, such alternative encryption workarounds may now be available to law enforcement officials.

Part 5.3.2 considers whether the alternative encryption workarounds identified in Part 5.2 are equally as effective as compelled production orders. Thereafter, Part 5.3.3 analyses whether, assuming they are as effective, they impose a lesser infringement on the rights of a suspect. If both of those conditions are satisfied, compelled production orders are likely to fail the proportionality requirement.

5.3.2 Are the workarounds capable of replacing compelled production orders?

Of the workarounds identified by Kerr and Schneier and authorised by the statutes discussed in Part 5.2.2, none of them are likely to work every time and their success rate is unclear.[72] They are not, however, mutually exclusive, so law enforcement can pursue any number of them simultaneously. Some of the workarounds, however, demand greater resources to pursue than others, potentially making them impractical for poorly funded law enforcement agencies.[73] This is true of attempts to exploit flaws in the

---

71 As the necessity element of the proportionality test is therefore the only element that remains in doubt when a compelled production order is sought, the necessity element effectively becomes the entirety of the proportionality test for such orders.

72 Kerr and Schneier, above n 3, 992.

73 Ibid 1014.

encryption software, for although law enforcement has had some success exploiting flaws, it has proven to be a costly exercise that not all police forces can afford. Cost concerns cannot be dismissed either, as the European Court of Human Rights has found that states have a wide margin of appreciation when allocating resources that are limited.[74] If, therefore, any of the alternative workarounds are deemed too costly to perform with regularity, that may preclude them from being considered a viable alternative. A further problem with exploiting software flaws is that it can be a time-consuming task, with success often taking months or years to achieve.[75] In certain instances, a delay of that nature may render this workaround unsuitable.

In addition to the broad concerns expressed above, the alternative workarounds may not be well suited to all the circumstances in which compelled production orders arise. In some of the cases in which compelled production orders have been sought, the encrypted electronic device was found without prior warning. For example, in the *Boucher* cases,[76] a traveller crossing the border was found with an encrypted laptop; in *Lenton v Western Australia*,[77] a person arrested for possession of illegal drugs was also found to have an encrypted smartphone with him, to which access was sought. This latter scenario, in particular, is likely to be encountered with some frequency by law enforcement officials, and it is one in which there will have been no prior opportunity for law enforcement to utilise certain of the powers contained in the *IPA* and *Assistance and Access Act*, including the power to place malware on a suspect's electronic device. Other investigatory techniques, most notably searches of file sharing networks, are also of no assistance in obtaining access to encrypted material on an electronic device that has already been seized or which has not downloaded material through such a network.

---

74 *McDonald v United Kingdom* (2015) EHRR 1, [55].

75 Manhattan District Attorney's Office, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (November 2017), 8-9 <https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf>.

76 *Boucher I* (D Vt, No 2:06-mj-91, 29 November 2007); *Boucher II* (D Vt, No 2:06-mj-91, 19 February 2009).

77 [2017] WASCA 224.

On those occasions, resort must be had to the other powers provided by these statutes, including the ability to hack the electronic device or to compel a telecommunications operator to remove encryption. The full scope of this latter power, however, may be limited. In a recent article, Koops and Kosta note that encryption can be implemented in different ways. They list four means by which encryption can occur: it can be centrally managed by a service provider who controls the encryption keys; a service provider may encrypt data that is in transit; a service provider may offer end-to-end encryption for the transmission of data; and end users may utilise their own end-to-end encryption.[78] Importantly, in the latter two methods, the telecommunications operator 'responsible for the channel [has] no capacity to decrypt communications'.[79] Where encryption occurs through one of those means, the power to compel a telecommunications operator to remove encryption is ineffective as that operator does not possess the decryption keys. This is reflected in the response by Signal, a popular messaging app renowned for the privacy protections it affords its users, to the passage of the *Assistance and Access Act*. In that response, Signal stated that it will be unable to comply with a request to remove encryption as it does not have access to the relevant decryption keys.[80] Apple, too, has stated that customer's encrypted material is 'out of our own reach' and that the only way to access it would be to build a backdoor into their software.[81] It is to be expected that other telecommunication operators may be in the same position.

An allegation by the telecommunications operator that it does not possess the decryption key may not be the end of the matter, however. In 2012, the Belgian Court of Appeal rejected an argument by Skype that it could not provide access to encrypted

---

78 Bert-Jaap Koops and Eleni Kosta, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 *Computer Law and Security Review* 890, 891.

79 Ibid.

80 Mallory Locklear, 'Signal Says It Can't Allow the Government Access to Users' Chats' (14 December 2018) *Engadget* <https://www.engadget.com/2018/12/14/signal-cant-allow-government-access/>. See also Ian Walden, 'The Sky is Falling! Response to the "Going Dark" Problem' (2018) 34 *Computer Law and Security Review* 901, 904 where the author notes that another messaging app, Telegram, made the exact same statements when Russian law enforcement required it to provide decryption keys.

81 Tim Cook, 'A Message to Our Customers' (16 February 2016) *Apple*, https://www.apple.com/customer-letter/>.

conversations because it did not possess the encryption key. The Court held that Skype should have designed its software to enable it to comply with orders to provide data in an unencrypted form.[82] Given the prohibition on inserting a systemic weakness, it is unclear how that ruling could apply under the *Assistance and Access Act*.

Ultimately, the efficacy of the alternative workarounds will vary from case to case, though in all cases any investigation can commence with the least intrusive workarounds, such as certain acts of finding or guessing the key. If those workarounds fail, in some, though not all, circumstances the remaining workarounds may also be available to use. That being so, depending on the facts of a matter there may be an equally efficacious means of decrypting encrypted data other than the use of a compelled production order. Next, Part 5.3.3 considers the second issue raised by the proportionality test: whether the alternative workarounds are more or less intrusive than compelled production orders.

5.3.3 The effect of alternative workarounds on the proportionality requirement

As set out in Part 5.3.1, for compelled production orders in England and Wales to satisfy the proportionality requirement they need to comply with the requirements of the right to privacy contained in Article 8 of the *ECHR*. In the recent decision of *Big Brother Watch v United Kingdom*,[83] the European Court of Human Rights was asked to determine whether large-scale electronic surveillance programs run by the United Kingdom, which involved the interception of electronic communications, infringed the rights contained in the *ECHR*, including the right to privacy under Article 8. In considering the proportionality element of Article 8, the Court noted that whether there were any alternative means of achieving the desired outcome was a relevant consideration, and that it was appropriate to consider the different levels of intrusion occasioned by alternative means of investigation.[84] It is that issue that is engaged by the emergence

---

82 Walden, above n 80, 904 where the author discusses the case *of Public Prosecutor's Office v Skype Communications SARL*, Court of Appeal of Antwerp, Case no 2016/CO/1006, 15 November 2017.

83 (European Court of Human Rights, First Section) Applications Nos 58170/13, 63422/14 and 24960/15, 13 September 2018.

84 Ibid [350], [384]-[386].

of alternatives to compelled production orders. In Australia, too, the element of necessity and alternative means is at the fore when considering proportionality. Under the test in *McCloy v New South Wales*, proportionality cannot be satisfied unless the action in question is necessary, which means that there is no alternative means of equal efficacy that imposes a lesser burden on the right in question while being obvious and compelling.[85] As identified in Part 5.3.2, the alternative workarounds may, depending on the facts, be an equally efficacious alternative to compelled production orders. The question thus becomes whether those alternative workarounds impose a lesser infringement on the rights in question than does a compelled production order. If they do, the necessity element of the proportionality analysis might not be satisfied.

5.3.3.1 The infringement of the right to privacy

The primary right implicated by a compelled production order is the privilege against self-incrimination. It is that right that stood at the heart of the challenge to *RIPA* in *R v S(F)*. It is, however, self-evident that the alternative workarounds impose less of an infringement on the privilege than do compelled production orders for the simple reason that none of the alternative workarounds implicate the privilege at all. Importantly, however, the privilege is not the only right that is engaged. So, too, as already noted, is the right to privacy, and it is arguable that some of the alternative workarounds result in a greater infringement of that right than do compelled production orders.

When a compelled production order is granted, the effect of that order is to give law enforcement officials access to the information protected by the encryption program. That can vary from a solitary file to the entire computer hard drive. Superficially, access to the entire hard drive will impose a significant burden on the right to privacy. However, that access will not be without limitations. Search warrants are required to be drafted narrowly and with a relatively high degree of specificity to ensure that they are proportionate.[86] That requirement ensures that the search warrant is drafted in a manner that excludes from the search any information that does not relate to the

85 *McCloy v New South Wales* (2015) 257 CLR 178, 217 [81].

86 *Niemietz v Germany* (1993) 16 EHRR 97, [37].

offence that is being investigated. Depending on how the search warrant is drafted, therefore, large parts of the unencrypted hard drive may remain off limits during the search. In this way the search warrant serves to provide as much protection as possible to the suspect's right to privacy.

By contrast, when the hacking powers are used to install a keylogger on the suspect's computer to capture the entry of his or her password while using the computer, that software will capture every keystroke that is entered prior to the entry of that password. If that password is not entered for a long period of time, extensive communications may be captured while awaiting the entry of that password. Those communications can include intimate emails, websites visited, passwords for those websites, including banking passwords, and any other work performed on the electronic device. It may include irrelevant information that would be excluded under a narrowly drafted search warrant. The scope of information that the keylogger obtains may therefore exceed that available through a compelled production order.

Moreover, a personal computer that is stored at home may be used by other members of the household. Keylogging software will capture their keystrokes just as they will those of the individual who is the target of the search warrant. Use of software of this nature may, therefore, have a greater impact on the private information of third parties than does a compelled production order. This is a relevant consideration. In *Szabo and Vissy v Hungary*, the European Court of Human Rights stated that

> Targeted surveillance of digital communication may constitute a necessary and effective measure for intelligence and law-enforcement entities when conducted in compliance with international and domestic law, but 'it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate'.[87]

That statement, made in respect of mandatory third-party data retention, recognises that the court should consider the effect of the measure in question not just on the

[87] *Szabo and Vissy v Hungary* (2016) 63 EHRR 3, OI-6 (concurring opinion of Judge Pinto De Albuquerque).

suspect (the needle), but also all third parties affected by the use of those powers (the haystack). In a similar vein, in *S v United Kingdom*, the Court stated that 'the interests of the data subjects and the community as a whole in protecting the personal data, including fingerprints and DNA information, may be outweighed by the legitimate interest in the prevention of crime' (emphasis added), though that determination required careful scrutiny.[88] In considering the intrusiveness of the statutory power in question, therefore, the effect of that power on the community as a whole was a relevant consideration to be weighed against the crime prevention purposes sought to justify it.

It is not only keylogging software that raises these concerns. The powers granted under the *IPA* and the *Assistance and Access Act* would enable other software programs, including those designed to extract information, to be inserted on the target computer. Such programs, in addition to searching the computer in question, may turn on and off cameras or microphones that are connected to the computer.[89] Like keylogging software, software programs of this nature are likely to have a greater effect on third parties than a compelled production order. Furthermore, the privacy implications in obtaining live sound and images from a computer or other electronic device arguably exceed those that accompany the search of a seized phone that has been decrypted through a compelled production order, particularly where the latter search is constrained by a narrowly drafted search warrant.

Though the respective rights intrusions are likely to differ on a case by case basis, the existence of a power to install keylogging or other software on a suspect's computer may result in a greater infringement of that suspect's right to privacy than would a compelled production order. Moreover, it arguably also exposes third parties to an increased risk that their right to privacy is infringed. It is notable, too, that while some of the alternative workarounds may impose a relatively substantial burden on the right to privacy, the English Court of Appeal in *R v S(F)* appeared to believe that compelled

88 *S v United Kingdom* (2009) 48 EHRR 50, [104].

89 See, eg, *In re Warrant to Search a Target Computer at Premises Unknown* 958 F Supp 2d 753 (SD Tex, 2013). See also *Szabo and Vissy v Hungary* (2016) 63 EHRR 3, [49].

production orders entailed at worst a relatively minor rights intrusion.[90] At an individual level, then, while compelled production orders implicate both the privilege and the right to privacy, and the alternative workarounds only implicate the right to privacy, the latter may, depending on the facts and the type of workaround, do so to a greater degree than do compelled production orders. It is to be expected, then, that determining which of a compelled production order or one of the alternative workarounds will impose the greatest rights infringement is a determination that will depend on the specific facts of each case.

5.3.3.2 The role of systemic risk considerations

It is not only at the individual level, however, that the intrusiveness occasioned by the competing measures is to be assessed. A further consideration demands attention: the systemic risk that certain of the workarounds pose for the security of electronic communications. The issue of systemic risk is relevant because of its consequences for third parties – which as identified above is a factor that needs to be taken into account. The systemic risk arises from the powers to compel decryption and to require telecommunications operators to assist in the exploitation of software vulnerabilities, particularly where those powers involve the creation of a software exploit. Encryption plays an essential role in modern society. More than one trillion encrypted transmissions occur over the internet daily, including online banking and credit card transactions;[91] critical elements of a country's infrastructure, such as powers grids and transportation, are protected by encryption.[92] Any actions that undermine the strength of encryption risk harm to those structures. The experiences of Ukraine – whose power

---

90 A view perhaps most clearly expressed in the Court's statement that a compelled production order only required the provision of the password and that no further questions could be asked: *R v S(F)* [2009] 1 WLR 1489, 1498 [25].

91 Apple, above n 92, 1.

92 Ibid; BSA, Submission No 48 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018, 2-3; Cisco, Submission No 42 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018, 4.

grid was hacked in late 2015, leaving almost a quarter of a million homes without power[93] – amply demonstrates the dangers attendant on weak electronic security.

Submissions to the Australian government during the consultation period for the *Assistance and Access Act* show that systemic risk was one of the, if not the primary, concerns raised by the technology industry. While the *Assistance and Access Act* expressly provides that the legislation cannot be used to create an exploit that causes systemic risk or vulnerability, many technology experts argue that the legislation nevertheless carries that very risk. At the heart of the criticism is the definition adopted in the legislation that a systemic weakness is one that 'affects a whole class of technology but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person'.[94] That definition is intended to allow law enforcement to insert 'a weakness or vulnerability in a particular service, device or item or software on a case-by-case basis'.[95] However, the idea that something can only be a systemic weakness if it affects the entire system is disputed, as a technique that is devised to gain access to a solitary device can be used many times over, thereby threatening the security of the system.[96]

Where tools are created that allow the insertion of a weakness on specific devices or software, systemic security is no longer based solely on the strength of the encryption algorithm but also on the ability of the creator of that weakness to ensure that the exploit is not made available more widely. That there have previously been leaks of

---

93 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (3 March 2016) *Wired* <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

94 *Telecommunications Act 1997* (Cth) s 317B as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

95 Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 17 [55].

96 Internet Architecture Board, Submission No 23 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 October 2018, 1-2; Apple, above n 91, 3; Mozilla, Submission No 46 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018, 3; Cisco, above n 92, 7; Australian Information Industry Association, Submission No 39 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018, 4.

United States government hacking tools raises doubts about any government's ability to maintain the secrecy of those tools.[97] Indeed, one of the largest cyberattacks in recent history, the Wannacry ransomware, is strongly believed to have utilised a hacking toolkit created by the United States National Security Agency which made its way into the wider community.[98] Unsurprisingly, some experts have questioned whether it is ever possible to create a power to compel decryption or to exploit a software weakness without inevitably creating a systemic weakness.[99]

There are, finally, reasons to doubt that some of the limitations imposed on the use of these powers will protect the security of electronic communications from harm. For example, both statutes limit the use of these measures to only those actions that are reasonably practicable.[100] However, what is reasonably practicable for the telecommunications operator to perform says nothing of whether those actions may create a security risk. Furthermore, though demands may only be made of telecommunications operators once the impact of those demands on cybersecurity have been considered (amongst other competing interests),[101] all that is required is that cybersecurity be considered. Neither statute precludes actions that may pose a risk to cybersecurity, and, as the definition of systemic risk in the *Assistance and Access Act* shows, what constitutes a security risk is highly contentious.

---

97 See, eg, Greg Miller and Ellen Nakashima, 'Wikileaks Says It Has Obtained Trove of CIA Hacking Tools' (7 March 2017) *The Washington Post* <https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.5642354ffb3f>.

98 Chris Culnane and Vanessa Teague, Submission No 16 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, September 2018, 4.

99 Massachusetts Institute of Technology: Internet Policy Research Initiative, Submission No 32 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 11 October 2018, 6-7 where the authors note that it remains unclear whether it is possible to create a system that remains secure while allowing third-party access to the system.

100 *IPA* s 128(5); *Telecommunications Act 1997* (Cth) ss 317JAA, 317P and 317V as amended by the *Assistance and Access Act* sch 1 pt 1 item 7 (where the requirement imposed needs to be reasonable and compliance with it practicable and feasible).

101 *IPA* s 2(2)(c); *Telecommunications Act 1997* (Cth) ss 317JC, 317RA and 317ZAA as amended by the *Assistance and Access Act* sch 1 pt 1 item 7.

It is not possible to here give a definitive answer as to which of compelled production orders or the alternative workarounds is the more intrusive means of accessing encrypted material. Certain of the workarounds, like guessing or finding the password, or accessing the material while it is being used, will impose less of an infringement on the rights of a suspect than would a compelled production order; others, such as the hacking powers, may impose a greater infringement. Each determination will need to be made by the court hearing the application based on the specific facts of the matter.

The analysis in this Part 5.3 suggests that both compelled production orders and the alternative workarounds may be available to law enforcement officials depending on the circumstances of the investigation, and that a proportionality assessment will determine which must be used in each case. However, as the proportionality assessment may preclude the granting of a compelled production order in certain circumstances, consider must be given to what that means for the scope of the privilege. That question is considered in Part 5.4.

5.4 ALTERNATIVE ENCRYPTION WORKAROUNDS AND THE SCOPE OF THE PRIVILEGE

5.4.1 Alternative encryption workarounds vary the scope of the privilege

The previous Parts to this Chapter established the following. Relatively recent legislative measures in England and Wales and Australia have facilitated the use of alternative encryption workarounds, like hacking, that can enable law enforcement officials to obtain access to plaintext versions of otherwise encrypted data. Depending on the circumstances, those alternative workarounds can be as effective as compelled production orders. Furthermore, and once more depending on the circumstances, they may impose a lesser infringement on the rights of a suspect than would a compelled production order. This is significant because of the requirements imposed by the English and Australian statutes when a compelled production order is sought, one of which is that compelled production orders must be a proportionate response to the problem caused by the encryption software. For the demands of proportionality to be satisfied, there must be no alternative means of accessing the desired data that is equally effective while imposing a smaller infringement on the rights of the suspect. In certain circumstances, the alternative encryption workarounds will be both equally effective

and a lesser burden. On those occasions, they are therefore required to be used instead of a compelled production order. This finding has two consequences.

First, depending on whether a compelled production order or an alternative workaround is the least intrusive means of accessing plaintext data, either the privilege against self-incrimination or the right to privacy will regulate the search in question. If a compelled production order is the least intrusive method, and is therefore a proportionate response, that order can be made under the relevant statute and the privilege will regulate the conduct of that search. In England and Wales, it will do so by ensuring that the essence of the privilege is not destroyed by the granting of the order. By contrast, if an alternative encryption workaround is the proportionate measure then the right to privacy will regulate a search using that workaround. The proportionality mechanism thus ensures that the least intrusive method is used to obtain the plaintext while also limiting the overlap that may occur between the protection offered by the privilege and the right to privacy, with each workaround (including compelled production orders) being regulated by one of the rights, but not both.

The second consequence flows from the first. When the search uses one of the alternative encryption workarounds, which is regulated by the right to privacy, the privilege is given the full scope of its operation by allowing it to preclude the use of a compelled production order (until such time as the alternative encryption workarounds are either no longer equally as effective or they impose a greater infringement on the suspect's rights). However, at the point that a compelled production order becomes the least intrusive means, the operation of the privilege will be restricted to enable such an order to be granted. That is: for as long as there is another effective mechanism by which law enforcement can access the encrypted material which imposes a lesser infringement on the suspect's rights than does a compelled production order, the privilege serves to preclude the granting of such an order. However, once there are no less intrusive alternative workarounds the privilege is no longer able to preclude the granting of a compelled production order as that order is now a proportionate response in the circumstances. In this latter scenario the privilege is given a more limited scope than when other less intrusive workarounds are available. The ability of the privilege to

prevent the granting of a compelled production order, what this thesis has considered to be the scope of the privilege, is therefore dependent on the existence of the alternative encryption workarounds.

It is important to remember that the reason that the privilege is able to contract in this manner (when compelled production orders are the least intrusive option) is because the English and Australian legislatures have abrogated the privilege in only those circumstances where it is the least intrusive means through which to access the plaintext data. If an alternative encryption workaround is available that imposes a lesser rights infringement, the conditions for the statutory abrogation of the privilege are not met and the compelled production order can no longer be granted as it now falls within the scope of the unabrogated privilege. Thus, the mechanism by which the privilege's scope varies is the operation of the act of abrogation. This raises the possibility that depending on how one interprets the effects of that act of abrogation, one may question whether the scope of the privilege does in fact vary.

It may be argued that there are two different understandings of what abrogation means for the privilege.[102] In the first, the act of abrogation alters the outer boundaries of the privilege; in the second, the outer boundaries of the privilege remains unaltered but the act of abrogation means that a particular search, though falling within the scope of the privilege, can nevertheless be performed because the privilege is held in abeyance. For three reasons, this thesis will adopt the first understanding – that the scope of the privilege is affected by the abrogation of the privilege. First, and most importantly, this thesis has used the word 'scope' in a particular way in the preceding Chapters. Scope, in this thesis, means the boundaries of the privilege as determined by judicial decisions. Those decisions are the sole determinant of the scope of the privilege. Court decisions on whether or not the privilege applies to a particular search or order take into account – as they must – the act of abrogation in determining the applicability of the privilege to that search or order. In so doing, their findings that the privilege has been abrogated of

[102] It is to be emphasised that these differing understandings, even if they exist, have no effect on the operation of the statutory provisions in question. They are, rather, simply two competing conceptions of how the abrogation may operate.

necessity are also findings that the act of abrogation has altered the scope of the privilege – for the scope of the privilege is (for purposes of this thesis) determined by whether courts have found it applicable to a particular search or order.

Secondly, while there are cases that give express voice to the first understanding, none of the cases considered in this thesis have explicitly supported the second understanding. In respect of the first understanding, in *Brown* the Privy Council considered the application of the privilege to certain motor vehicle reporting obligations. In upholding the validity of the abrogating provisions, Lord Hope held that 'it is reasonable to conclude that the limited modification which section 172(2)(a) makes…to the right not to incriminate oneself is compatible with the right to a fair trial' (emphasis added).[103] On this view, then, the privilege itself is modified: its scope altered. This same view has been endorsed in subsequent cases.[104] In none of the cases considered in this thesis was similar support found for the second understanding. In *Luppino (No 1)*, for example, the Court recognised that absent an act of abrogation, the privilege would apply to compelled production orders.[105] Its subsequent decision in *Luppino (No 2)* recognised that as a result of that act of abrogation, the privilege no longer operated to exclude evidence obtained as a result of an order that complied with s 3LA of the *Crimes Act 1914* (Cth).[106] What the *Luppino* cases – and other cases like it – do not expressly state, however, is that by abrogating the privilege its scope remains unchanged though it is held in abeyance. In the *Luppino* cases it is not inconsistent with the Court's decision to say that the act of abrogation varied the scope of the privilege, just as it is not inconsistent to say that the scope of the privilege has not been varied but is being held in abeyance. They are merely two ways of describing the same outcome, neither of which is explicitly endorsed in the case. Consider, too, cases such as *Loges v Martin*, in which the Court found that the privilege 'has necessarily been extinguished'.[107] To say that the privilege has been extinguished is arguably more

103 *Brown* [2003] 1 AC 681, 723.

104 See, eg, *R v S(F)* [2009] 1 WLR 1489, 1494 [17] (where the Court noted that the privilege may 'limit, amend or abrogate the privilege in specified circumstances' (emphasis added)).

105 *Luppino (No 1)* [2018] FCA 2106.

106 *Luppino (No 2)* [2019] FCA 1100.

107 *Loges v Martin* (1991) 13 MVR 405, 409.

consistent with the first understanding – that the scope of the privilege has been varied – than it is with an understanding that the scope of the privilege is unvaried (notwithstanding its extinguishment) but that it is being held in abeyance.

Thirdly, there are reasons to be dissatisfied with the second understanding. When English courts and the European Court of Human Rights assess the impact of an act of abrogation on the privilege, they ask whether the abrogation has destroyed the essence of the privilege. If it has, then the admission in court of evidence arising from that order will constitute a breach of Article 6 of the *ECHR* and the right to a fair trial. In *Brown* and *O'Halloran and Francis*, for example, the act of abrogation did not destroy the essence of the privilege and therefore the evidence obtained through the order in question was admissible. In cases such as those, the second understanding – that the scope of the privilege is unchanged, but it is held in abeyance to allow the order to be made – appears inconsistent with the outcome in those cases. This is so for at the point that the court makes its ruling, it grants the order and allows the evidence in question to be obtained, a tangible outcome that means that the privilege has been unable to operate in respect of an order to which it has previously been understood to apply. That is, when the principle that the essence of the privilege must not be destroyed is applied on the facts, it results in the privilege being given a reduced field of operation in those situations where the essence is not destroyed. In the terminology used in this thesis: it results in a reduced scope for the privilege. To argue that despite this outcome the scope of the privilege remains unchanged (it being merely suspended, as it were) is to miss the point that whatever its theoretical scope may be, it has been unable to prevent the admission of evidence obtained through the order in question.

The result of the above is that to the extent that these two understandings can be said to exist, the first of them – that abrogation varies the scope of the privilege – is consistent with the understanding of the scope of the privilege that has been applied in this thesis and is, therefore, the one adopted in this Part.

The preceding analysis has revealed the following. In England and Wales and Australia, the existence of alternative workarounds can affect the scope of the privilege.

Specifically: where an equally effective alternative is available which imposes less of an infringement on the rights of the suspect than does a compelled production order, the use of the compelled production order would be disproportionate and, therefore, outside the scope of the compelled production order legislation. By virtue of falling outside the legislation, the privilege is not abrogated but instead is given its full scope. By contrast, if the compelled production order is a proportionate measure by virtue of there being no equally effective and less intrusive alternative encryption workaround, the statutory abrogation of the privilege is effective and the compelled production order may be made. In this scenario the scope of the privilege has been limited.

The above outcome raises the question of whether the scope of the privilege varies in the same manner in Canada and the United States – being jurisdictions without specific statutory provisions dealing with compelled production orders. The answer is no. In the United States, the applicability of the privilege is determined by the act of production and foregone conclusion doctrines: when the latter is satisfied, the privilege is not engaged; when its conditions are not met, the privilege operates to bar the granting of a compelled production order. Whether there exists a less intrusive but equally effective alternative workaround is irrelevant to the foregone conclusion doctrine, with the result that the existence of such an alternative has no effect on the scope of the privilege.

In Canada, too, the existence of alternative workarounds has no effect on the scope of the privilege. It is the absence of an alternative workaround that broadens the scope of the privilege in England and Wales and Australia, yet in Canada the privilege has been effective at prohibiting the granting of a compelled production order even where no alternative workarounds exist. Should an alternative workaround become available, it will not serve to expand the scope of the privilege – not least because its existence lessens the need for the compelled production order.

5.4.2 The response to alternative encryption workarounds is a pragmatic one

By adopting a mechanism that ensures that the least intrusive means is used to access a plaintext version of encrypted data, the English and Australian statutes have adopted a pragmatic response to the problem of encrypted data, one that seeks to give the

privilege the broadest scope possible while still enabling law enforcement to gain access to plaintext versions of encrypted material that they have lawfully seized. In adopting this approach those statutes have followed a path consistent with earlier judicial decisions that have adopted a similarly pragmatic approach to the privilege.

The adoption of a pragmatic approach of this nature is a relatively long-standing feature of the privilege. Writing in *Evidence in Trials at Common Law*, Wigmore argued that the privilege required a restrictive interpretation in order to prevent the scope of the privilege extending too far. If left unrestrained, he said, an accused person could argue that by being compelled to stand trial his right to the privilege is being infringed as the trial requires him 'to expose his features to the witnesses for identification', a compelled self-incriminatory act.[108] Similar sentiments have long been expressed by the courts, including in respect of the related orders that have been considered in this thesis. In the United States, in holding that a motor vehicle reporting obligation did not infringe the privilege, Burger CJ stated that the significance of the privilege was not such that it compelled 'substantial sacrifices in the efficient pursuant of other governmental objectives';[109] and in *Schmerber*, Brennan J noted that 'the privilege has never been given the full scope which the values it helps to protect suggest'[110] – a nod to the pragmatic manner in which the privilege has been applied.

The application of the privilege in the four jurisdictions in respect of the related orders further demonstrates the role played by pragmatic considerations. In Canada, the public importance in allowing DNA samples to be compelled (the epitome of a pragmatic consideration) was a key factor in finding that compelling such samples was lawful;[111] the English House of Lords relied upon the public interest in holding that motor reporting obligations did not infringe the privilege;[112] and in Australia, motor vehicle reporting obligations were permissible due to their importance to the investigation and

---

108 John Wigmore, *Evidence in Trials at Common Law* (McNaughton rev, vol 8, 1961) 386.

109 *Byers* 402 US 424, 448 (1971).

110 *Schmerber* 384 US 757, 762 (1966).

111 *R v B(S.A.)* [2003] 2 SCR 678, [60]. Note, too, that the public interest was considered by the Court in *Talbot* when asked to grant a compelled production order: *Talbot* 2017 ONCJ 814, [38].

112 *Brown* [2003] 1 AC 681.

prosecution of driving offences.[113] In each of those instances the role played by pragmatic considerations is consistent with Ashworth's argument that the privilege can be limited where a 'considered exception' is identified.[114]

Arguably one the most prominent examples of the pragmatic streak that runs through the privilege is the foregone conclusion doctrine in the United States. In circumstances where an act of production concedes the existence of the evidence in question, its possession by the suspect or if it authenticates the evidence, that act of production has a communicative aspect that engages the privilege. However, if the state already knows that the evidence exists, that the suspect possesses it and the state is able to authenticate it by independent means, the foregone conclusion doctrine is engaged and the privilege no longer applies. It is significant that even where the foregone conclusion doctrine is satisfied, the state's knowledge alone is insufficient to obtain a conviction; and if the evidence that is sought is a written document, the state's knowledge does not need to extend to knowledge of the contents of that document. Therefore, the foregone conclusion doctrine can be satisfied in circumstances where the suspect is compelled to produce self-incriminating evidence that the state is otherwise unable to obtain and which may be essential to a successful prosecution. This outcome appears to reflect a concession to pragmatic considerations about the desired scope of the privilege rather than one of principle.

5.5 CONCLUSION

Recent legislative developments have facilitated the use of alternative encryption workarounds in England and Wales and Australia. As those workarounds have become more accessible, so they have affected the scope of the privilege when applied to compelled production orders. Specifically, the existence of an equally effective and less intrusive alternative workaround allows the privilege to assume its full scope when a compelled production order is sought, in so doing precluding the making of such an order.

---

113 See, eg, *R v Hooper* (1995) 64 SASR 480.

114 Andrew Ashworth, 'Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism?' (2008) 30 *Cardozo Law Review* 751, 764.

The introduction of the alternative encryption workarounds has not, however, removed the need for compelled production orders. This is reflected most clearly in the *Assistance and Access Act*, which strengthened the ability of compelled production orders to operate effectively at the same time as it enabled the use of the alternative encryption workarounds. The existence of these alternative workarounds has not, and is not intended to, replace compelled production orders or the statutes that provide for them in England and Wales and Australia. Rather, it appears to be the case that compelled production orders and the alternative encryption workarounds are intended to operate in a complementary manner. As the alternative workarounds also contain a proportionality requirement – meaning that they are not an appropriate mechanism in circumstances where compelled production orders are less intrusive – it seems tolerably clear that the legislatures intended for law enforcement to use whichever of the mechanisms is the least intrusive on the facts of each individual matter.

The result is that the operation of the privilege in England and Wales and Australia takes on a fluid form. Where an alternative workaround that is less intrusive is available to law enforcement officials, the use of a compelled production order will be prohibited by the operation of the privilege (as any compelled production order would fall outside the scope of the respective statutes authorising such orders). By contrast, where no such alternative is available, the requirements of the respective statutes are met causing the privilege to be abrogated and its scope reduced accordingly to allow the order to be made. In this fashion the privilege expands and contracts to ensure that it is only infringed when there is no alternative, less intrusive means of gaining access to the encrypted material.

CONCLUSION

THESIS QUESTIONS AND METHODOLOGY

As the use of encryption to protect smartphones, computers and other electronic devices has increased in recent years, so have law enforcement concerns that its use may prevent them from accessing the encrypted data. An early response by law enforcement officials when confronted with this situation was to seek a compelled production order. A common defence to such an application is to argue that to compel a person to provide a password is to infringe that person's privilege against self-incrimination. Over the previous five Chapters this thesis has considered whether compelled production orders fall within the scope of the privilege, both in Australia and the comparator jurisdictions. The scope of the privilege, as described in this thesis, means those circumstances in which courts have applied the privilege to related orders.

Answering that primary question has entailed addressing several further questions, including whether court decisions on compelled production orders have been consistent with earlier decision on related orders; how courts have weighed the competing interests of the suspect in preserving the privilege and the public in having criminal offences investigated; what role abrogation plays in determining whether the privilege can prevent the granting of a compelled production order; and, lastly, whether the increasing availability of alternative encryption workarounds has an effect on the applicability of the privilege to compelled production orders.

As the primary concern of this thesis is with how this issue is resolved in Australia, what have the previous five Chapters revealed about the scope of the privilege in Australia, whether compelled production orders fall within that scope and how Australia legislatures and courts have responded to requests for compelled production orders?

COMPELLED PRODUCTION ORDERS IN AUSTRALIA

In Chapter 1, an examination of how the privilege has been applied to related orders in Australia revealed that the privilege is engaged by one of the closest comparable orders: single question reporting obligations such as those applied to motor vehicle drivers.

Notably, however, while motor vehicle reporting cases are closely related to alphabetic and numeric passwords, for which a compelled production order requires the production of a solitary piece of information (the password), biometric passwords require the compelled production of that biometric feature. In that situation, how Australian courts have dealt with bodily samples is a closer analogue. Chapter 1 revealed that Australian courts have consistently held – as have the courts of England and Wales and the United States – that bodily samples do not fall within the scope of the privilege.

With regard to alphabetic and numeric passwords, the consequences of motor vehicle reporting obligations engaging the privilege are avoided through the abrogation of the privilege in respect of such obligations. In Chapter 2, it was discovered that, despite the absence of an express abrogation in the relevant statutes, courts had read in such an abrogation by necessary implication. Importantly, in determining whether such abrogation had occurred courts did not limit themselves to considering whether a failure to abrogate the privilege would undermine the purpose of the statutory provision; they also considered factors typically utilised in a balancing exercise to determine the appropriateness of such abrogation. For example, in *R v Hooper* the number of questions that could be asked and the public interest in investigating criminal offences were both relied upon in holding that abrogation was to be implied.[1]

The weighing up of competing factors in that manner was a process adopted in each of the other three jurisdictions, though with a notable difference. While Australian courts weighed the competing interests to determine if abrogation had occurred, in Canada, England and Wales and the United States that balancing – which relied upon the same factors – occurred to determine whether the privilege was engaged in the first place.

With the scope of the privilege and the availability of an act of abrogation having been established in Chapters 1 and 2, Chapter 4 revealed that cases concerning compelled production orders have been resolved in a manner consistent with the outcomes

1 *R v Hooper* (1995) 64 SASR 480, 486.

identified in those earlier Chapters. The clearest statements on the applicability of the privilege to alphabetic and numeric passwords were contained in the recent decisions in *Luppino*, in the first of which the Federal Court found that absent an act of abrogation the privilege was engaged by such an order.[2] In that decision, White J held that the privilege would be infringed by requiring the suspect to provide evidence 'out of [his] own mouth' or by requiring him to disclose information that 'could be used to implicate him in criminal offences'.[3] Importantly, both compelled production orders and motor vehicle reporting obligations remain lawful as a result of the abrogation of the privilege in respect of both measures. For the former, that act of abrogation occurs through statutory provisions at the state and federal level which address this specific issue.

Notably, too, the abrogation of the privilege in respect of motor vehicle reporting obligations and compelled production orders occurs after weighing the interests of the suspect against the public interest. For motor vehicle reporting obligations, that weighing exercise was performed by the court; for compelled production orders, it occurred at the legislative level. For example, the statement of compatibility to the relevant provision in the Victorian statute justified the abrogation of the privilege and consequent limitation of its scope on the basis of the serious nature of the offences being investigated and the problems that would arise if law enforcement was stymied in their investigations.[4] As already noted above, similar factors were relied upon to find that motor vehicle reporting obligations abrogated the privilege. In both instances, those factors were relied upon for a finding that the privilege had been abrogated and its scope accordingly limited to allow the order in question to be made.

With regard to biometric passwords, no Australian cases were identified that expressly dealt with them.[5] While it is not therefore possible to say with certainty that biometric passwords do not engage the privilege, the findings from Chapter 1 reveal that the

---

2 *Luppino (No 1)* [2018] FCA 2106.

3 Ibid [28], [32].

4 Victoria, *Parliamentary Debates*, Legislative Assembly, 5 August 2015, 2417 (Martin Pakula, Attorney-General).

5 Though *Luppino (No 2)* [2019] FCA 1100 makes clear that the relevant statutes can compel the production of a biometric feature to unlock an encrypted device.

privilege is not ordinarily applied to bodily features – a finding that the United States and England and Wales also made. This strongly suggests that the compelled production of a biometric feature to decrypt an encrypted device would not infringe the privilege. To use the words of White J, there is no 'evidence out of the plaintiff's own mouth' with which the plaintiff could be convicted.[6]

The above findings dispose of the primary question asked in this thesis: whether compelled production orders infringed the privilege in Australia, and whether the manner in which Australian courts have addressed this issue is consistent with how they dealt with the privilege in respect of related orders. The section below reviews how the three remaining jurisdictions addressed the issue of compelled production orders and what lessons, if any, Australia can draw from their responses.

FINDINGS FROM THE COMPARATOR JURISDICTIONS

Before a court can consider whether the privilege applies to a compelled production order, it must ask whether there is a statutory power authorising the issue of such an order. The Canadian decisions considered in Chapter 3 highlight the importance of this requirement. In several of those decisions, the absence of an empowering provision played a role in the courts' decisions to refuse the compelled production order. In *Boudreau-Fontaine*, arguably the leading case in that jurisdiction, the Court found that the provisions of the *Criminal Code* relied upon did not support the order that was sought.[7] This finding appears consistent with Australian decisions, which have suggested that compelled production orders can only be made within the parameters of the specific statutory provisions authorising such orders.[8]

Canada also stands as an example of the difficulties that arise when abrogation of the privilege (without a commensurate grant of immunity) is not possible. As abrogation in that jurisdiction is, for practical purposes, not feasible, whether a compelled production

---

6 *Luppino (No 1)* [2018] FCA 2106, [28].

7 *Boudreau-Fontaine* 2010 QCCA 1108, [46]. Note, however, that at least one later decision found that such orders could be authorised under a different provision (though the privilege remained an obstacle to the granting of the order): *Talbot* 2017 ONCJ 814, [15]-[16].

8 See, eg, *Luppino (No 1)* [2018] FCA 2106; *R v Ford* [2017] QSC 205.

order can be granted is determined solely by whether such an order falls within the existing scope of the privilege. There is no additional flexibility that comes from an ability to abrogate the privilege in appropriate circumstances. Chapter 1 showed that in Canada, the scope of the privilege is determined by weighing the interests of the suspect in preserving the privilege against the interests of society in investigating criminal activity; furthermore, court decisions in respect of related orders revealed that the importance of preserving the privilege routinely outweighed society's interest in the ability of law enforcement to perform the search in question. Consistently with those findings, when confronted with compelled production orders Canadian courts have performed the same weighing exercise and reached the same conclusion: the interests of society in allowing such searches does not supersede the suspect's interest in protected the privilege. England and Wales and Australia came to a different conclusion.

In a further example of Canada's exceptionalism, there is some case support for the finding that biometric passwords also infringe the privilege[9] – a finding not made in any of the other jurisdictions. This finding, though, is consistent with Supreme Court dicta that the privilege is engaged in any circumstance in which a suspect is compelled to 'participate in the creation or discovery of self-incriminating evidence in the form of confessions, statements or the provision of bodily samples'.[10] That position grants a far broader remit to the privilege than do the other jurisdictions.[11] Whether Canada can maintain this approach in future years is an open question, however. If, as law enforcement alleges, the challenges imposed by encryption continue to grow, it is possible that there may become a point at which the public interest in granting law enforcement access to encrypted material outweighs the individual's interest in the privilege. Such an outcome would, however, entail a not inconsiderable shift from the established scope of the privilege, and until such time as such a shift occurs compelled production orders will remain unlawful in Canada.

---

9 *Re Impression Warrant Application (s. 487.092)* 2016 ONCJ 197, 129 WCB (2d) 485, [15].

10 *Stillman* [1997] 1 SCR 607, [73].

11 Though it should be noted that the European Court of Human Rights, in its inconsistent approach to the scope of the privilege, has at times given the privilege a broad scope too. See, eg, *Jalloh* (2007) 44 EHRR 32.

The United States is the second jurisdiction in which abrogation of the privilege without commensurate immunity is prohibited. As a result, like Canada, a finding that the privilege applies to compelled production orders is decisive in prohibiting the granting of such an order. Where the United States stands apart from Canada (and Australia) is its use of the act of production and foregone conclusion doctrines to determine whether compelled production orders (in respect of alphabetic and numeric passwords) fall within the scope of the privilege. The findings in Chapter 3, however, reveal difficulties with the application of that doctrine to such orders. The act of production and foregone conclusion doctrines were a response to demands for pre-existing documentary evidence that was itself incriminating. Though such documentary evidence is superficially similar to a pre-existing password, the password itself is not ordinarily incriminating though it is used to reveal incriminating evidence. That distinction is the reason for the existence of the competing control and contents tests when applying the foregone conclusion doctrine.

Under the control test, the focus is on knowledge of the password; under the contents test, the knowledge that is critical is knowledge about the contents of the encrypted device. It is the adoption of the contents test, it was argued in Chapter 3, that has distorted the application of the foregone conclusion doctrine to compelled production orders. Properly understood, the 'document' that is sought in a compelled production order scenario is the password, not the encrypted documents. Law enforcement already possess the encrypted documents – what they seek is the key to unlock them. So understood, the foregone conclusion doctrine can be satisfactorily applied to compelled production orders, though there remains substantial opposition to adopting this understanding.

Chapter 3 further revealed that when the contents test is used, a formidable evidentiary burden is imposed on the applicant for a compelled production order, a burden that far exceeds that which exists in Australia and England and Wales. Under the contents test, the applicant must show that it knows what is contained on the encrypted drive with 'reasonable particularity', an onerous requirement. By contrast, the control test merely requires probable cause to believe there was evidence on the encrypted device, the

same standard imposed on an applicant for a search warrant. That standard correlates to the Australian standard of reasonable grounds for suspecting that evidentiary material will be found, and is therefore likely to be satisfied by evidence that the electronic device was found in the suspect's possession or under his or her control.[12] As a result of the contest between the control and contents tests, the findings from the United States provide little guidance for Australian courts. The reliance on the act of production doctrine appears to have caused more confusion than clarity, and the use of the contents test entails the imposition of an evidentiary burden that has not been adequately justified and which would be out of place in Australian jurisprudence.

The difficulties with the act of production doctrine do, however, give rise to one unanswered question. Chapter 1 found that early Supreme Court decisions on bodily evidence (such as blood samples) held that the taking of such samples (and the finding that their taking fell outside the scope of the privilege) was justified after weighing the competing interests of society and the individual.[13] Similarly, before finding that the privilege was not implicated by certain motor vehicle reporting obligations, the Supreme Court first noted that the applicability of the privilege should be 'resolved in terms of balancing the public need on one hand, and the individual claim to constitutional protections on the other; neither interest can be lightly treated'.[14] There is, therefore, precedent for determining the scope of the privilege by reference to a weighing of interests.

While the act of production doctrine was established after those early cases were decided, its existence does not appear to preclude the use of a weighing exercise to determine whether compelled production orders infringe the privilege, just as was done for blood samples and certain reporting obligations. Such an exercise has been adopted by each of the other three jurisdictions, and it is notable that the United States has refused to engage in a similar exercise, notwithstanding its earlier use for certain related

12 As is the case in Australia. See, eg, *Garbellini v The State of Western Australia* [2017] WASC 93, [9]; *The State of Western Australia v Doyle* [2017] WASCA 207, [7].

13 See, eg, *Breithaupt* 352 US 432 (1957).

14 *Byers* 402 US 424, 427 (1971).

orders. It is unclear why this is the case, and the apparent failure to utilise such a weighing of interests test has encouraged the confusion that has resulted from the competing contents and control tests.

One finding from the United States that is relevant to Australia is its approach to biometric passwords. In a leading decision from the Court of Appeal of the Eleventh Circuit, the Court noted that the privilege is not engaged through the compulsion of a merely physical act that does not require the defendant to use the contents of his mind.[15] Biometric passwords appear to fall squarely within that description, a position that has been accepted by the courts of the United States with near unanimity. Though no Australian court has directly addressed this issue, it is to be expected that it will adopt the same position as the United States. Australia, like the United States, accepts that the privilege is not engaged by purely physical acts, and that finding must lead to the conclusion that a biometric password – which requires no cognitive act from the suspect – falls outside the scope of the privilege.

Lastly, England and Wales is the jurisdiction most closely aligned with Australia, and the findings from Chapters 1, 2 and 4 reveal overwhelming similarities in the way the two jurisdictions have treated compelled production orders and the privilege more generally. In both jurisdictions, the privilege can, and has been, abrogated to allow compelled production orders to be made. In England and Wales, that act of abrogation is subject to the requirement that the essence of the privilege not being destroyed – a requirement identified in Chapter 2. If it is, evidence so obtained will be inadmissible in court. While Australia does not explicitly follow the same approach, the apparent use of a balancing exercise to justify the abrogation of the privilege to allow compelled production orders (just as a balancing exercise was earlier used to uphold motor vehicle reporting obligations) is evidence of a similar, though less strict, approach.

Arguably one of the most instructive lessons from England and Wales concerns its rejection of the concept of the will of the accused, which has been relied upon by the

---

15 *In re Grand Jury Subpoena Duces Tecum* 670 F 3d 1335, 1345 (11th Cir, 2012). The Court noted the 'famous' example of the key to the lock of a safe as an example of such compulsion.

European Court of Human Rights to determine whether there has been an infringement of the privilege. As Chapter 1 revealed, early decisions of the European Court of Human Rights spoke of how the privilege was intended to ensure that evidence was not obtained in contravention of 'the will of an accused person to stay silent'.[16] Importantly, those early decisions recognised that evidence having an independent existence did not implicate the will of the accused.[17] With time, however, the European Court of Human Rights appears to have given greater weight to the will of the accused than to whether the evidence has an independent existence. That development has led to two consequences: first, the jurisprudence of the European Court became inconsistent as decisions were handed down in which evidence having an existence independent of the suspect was nevertheless found to have fallen within the scope of the privilege;[18] and, secondly, as England and Wales rejected reference to the will of the accused, its understanding of the privilege continued on a clearer path than that applied by the European Court of Human Rights, one that also grants the privilege a slightly narrower scope. England and Wales, in focusing on whether the evidence had an independent existence, has adopted the same standard as that used in Australia, where courts have spoken of the privilege not applying to evidence that already exists.[19]

England and Wales, then, stands as an endorsement of the Australian approach. Chapter 1 revealed a broadly shared understanding of the scope of the privilege with similar outcomes from the weighing of competing interests test; Chapter 2, a shared ability to abrogate the privilege without commensurate immunity in certain circumstances; Chapter 4, the use of similar statutory provisions to govern the granting of compelled production orders; and Chapter 5, the imposition of a proportionality requirement that ensures that compelled production orders can only be used when there is no less intrusive and equally effective alternative encryption workaround available. It is this last element, the role played by alternative encryption workarounds, that stands as one of the most important features of the Australian and English response

16 See, eg, *Saunders* (1997) 23 EHRR 313, [76].
17 Ibid [76].
18 See, eg, *Jalloh* (2007) 44 EHRR 32.
19 See, eg, *King v McLelland* [1974] VR 773, 777.

to compelled production order. It is, furthermore, a feature that arguably ensures that the application of the privilege to compelled production orders is done in a manner that is consistent with how the privilege has been treated in the past in respect of related orders.

THE ROLE OF ALTERNATIVE ENCRYPTION WORKAROUNDS

The preceding five Chapters reveal how the privilege has long been spoken of in two competing voices. With the first, the importance of the privilege is acknowledged. Thus, the Australian High Court has spoken of the privilege as being a 'deeply engrained' right,[20] one that serves as a 'fundamental bulwark of liberty'.[21] In the United States and Canada, the importance of the privilege is evidenced through its constitutional protection. With the second voice, however, courts and legislatures have recognised that it will not always be appropriate to give the privilege its full expression. In the United States, the Supreme Court noted in *Schmerber* that 'the privilege has never been given the full scope which the values it helps to protect suggest'.[22] In Australia, the Full Court of the Victorian Supreme Court, in holding that breathalyser samples did not implicate the privilege, stated that to allow the privilege to prevent the taking of such a sample would be to give the privilege 'a breadth of operation which it does not have'.[23] While acknowledging the importance of the privilege, courts have also been quick to note that its curtailment is often necessary.

These duelling voices are evident when courts weigh competing interests to determine whether the privilege has been infringed by a particular search or order. In that circumstance, the competing interests of the individual in protecting the privilege are at odds with the interests of society in having law enforcement officials investigate suspected criminal activity. When the scales tip towards a finding that the privilege has not been infringed, it is a recognition that the practicalities of law enforcement have outweighed the values that lie behind the privilege. The application of the privilege,

---

20 *Sorby* (1983) 152 CLR 281, 309 (Mason, Wilson and Dawson JJ).

21 *Pyneboard Pty Ltd v Trade Practises Commission* (1983) 152 CLR 281, 294 (Gibbs CJ).

22 *Schmerber* 384 US 757, 763 (1966).

23 *King v McLelland* [1974] VR 773, 776.

therefore, takes place with a healthy acknowledgement that it is to be done in a pragmatic manner that recognises the realities of law enforcement. It is that pragmatic streak that has seen bodily features removed from the scope of the privilege and motor vehicle reporting obligations found not to infringe the privilege. In respect of the latter in particular, the giving of an incriminating oral statement under compulsion would appear to infringe the privilege. That Australia, England and Wales and the United States have found that it does not is a result of the balance in the weighing exercise tilting towards the public interest – a pragmatic outcome.

In Australia and England and Wales, those competing voices are recognised in the respective statutory provisions allowing compelled production orders. This occurs through the imposition of the obligation that such an order can only be granted where there is no less intrusive but equally effective alternative encryption workaround. By imposing this obligation, the legislatures have recognised that while the privilege may be limited to allow such orders to be made, that limitation should only occur when necessary – and it is not necessary if there is a reasonably practicable alternative means of obtaining the desired electronic data. The privilege is, therefore, to be protected to the greatest extent possible without unduly undermining the public interest.

As noted in Chapter 5, the effect of this is that in Australia, the privilege does not have a fixed ambit when applied to compelled production orders. When no alternative encryption workaround is available, the scope of the privilege constricts through its abrogation to allow the compelled production order to be made. Conversely, where such an alternative is available, the privilege is given its unabrogated scope, which encompasses – and therefore precludes the granting of – compelled production orders. In this way the legislation has continued the path identified in the decisions examined in Chapters 1 and 2: a path that accepts appropriate limitations where necessary notwithstanding the importance of the privilege.

Somewhat surprisingly, then, in Australia (and England and Wales) the answer to whether compelled production orders fall within the scope of the privilege is to be determined by examining whether there are appropriate alternative encryption

workarounds available. There is no one answer to this question which will apply in all circumstances; each case will depend on whether the facts allow for the use of such an alternative workaround. This outcome reflects the pragmatic approach to the privilege that was found in Chapters 1 and 2 when identifying the scope of the privilege. As a long-standing right of substantial importance, the privilege is not to be cast aside lightly. That does not mean, however, that it is sacrosanct, and where the pragmatic concerns of law enforcement become sufficiently vital the privilege will bend – as its history shows it has long done. In Australia, then, the question of whether the privilege must bend – and with it the question of what the scope of the privilege is – is answered by asking whether there is an alternative encryption workaround that can be used instead.

BIBLIOGRAPHY

CASES

Australia

A v Boulton (2004) 207 ALR 342

Boulton v R (2014) 46 VR 308

Bradley v Commonwealth (1973) 128 CLR 557

Bulejcik v The Queen (1996) 185 CLR 375

Bunning v Cross (1978) 141 CLR 54

Carr v The Queen (1973) 127 CLR 662

Chadburne v The State of Western Australia [2017] WASCA 216

Chester v The Queen (1988) 165 CLR 611

Commissioner of the Australian Federal Police v Hart (2018) 351 ALR 1

Construction, Forestry, Mining and Energy Union v Boral Resources (Vic) Pty Ltd (2015) 256 CLR 375

Controlled Consultants Proprietary Limited v Commissioner for Corporate Affairs (1985) 156 CLR 385

Dias v The State of Western Australia [2017] WASCA 49

Do Young Lee v The Queen (2014) 253 CLR 455

DPP (Cth) v D'Alessandro (2010) 26 VR 477

Electrolux Home Products Pty Ltd v Australian Workers' Union (2004) 221 CLR 309

Environment Protection Authority v Caltex (1993) 178 CLR 477

Garbellini v The State of Western Australia [2017] WASC 93

George v Rockett (1990) 170 CLR 104

Grollo v Bates (1994) 53 FCR 218

Haddara v R (2014) 43 VR 53

Hamilton v Oades (1989) 166 CLR 486

Harriman v R (1989) 167 CLR 590

Heathcote (A Pseudonym) v R [2014] VSCA 37

Hoare v The Queen (1989) 167 CLR 348

Homes v Thorpe [1925] SASR 286

K v Children's Court of Victoria [2015] VSC 645

King v McLelland [1974] VR 773

Lange v Australian Broadcasting Corporation (1997) 189 CLR 520

Lee v New South Wales Crime Commission (2013) 251 CLR 196

Lenton v Western Australia [2017] WASCA 224

Loges v Martin (1991) 13 MVR 405

Luppino v Fisher [2018] FCA 2106

Luppino v Fisher (No 2) [2019] FCA 1100

Lyons v R [2017] NSWCCA 204

McCloy v New South Wales (2015) 257 CLR 178

McKinnon v Secretary, Department of Treasury (2006) 228 CLR 423

Mills v Meeking (1990) 169 CLR 214

Mill v The Queen (1988) 166 CLR 59

Momcilovic v The Queen [2011] 245 CLR 1

Mortimer v Brown [1970] 122 CLR 493

Muldrock v The Queen (2011) 244 CLR 120

North Australian Aboriginal Justice Agency Limited v Northern Territory (2015) 256 CLR 569

Police v Dunstall (2015) 256 CLR 403

Postiglione v The Queen (1997) 189 CLR 295

Project Blue Sky Inc v Australian Broadcasting Authority (1998) 194 CLR 355

Pyneboard Pty Ltd v Trade Practises Commission (1983) 152 CLR 281

R v Carr [1972] 1 NSWLR 608

R v Coffey (2003) 6 VR 543

R v Cook; ex Parte Director of Public Prosecutions (Cth) [2004] QCA 469

R v Davis [1976] 1 NSWLR 84

R v De Leeuw [2015] NSWCCA 183

R v Ford [2017] QSC 205

R v Hooper (1995) 64 SASR 480

R v Independent Broad-Based Anti-Corruption Commission (2016) 256 CLR 459

R v Ireland (1970) 126 CLR 321

R v Jones (1999) 108 A Crim R 50

R v Jongsma (2004) 150 A Crim R 386

R v Knight (2001) 160 FLR 465

R v Lee (1950) 82 CLR 133

R v Monaghan [2014] ACTSC 278

R v Porte [2015] NSWCCA 174

R v Riddell [2009] NSWCCA 96

R v SW [2008] NSWDC 148

R v Zotti (2002) 82 SASR 554

Re Application under the Major Crime (Investigative Powers) Act 2004 (2009) 24 VR 415

Reid v Howard (1995) 184 CLR 1

Rozenes v Beljajev [1995] 1 VR 533

Ruddock v Taylor (2005) 222 CLR 612

Sorby v The Commonwealth (1983) 152 CLR 281

Sumption v Grant [2013] WASC 258

The State of Western Australia v Doyle [2017] WASCA 207

Tulloh v The Queen [2004] WASCA 169

Veen v The Queen (1979) 143 CLR 458

Veen v The Queen (No. 2) (1988) 164 CLR 465

W.A. Pines Pty Ltd v Bannerman [1980] 30 ALR 559

X7 v Australian Crime Commission (2013) 248 CLR 92

X v Callanan and Anor [2016] QCA 335

Zheng v Cai (2009) 239 CLR 446

Canada

Attorney-General of Quebec v Begin [1955] SCR 593

British Columbia (Securities Commission) v Branch [1995] 2 SCR 3

Hogan v R [1975] 2 SCR 574

Thomson Newspapers Ltd v Canada [1990] 1 SCR 425

Marcoux v R [1976] 1 SCR 763

R v B (S.A.) [2003] 2 SCR 678

R v Bartle [1984] 3 SCR 173

R v Beare [1988] 2 SCR 387

R v Boudreau-Fontaine 2010 QCCA 1108

R v Burke 2015 SKPC 173, 126 WCB (2d) 584

R v Burlington [1995] 2 SCR 206

R v Buss 2014 BCPC 16

R v Capancioni 2016 ONSC 4615

R v Collins [1987] 1 SCR 265

R v Curr [1972] SCR 889

R v Cusick 2015 ONSC 6739, 126 WCB (2d) 270

R v Cusick 2019 ONCA 524

R v Dubois [1985] 2 SCR 350

R v Jones [1994] 2 SCR 229

R v Fitzpatrick [1995] 4 SCR 154

R v Grant [2009] 2 SCR 353

R v Henry [2005] 3 SCR 609

R v Herbert [1990] 2 SCR 151

R v M(C) 2012 MBQB 141, 101 WCB (2d) 168

R v P (M.B) [1994] 1 SCR 555

R v Pratchett 2016 SKPC 19

R v Rothman [1981] 1 SCR 640

R v Saeed [2016] 1 SCR 518

R v S (R.J.) [1995] 1 SCR 451

R v Seguin 2015 ONSC 1908, 120 WCB (2d) 234

R v Shepherd [2009] 2 SCR 527

R v Shin 2015 ONCA 189

R v Simmons [1988] 2 SCR 495

R v Spencer [2014] 2 SCR 212

R v Stillman [1997] 1 SCR 607

R v Strachan [1988] 2 SCR 980

R v Talbot 2017 ONCJ 814

R v Therens [1985] 1 SCR 613

R v White [1999] 2 SCR 417

R v Wittwer [2008] 2 SCR 235

Reference re s 92(4) of the Vehicles Act, 1957 (Saskatchewan) [1958] SCR 608

Re Impression Warrant Application (s. 487.092) 2016 ONCJ 197, 129 WCB (2d) 485

The Queen v Wray [1971] SCR 272

Thompson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission) [1990] 1 SCR 425

England and Wales

Ali v Jayaratne [1951] AC 66

Allan v United Kingdom (2002) 36 EHRR 12

Attorney General's Reference (No 7 of 2000) [2001] 1 WLR 1879

Beghal v Department of Public Prosecutions [2016] AC 88

Brown v Stott [2003] 1 AC 681

C plc v P (Attorney General Intervening) [2008] Ch 1

Ghaidan v Godin-Mendoza [2004] 2 AC 557

Gold Nuts Ltd v Revenue and Customs Commissioners [2016] UKFTT 82 (TC)

Greater Manchester Police v Andrews [2011] EWHC 1966 (Admin)

Hussein v Chong Fook Kam (1970) AC 942

Inland Revenue Commissioners v Rossminster [1980] All ER 80

Mohammed v The Secretary of State for the Home Department [2014] EWHC 4317 (Admin)

Phillips v News Group Newspapers Ltd [2013] 1 AC 1

R v A (No 2) [2002] 1 AC 45

R v Abdul-Razak [2015] EWCA Crim 2370

R v Button [2005] EWCA Crim 516

R v Chalkley [1998] 2 Cr App R 79

R v Christie [1914] AC 545

R v Delucca [2010] EWCA Crim 710

R v Director of Serious Fraud Office, Ex parte Smith [1993] AC 1

R v Hertfordshire County Council, ex parte Green Industries Environmental Industries Ltd 2 AC 412

R v Home Secretary; Ex parte Pierson [1998] AC 539

R v K(A) [2009] EWCA Crim 1640

R v Kearns [2002] 1 WLR 2815

R v Khan (Sultan) [1997] AC 558

R v Mahroof [2015] EWCA Crim 1184

R v Mushtaq [2005] UKHL 25

R v Padellec [2012] EWCA Crim 1956

R v Sang [1980] AC 402

R v S(F) [2009] [2009] 1 WLR 1489

R v Southwell [2012] EWCA Crim 2882

R (Westminster City Council) v National Asylum Support Service [2002] UKHL 38

Sheldrake v Director of Public Prosecutions [2005] 1 AC 264

European Court of Human Rights

Case of Big Brother Watch v United Kingdom (European Court of Human Rights, First Section) Applications Nos 58170/13, 63422/14 and 24960/15, 13 September 2018

Dudgeon v United Kingdom (1981) 4 EHRR 149

Funke v France (1993) 16 EHRR 297

Gafgen v Germany (2011) 52 EHRR 1

Heaney and McGuinness v Ireland (2000) 33 EHRR 12

Heglas v Czech Republic (2009) 48 EHRR 44

Ibrahim v United Kingdom (2015) 61 EHRR 9

Ivashchenko v Russia (2018) 67 EHRR 20

Jalloh v Germany (2007) 44 EHRR 32

JB v Switzerland App. No. 31827/96, May 3, 2001

Khan v United Kingdom (2001) 31 EHRR 45

L v United Kingdom [2000] 2 FLR 322

Liberty v United Kingdom (2009) 48 EHRR 1

McDonald v United Kingdom (2015) EHRR 1

McGuinness v Ireland (2001) 33 EHRR 12

Murray v United Kingdom (1996) 22 EHRR 2

Niemietz v Germany (1993) 16 EHRR 97

O'Halloran and Francis v The United Kingdom (2008) 46 EHRR 21

S v United Kingdom (2009) 48 EHRR 50

Saunders v United Kingdom (1997) 23 EHRR 313

Schenk v Switzerland (1988) 13 EHRR 242

Szabo and Vissy v Hungary (2016) 63 EHRR 3

Weh v Austria (2005) 40 EHRR 37

United States

Aguilar v State (Tenn Ct Crim App, No M2015-00430-CCA-R3-PC, 30 December 2015)

Beecher v Alabama 389 US 35 (1967)

Blefare v United States 362 F 2d 870 (9th Cir, 1966)

Boyd v United States 116 US 616 (1886)

Breithaupt v Abram 352 US 432 (1957)

California v Byers 402 US 424 (1971)

Commonwealth v Baust 89 Va Cir 267 (2014)

Commonwealth v Davis 176 A 3d 869 (Pa Super Ct, 2018)

Commonwealth v Gelfgatt 11 NE 3d 605 (Mass, 2014)

Commonwealth v Jones 34 Mass L Rptr 287 (Mass Super Ct, 2017)

Counselman v Hickman 142 US 547 (1892)

Davis v United States 564 US 229 (2011)

Doe v United States 487 US 201 (1988)

Fisher v United States 425 US 391 (1976)

GAQL v Florida 257 So 3d 1058 (Fla App 4 Dist, 2018)

Gilbert v California 388 US 263 (1967)

Gouled v United States 255 US 298 (1921)

Herring v United States 555 US 135 (2009)

Holt v United States 218 US 245 (1910)

Hudson v Michigan 547 US 586 (2006)

In re Application for a Search Warrant (ND Ill, No 17M081, 16 February 2017)

In re Harris 221 US 274 (1911)

In re Grand Jury Subpoena Duces Tecum 670 F 3d 1335 (11th Cir, 2012)

In re Warrant to Search a Target Computer at Premises Unknown 958 F Supp 2d 753 (SD Tex, 2013)

In the Matter of the Search Warrant Application for [redacted text] 279 F Supp 3d 800 (ND Ill, 2017)

In the Matter of the Decryption of a Seized Data Storage System (ED Wis, No 13-M-449, 19 April 2013)

In the Matter of the Search of a Residence in Aptos, California 95003 (ND Cal, Case no. 17-mj-70656-JSC-1, 20 March 2018)

In the Matter of the Search of Apple iPhone 8 recovered from the Residence of Grant Michalski, 221 N. Front Street, #105 Columbus, OH, and Currently Held in FBI Secure Evidence Storage, 425 W. Nationwide Blvd, Columbus, OH (SD Ohio, No 2:18-MJ-707, 19 September 2018)

Kastigar v United States 406 US 441 (1972)

Mackey v Montrym, 443 US 1 (1979)

Mapp v Ohio 367 US 643 (1961)

Mincey v Arizona 437 US 397 (1978)

Miranda v Arizona 384 US 436 (1966)

Murphy v Waterfront Commission of New York Harbor 378 US 52 (1964)

Olmstead v United States 277 US 438 (1928)

Outlaw v City of Cahokia (SD Ill, No 16-cv-456-JPG-SCW, 26 April 2017)

Pachas-Luna v State (Tex Ct App, No 01-14-00516-CR, 15 October 2015)

Pennsylvania v Muniz 496 US 582 (1990)

People v Johnson 90 NE 3d 634 (Ill App, 2017)

Phillips v United States (D Del, Cr Act No 08-031-LPS 12 August 2014)

Pillsbury v Conboy 459 US 248 (1983)

Reck v Pate 367 US 433 (1961)

Re Grand Jury Subpoena to Sebastian Boucher (D Vt, No 2:06-mj-91, 29 November 2007)

Re Grand Jury Subpoena to Sebastian Boucher (D Vt, No 2:06-mj-91, 19 February 2009)

Riley v California 134 S Ct 2473 (2014)

Schmerber v California 384 US 757 (1966)

Securities Exchange Commission v Huang (ED Pa, Civ No 15-269, 23 September 2015)

Seo v State 109 NE 3d 418 (Ind Ct App, 2018)

South Dakota v Neville 459 US 553 (1983)

State v Andrews 197 A 3d 200 (NJ Super App Div, 2018)

State v Cooley 165 So 3d 1237 (La Ct App, 2015)

State v Diamond 890 NW 2d 143 (Minn App, 2017)

State v Landrum (Ariz Ct App, No 1 CA-CR 14-0203, 25 June 2015)

State v Stahl 206 So 3d 124 (Fla Ct App, 2016)

State v Trant (Me Super Ct, No 15-2389, 22 October 2015)

United States v Apple Mac Pro Computer 851 F 3d 238 (3rd Cir, 2017)

United States v Blatney (A F Ct Crim App, No 2016-16, 22 May 2017)

United States v Bright 596 F 3d 683 (9th Cir, 2010)

United States v Cunningham 694 F 3d 372 (3rd Cir, 2012)

United States v Dennis (ND Da, No 3:13-cr-00010-TCB-RGV, 7 April 2014)

United States v Dionisio 410 US 1 (1973)

United States v Doe 465 US 605 (1984)

United States v Espinoza 338 F Supp 1304 (Cal, 1972)

United States v Fricosu 841 F Supp 2d 1232 (D Colo, 2012)

United States v Gavegnano 305 Fed Appx 954 (4th Cir, 2009)

United States v Green 272 F 3d 748 (5th Cir, 2001)

United States v Greenfield 831 F 3d 106 (2nd Cir, 2016)

United States v Guadalupe-Garza 421 F 2d 876 (9th Cir, 1970)

United States v Hubbell 530 US 27 (2000)

United States v Kirschner 823 F Supp 2d 665 (ED Mich, 2010)

United States v LeBrun 363 F 3d 715 (8th Cir, 2004)

United States v Leon 468 US 897 (1984)

United States v Mara 410 US 19 (1973)

United States v Ortega (SD Ga, No CR415-134, 30 October 2015)

United States v Pearson (ND NY, No 1:04-CR-340, 24 May 2006)

United States v Scarfo 180 F Supp 2d 572 (D NJ, 2001)

United States v Schimley (ND Ohio, No 1:08 CR 510, 21 December 2009)

United States v Spencer (ND Cal, Case No. 17-cr-00259-CRB-1, 26 April 2018)

United States v Wade 388 US 218 (1967)

Weeks v United States 232 US 383 (1914)

Other Courts

MacLean v HM Advocate 2012 JC 293

McFadden v HM Advocate 2010 SCL 247

Public Prosecutor's Office v Skype Communications SARL, Court of Appeal of Antwerp, Case no 2016/CO/1006, 15 November 2017

LEGISLATION

Australia

Acts Interpretation Act 1901 (Cth)

Charter of Human Rights and Responsibilities 2006 (Vic)

Competition and Consumer Act 2010 (Cth)

Controlled Substances Act 1984 (SA)

Criminal Assets Confiscation Act 2005 (SA)

Crimes Act 1900 (ACT)

Crimes Act 1914 (Cth)

Crimes Act 1958 (Vic)

Crimes (Forensic Procedures) Act 2000 (NSW)

Crimes (Forensic Procedures) Act 2000 (ACT)

Criminal Code Act 1924 (Tas)

Criminal Code Act 1899 (Qld)

Criminal Code Act 1995 (Cth)

Criminal Investigations Act 2006 (WA)

Criminal Law (Forensic Procedures) Act 2007 (SA)

Criminal Organisations Control and Other Acts Amendment Act 2014 (Vic)

C*ustoms Act 1901* (Cth)

Drugs Misuse Act 1986 (Qld)

Drugs, Poisons and Controlled Substances Act 1981 (Vic)

Evidence Act 1995 (Cth)

Evidence Act 1995 (NSW)

Evidence Act 2001 (Tas)

Evidence Act 2008 (Vic)

Evidence Act 2011 (ACT)

Evidence (National Uniform Legislation) Act 2011 (NT)

Fair Trading Act 2010 (WA)

Federal Court of Australia Act 1976 (Cth)

Forensic Procedures Act 2000 (Tas)

Human Rights Act 2004 (ACT)

Human Rights Act 2019 (Qld)

Law Enforcement (Powers and Responsibilities) Act 2002 (NSW)

Major Crime (Investigatory Powers) Act 2004 (Vic)

Misuse of Drugs Act 1981 (WA)

Police Administration Act (NT)

Police Offences Act 1935 (Tas)

Police Powers and Responsibilities Act 2000 (Qld)

Proceeds of Crime Act 2002 (Cth)

Search Warrants Act 1997 (Tas)

Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019 (SA)

Summary Offences Act 1953 (SA)

Surveillance Devices Act 2004 (Cth)

Taxation Administration Act 1953 (Cth)

Telecommunications Act 1997 (Cth)

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)

Canada

Canada Evidence Act RSC 1985, c C-5

Criminal Code RSC 1985, C-46

England and Wales

Canada Act 1982 c 11, sch B pt I

Human Rights Act 1998 c 42

Investigatory Powers Act 2016 c 25

Police and Criminal Evidence Act 1984 c 60

Protection of Children Act 1978 c 37

Regulation of Investigatory Powers Act 2000 c 23

Road Traffic Act 1988 c 52

Terrorism Act 2006 c 11

United States

All Writs Act 1789 28 USC § 1651

ARTICLES AND BOOKS

Akdeniz, Yaman, 'Regulation of Investigatory Powers Act 2000: Part 1: BigBrother.gov.uk: State Surveillance in the Age of Information and Rights' (2001) *Criminal Law Review* 73

Akdeniz, Yaman, 'Possession and Dispossession: A Critical Assessment of Defences in Possession of Indecent Photographs of Children Cases' (2007) *Criminal Law Review* 274

Allen, Ronald J and M Kristen Mace, 'The Self-Incrimination Clause Explained and its Future Predicted' (2004) 94(2) *Journal of Criminal Law and Criminology* 243

Amar, Akhil Reed and Renee B Lettow, 'Fifth Amendment, First Principles: The Self-Incrimination Clause' (1995) 93 *Michigan Law Review* 857

Ashworth, Andrew, 'Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism?' (2008) 30 *Cardozo Law Review* 751

Ashworth, Andrew, 'The Exclusion of Evidence Obtained by Violating a Fundamental Right: Pragmatism Before Principle in the Strasbourg Jurisprudence' in Paul Roberts and Jill Hunter (eds), *Criminal Evidence and Human rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012)

Atwood, J Riley, 'The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement' (2015) 34 *Saint Louis University Public Law Review* 407

Bales, Chase, 'Unbreakable: The Fifth Amendment and Computer Passwords' (2012) 44 *Arizona State Law Journal* 1293

Berger, Mark, *Taking the Fifth: The Supreme Court and the Privilege Against Self-Incrimination* (Lexington Books, 1980)

Berger, Mark, 'American Perspectives on Self-Incrimination and the Compelled Production of Evidence' (2002) 6 *International Journal of Evidence and Proof* 218

Blackstone, William, *Commentaries on the Laws of England* (The Legal Classics Library, vol IV, 1765)

Bonin, Adam C, 'Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation' (1996) *University of Chicago Legal Forum* 495

Brenner, Susan W, 'Encryption, Smart Phones and the Fifth Amendment' (2012) 33 *Whittier Law Review* 525

Chatterjee, Bela Bonita, 'New but Not Improved: A Critical Examination of Revisions to the Regulation of Investigatory Powers Act 2000 Encryption Provisions' (2011) 19(3) *International Journal of Law and Information Technology* 264

Chatterjee, Bela, 'Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury?' (2012) 24 *Children and Family Law Quarterly* 410

Chertoff, Michael, 'International Travel with a Digital Briefcase: If Customs Officials Can Search a Laptop, Will the Right Against Self-Incrimination Contravene This Authority?' (2009) 37 *Pepperdine Law Review* 105

Choo, Andrew L-T and Susan Nash, 'Evidence Law in England and Wales: The Impact of the Human Rights Act 1998' (2003) 7 *International Journal of Evidence and Proof* 31

Choo, Andrew L-T, 'Give Us What You Have – Information, Compulsion and the Privilege Against Self-Incrimination as a Human Right' in Paul Roberts and Jill Hunter (eds), *Criminal Evidence and Human rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012)

Choo, Andrew L-T, *The Privilege against Self-Incrimination and Criminal Justice* (Hart Publishing, 2013)

Choo, Andrew L-T, *Evidence* (Oxford University Press, 2015)

Churchhouse, Robert, *Codes and Ciphers: Julius Caesar, the Enigma and the Internet* (Cambridge University Press, 2002)

Clemens, Aaron M, No Computer Exception to the Constitution: The Fifth Amendment Protects against Compelled Production of an Encrypted Document or Private Key (2004) *University of California Los Angeles Journal of Law and Technology* 2

Colarusso, David, 'Heads in the Cloud, a Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination' [2011] 17 *Boston University Journal of Science and Technology Law* 69

Corn, Geoffrey S and Dru Brenner-Beck, '"Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance"' in D Gray and S Henderson (eds) *The Cambridge Handbook of Surveillance Law* Cambridge University Press (2017) 330

Dennis, Ian, 'Instrumental Protection, Human Right or Functional Necessity? Reassessing the Privilege against Self-Incrimination' (1995) 54(2) *Cambridge Law Journal* 342

Dennis, Ian, 'The Human Rights Act and the Law of criminal Evidence: Ten Years On' (2011) 33 *Sydney Law Review* 333

Dennis, Ian, *The Law of Evidence* (Sweet & Maxwell, 2013)

Dirkis, M J, '1984 Revisited? Review of the Commissioner of Taxation's Access Powers under Section 263 of the Income Tax Assessment Act 1936' (1989) 12 *Adelaide Law Review* 126

Dolinko, David, 'Is There a Rationale for the Privilege against Self Incrimination?' (1986) 33 *UCLA Law Review* 1063

Duong, John, 'The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border' (2009) 2 *Drexel Law Review* 313

Emmerson, Ben et al, *Human Rights and Criminal Justice* (Sweet & Maxwell, 3rd ed, 2012)

Engels, Joshua A, 'Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing' (2012) 33 *Whittier Law Review* 543

Folkinshteyn, Benjamin, 'A Witness against Himself: A Case for Stronger Legal Protection of Encryption' (2013) 30 *Santa Clara High Tech Law Journal* 375

Froomkin, Michael A, 'The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution' (1995) 143 *University of Pennsylvania Law Review* 709

Froomkin, Michael A, 'Lessons Learnt Too Well: Anonymity in a Time of Surveillance' (2017) 59 *Arizona Law Review* 95

Gans, Jeremy et al, *Criminal Process and Human Rights* (Federation Press, 2011)

Gershowitz, Adam M, Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest? (2011) 96 *Iowa Law Review* 1125

Gillespie, Alisdair A, 'Jurisdictional Issues Concerning Online Child Pornography' (2012) 20 *International Journal of Law and Information Technology* 151

Goodman, Jody, 'Forced Data Decryption: Does it Violate the Fifth Amendment?' (2013, Winter) 27 *Criminal Justice* 43

Goss, Ryan, *Criminal Fair Trial Rights: Article 6 of the European Convention on Human Rights* (Hart Publishing, 2014)

Green, Michael S, 'The Privilege's Last Stand: The Privilege against Self-Incrimination and the Right to Rebel against the State' (1999) 65(3) *Brooklyn Law Review* 627

Harvie, Robert and Hamar Foster, 'Ties That Bind? The Supreme Court of Canada, American Jurisprudence, and the Revision of Canadian Criminal Law under the Charter' (1990) 28(4) *Osgoode Hall Law Journal* 729

Helmholz, R H, 'Origins of the Privilege against Self-Incrimination: The Role of the European Ius Commune' (1990) 65 *New York University Law Review* 962

Hogg, Peter W, *Constitutional Law of Canada* (Carswell, 2011)

Ives, Dale E, 'R v Henry: A Welcome Retreat from an Overly Broad Interpretation of s. 13 of the Canadian Charter of Rights and Freedoms' (2006) 10 *The International Journal of Evidence and Proof* 212

Jaffer, Jamil N and Daniel J Rosenthal, 'Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge' (2014) *Catholic University Journal of Law and Technology* 273

James, Nickolas John, 'Handing over the Keys: Contingency, Power and Resistance in the Context of Section 3LA of the Australian Crimes Act 1914' (2004) 23 *University of Queensland Law Journal* 7

Jarone, Joseph, 'An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption' (2015) *Florida International University Law Review* 767

Jones, Oliver, *Bennion on Statutory Interpretation* (LexisNexis, 2013)

Kerr, Orin, 'Digital Evidence and the New Criminal Procedure' (2005) 105 *Columbia Law Review* 279

Kerr, Orin, 'Ex Ante Regulation of Computer Search and Seizure' (2010) 96(6) *Virginia Law Review* 1241

Kerr, Orin and Bruce Schneier, 'Encryption Workarounds' (2018) 106 *Georgetown Law Journal* 989

Kerr, Orin, 'Compelled Decryption and the Privilege against Self-Incrimination' (2019) 97 *Texas Law Review* 767

Kiok, Jeffrey, 'Missing the Metaphor: Compulsory Decryption and the Fifth Amendment' (2015) 24 *Boston University Public Interest Law Journal* 53

Klein, Philip N, *A Cryptography Primer: Secrets and Promises* (Cambridge University Press, 2014)

Koops, Bert-Jan, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer Law International, 1999)

Koops, Bert-Jaap and Eleni Kosta, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 *Computer Law and Security Review* 890

Larkin, John E D, 'Compelled Production of Encrypted Data' (2012) 14 *Vanderbilt Journal of Entertainment and Technological Law* 253

Lowe, David and Charlie Potter, *Understanding Legislation: A Practical Guide to Statutory Interpretation* (Hart Publishing, 2018)

Mahoney, Michael S, 'Compelling the Production of Passwords: Government's Ability to Compel the Production of Passwords Necessary to the Discovery of Encrypted Evidence in Criminal Proceedings, Merely a Choice of Words' (2003) 6 *T M Cooley Journal of Practical and Clinical Law* 83

McGregor, Nathan K, 'The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege' (2010) 12 *Vanderbilt Journal of Entertainment and Technology Law* 581

Mckay, Simon, *Blackstone's Guide to the Investigatory Powers Act 2016* (Oxford University Press, 2017)

McNicol, Suzanne B, *A Non-Curial Privilege Against Self-Incrimination* (Faculty of Law, Monash University, 1984)

Meagher, Dan and Matthew Groves (eds), *The Principle of Legality in Australia and New Zealand* (Federation Press, 2017)

Meyerson, Denise, 'Why Courts Should Not Balance Rights against the Public Interest' (2007) 31 *Melbourne University Law Review* 873

Mohan, Vivek and John Villasenor, 'Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era' (2012) 15 *University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny* 11

Morrison, Carin Myers, 'Passwords, Profiles, and the Privilege against Self-Incrimination: Facebook and the Fifth Amendment' (2012) 65 *Arkansas Law Review* 133

O'Floinn, Michael and David Ormerod, 'Social Networking Sites, RIPA and Criminal Investigations' (2011) *Criminal Law Review* 766

Opderbeck, David W, 'The Skeleton in the Hard Drive: Encryption and the Fifth Amendment' (2018) 70 *Florida Law Review* 883

Paciocco, David M, 'Self-Incrimination: Removing the Coffin Nails' (1989) 35 *McGill Law Journal* 73

Palfreyman, Brendan M, 'Lessons from the British and American Approaches to Compelled Decryption' (2009) 75 *Brooklyn Law Review* 345

Pearce, Dennis and Robert Geddes, *Statutory Interpretation in Australia* (LexisNexis Butterworths, 8th ed, 2014)

Pell, Stephanie K, 'You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?' (2016) 17 *North Carolina Journal of Law and Technology* 599

Penney, Steven M, 'Unreal Distinctions: The Exclusion of Unfairly Obtained Evidence under s 24(2) of the Charter' (1994) 32(4) *Alberta Law Review* 782

Penney, Steven, 'What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination Law in the Post-Charter Era. Part I: Justifications for Rules Preventing Self-Incrimination' (2003) 48 *Criminal Law Quarterly* 249

Penney, Steven, 'What's Wrong with Self-Incrimination? The Wayward Path of Self-Incrimination Law in the Post-Charter Era. Part II: Self-Incrimination in Police Investigations' (2003) 48 *Criminal Law Quarterly* 280

Pinto, Minerva, The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing (2016) 25 *Temple Political and Civil Rights Law Review* 223

Piper, Fred and Sean Murphy, *Cryptography: A Very Short Introduction* (Oxford University Press, 2002)

Ratushny, Ed, *Self-Incrimination in the Canadian Criminal Process,* Carswell's Criminal Law Series (Carswell Company Limited, 1979)

Redmayne, Mike, 'Rethinking the Privilege against Self-Incrimination' (2007) 27(2) *Oxford Journal of Legal Studies* 209

Reid, Alan S and Nicholas Ryder, 'For Whose Eyes Only: A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000' (2001) 10 *Information and Communications Technology Law* 179

Reitinger, Phillip R, 'Compelled Production of Plaintext and Keys' (1996) *The University of Chicage Legal Forum* 171

Roach, Kent, 'The Consequences of Compelled Self-Incrimination in Terrorism Investigations: A Comparison of American Grand Juries and Canadian Investigative Hearings' (2008) 30 *Cardozo Law Review* 1089

Roberts, Paul, and Jill Hunter (eds), *Criminal Evidence and Human Rights: Reimagining Common Law Procedural Traditions* (Hart Publishing, 2012)

Sales, Erin M, 'The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to be Free from Self-Incrimination' (2014) 63 *University of Miami Law Review* 193

Sacharoff, Laurent, 'Unlocking the Fifth Amendment: Passwords and Encrypted Devices' (2018) 87 *Fordham Law Review* 203

Sacharoff, Laurent, 'What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr' (2019) 97 *Texas Law Review* 63

Sanson, Michelle, *Statutory Interpretation* (Oxford University Press, 2nd ed, 2016)

Saper, Nathan, 'International Cryptography Regulation and the Global Information Economy' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 673

Schulhofer, Stephen J, 'Miranda, Dickerson, and the Puzzling Persistence of Fifth Amendment Exceptionalism' (2001) 99 *Michigan Law Review* 941

Sharpe, Robert J and Kent Roach, *The Charter of Rights and Freedoms* (Irwin Law, 2009)

Sharpe, Sybil, 'The Privilege Against Self-Incrimination: Do We Need a Preservation Order?' (1998) 27 *Anglo-American Law Review* 494

Soares, Nicholas, 'The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age' (2012) 49 *American Criminal Law Review* 2001

Spraul, V Anton, *How Software Works: The Magic Behind Encryption, CGI, Search Engines and Other Everyday Items* (No Starch Press, 2015)

Stallings, William and Brown, Lawrie, *Computer Security: Principles and Practice* (Pearson, 2015)

Stewart, Hamish, 'The Privilege against Self-Incrimination: Reconsidering Redmayne's Rethinking' (2016) 20(2) *The International Journal of Evidence and Proof* 95

Stuesser, Lee, 'R v SAB: Putting "Self-Incrimination" in Context' (2004) 42(2) *Alberta Law Review* 543

Stuntz, William J, Self-Incrimination and Excuse' (1988) 88 *Columbia Law Review* 1227

Terzian, Dan, The Fifth Amendment, Encryption and the Forgotten State Interest (2014) 61 *University of California Law Review Discourse* 298

Terzian, Dan, 'Forced Decryption as a Foregone Conclusion' (2015) 6 *California Law Review Circuit* 27

Ungberg, Andrew J, 'Protecting Privacy through a Responsible Decryption Policy' (2009) 22(2) *Harvard Journal of Law and Technology* 537

Wadham, John et al, *Blackstone's Guide to the Human Rights Act 1998* (Oxford University Press, 2nd ed, 2015)

Walden, Ian, 'The Sky is Falling! Response to the "Going Dark" Problem' (2018) 34 *Computer Law and Security Review* 901

Ward, Tim and Piers Gardner, 'The Privilege against Self-Incrimination: In Search of Legal Certainty' (2003) *European Human Rights Law Review* 388

Wigmore, John, *Evidence in Trials at Common Law* (McNaughton rev, vol 8, 1961)

Winkler, Andrew T, 'Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era' (2013) 39 *Rutgers Computer and Technology Law Journal* 194

Wiseman, Timothy A, 'Encryption, Forced Decryption, and the Constitution' (2015) 11 *I/S: A Journal of Law and Policy for the Information Society* 525

Woellner, Robin, 'Section 263 Powers of Access – Why Settle for Second Best' (2005) 20 *Australian Tax Forum* 365

OTHER

Australia

Access Now, Submission No 33 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Apple, Submission No 53 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018

Australian Communications Consumer Action Network, Submission No 49 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Australian Government Department of Home Affairs, Submission No 18 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018

Australian Human Rights Commission, Submission No 47 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Australian Information Industry Association, Submission No 39 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018

Australian Law Reform Commission, *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws*, Report No 129

BSA, Submission No 48 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Cisco, Submission No 42 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Communications Alliance, Australian Industry Group, Australian Information Industry Association and Australian Mobile Telecommunications Association, Submission No 43 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Crimes Amendment (Child Pornography and Other Matters) Bill 2015

Crime and Corruption Commission Queensland, *Assessing Electronically Stored Evidence of Child Exploitation Material Offences: An Examination of the Limitations of section 154 of the Police Powers and Responsibilities Act 2000*, October 2015

Culnane, Chris and Vanessa Teague, Submission No 16 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, September 2018

Explanatory Memorandum, Justice Legislation Amendment (Confiscation and other Matters) Bill 2014

Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Internet Architecture Board, Submission No 23 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 October 2018

Justice Legislation Amendment (Confiscation and other Matters) Bill 2014

Kaspersky Lab, Submission No 13 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018

Massachusetts Institute of Technology: Internet Policy Research Initiative, Submission No 32 to the Parliamentary Joint Committee on Intelligence and Security, *Review*

of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 11 October 2018

Mozilla, Submission No 46 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Office of the Victorian Information Commissioner, Submission No 45 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Optus, Submission No 41 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, October 2018

Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009

Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Alert Digest*, No 9 of 2015, 18 August 2015

Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Alert Digest*, No 13 of 2014, 14 October 2014

South Australia, *Parliamentary Debates*, Legislative Council, 18 October 2017

Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA)

Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2018 (SA)

Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth)

Telstra Corporation Limited, Submission No 44 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

The Software Alliance, Submission No 48 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 12 October 2018

Victoria, *Parliamentary Debates*, Legislative Assembly, 26 June 2014

Victoria, *Parliamentary Debates*, Legislative Assembly, 5 August 2015

Victoria, *Parliamentary Debates*, Legislative Council, 17 September 2014

Western Australia Police Force, *Statutory Review of the Criminal Investigation Act 2006* (Issues Paper, January 2017)

England and Wales

Home Office, *Protected Electronic Information: Revised Code of Conduct* (August 2018)

Home Office, *Equipment Interference: Code of Practice* (March 2018)

Investigatory Powers (Technical Capability) Regulations 2018

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2009-2010*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2010-2011*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2012-2013*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2013-2014*

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2014*-2015

United States

Manhattan District Attorney's Office, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (November 2017) <https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf>

Brewster, Thomas, 'The Feds Can Now (Probably) Unlock Every iPhone Model in Existence', *Forbes*, 26 February 2018

<https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#4c280c9e667a>

Brewster, Thomas, 'Mysterious $15,000 "GrayKey" Promises to Unlock iPhone X for the Feds' *Forbes*, 5 March 2018

<https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#4c7ef5362950>

Cook, Tim, 'A Message to Our Customers' (16 February 2016) *Apple* <https://www.apple.com/customer-letter/>

Farivar, Cyrus, 'Apple Expands Data Encryption under IOS 8, Making Handover to Cops Moot' (18 September 2014) *Arstechnica*

<https://arstechnica.com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/>

Kerr, Orin, 'A Revised Approach to the Fifth Amendment and Obtaining Passwords', *The Washington Post* (online), 15 August 2017

<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/>

Kerr, Orin, 'The Fifth Amendment Limits on Forced Decryption and Applying the Foregone Conclusion Doctrine', *The Washington Post* (online), 7 June 2016

<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/>

Kerr, Orin, 'Fifth Amendment Protects Passcode on Smartphone, Court Holds', *The Washington Post* (online), 24 September 2015

<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds/>

Locklear, Mallory, 'Signal Says It Can't Allow the Government Access to Users' Chats' (14 December 2018) *Engadget* <https://www.engadget.com/2018/12/14/signal-cant-allow-government-access/>

Miller, Greg and Ellen Nakashima, 'Wikileaks Says It Has Obtained Trove of CIA Hacking Tools' (7 March 2017) *The Washington Post*

<https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.5642354ffb3f>

Zetter, Kim, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (3 March 2016) *Wired* <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>