ENCRYPTION AND THE PRIVILEGE AGAINST SELF-INCRIMINATION: WHAT HAPPENS WHEN A SUSPECT REFUSES TO DIVULGE A PASSWORD

DANIEL HOCHSTRASSER*

The use of encryption to protect electronic devices, including smartphones and computers, is commonplace. This may impede the ability of law enforcement officials 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. This article considers the role of the privilege against self-incrimination in the face of a court order to produce the password to an encrypted device. It does this through a comparative approach, examining how the privilege is understood in Australia and the comparator jurisdictions. It concludes that the express abrogation of the privilege is an appropriate legislative response to this issue in Australia.

I INTRODUCTION

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 ('the privilege'). On the facts before it, the Court held that the defendant's privilege was not infringed. Since that first decision, the issue of whether the privilege could

* Lecturer, Graduate School of Business and Law, RMIT University. Email: daniel.hochstrasser@rmit.edu.au. This article is drawn from my PhD thesis at Melbourne Law School, which was supported by an Australian Government Research Training Program Scholarship. My thanks to both my PhD supervisors, Professor Jeremy Gans and Associate Professor Andrew Roberts, whose guidance during my PhD allowed me to produce this article, and to the anonymous referees who provided valuable feedback.

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

be relied upon by a suspect to prevent a compelled production order being made against him or her has produced an extensive record of decisions in the United States ('US').[2] The issue has also arisen in several other jurisdictions including England and Wales, Canada and Australia.

In Australia, the body of decisions is substantially smaller than in the US and has only started to develop in recent years. As Australian courts grapple with this issue, some guidance can be obtained from the decisions of the courts of England and Wales, Canada and the US. Each of those jurisdictions share a common law heritage with Australia, all of which have long recognised the privilege. How courts in those jurisdictions have determined compelled production orders may be of assistance to Australian courts. For example: how those jurisdictions have assessed the evidentiary burden that must be satisfied before an order can be made; what they say about biometric passwords, an issue that has not yet been directly addressed by an Australian court; and how they have dealt with objections to such orders based on the privilege? The importance of this analysis, though, lies not only in the assistance that it may provide to Australian courts. An improved understanding of the legislative framework can assist Australian lawmakers as they continue to consider their response to this issue. In this regard, the contrast between Canada and England and Wales is stark: the former jurisdiction, addressing these orders in the absence of specific legislative measures, has an undeveloped approach to this issue; the latter, through its statutory response, possessing a relatively settled body of law on this issue.

Each of the US, Canada, and England and Wales will be considered in turn in Parts II, III and IV. In analysing how courts of those jurisdictions have resolved orders for compelled productions orders, specific issues will be addressed, including the source of the power to make a compelled production order and the evidentiary burdens imposed on the state regarding the suspect's knowledge of the password to the electronic device and the contents of that device. Part V will thereafter analyse Australian case law on compelled production orders, noting in particular the similarities and differences that exist between Australia and the comparator jurisdictions. Finally, the conclusion in Part VI will argue that the Australian statutory regime has avoided many of the problems present in the US case law, while following a broadly similar, and successful, path to that taken by England and Wales. Readers should note that the scope of this article does not encompass recent legislative changes introduced in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth). Those changes are primarily concerned with 'back door' access to encrypted devices, while the concern of this article is with compelling the production of the password from an individual in possession of that password.

We start by looking at the US, the jurisdiction with the largest body of case law on this issue.

---

2 This article 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.

II THE UNITED STATES

A The United States' Approach to the Privilege against Self-Incrimination

The privilege is protected in the US 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'.[3] A consequence of its constitutional protection is that it cannot be abrogated without the grant of immunity that is 'coextensive with the scope of the privilege', which only occurs if direct and derivative-use immunity is granted.[4] In instances where the privilege is breached without such grant of immunity, exclusion of the evidence is required.[5]

Over recent decades, the courts of the US have developed two doctrines that require brief explanation in order to understand how those courts have resolved applications for a compelled production order. These are the act of production and foregone conclusion doctrines. In the US, the privilege only applies to testimonial evidence, which has been described as a communication that 'must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a "witness" against himself'.[6] Importantly, the privilege does not ordinarily apply to pre-existing, real evidence, such as bodily samples.[7] This would suggest it is inapplicable to encrypted files, which are pre-existing evidence.

In certain instances, however, the privilege can apply to physical, pre-existing evidence. This can occur through the act of production doctrine. In *Fisher v United States*,[8] 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.[9] The Fifth Amendment only applied when the accused was compelled to make an

---

3 *United States Constitution* amend V.

4 *Kastigar v United States*, 406 US 441, 449 (Powell J) (1972). See also *Murphy v Waterfront Commission of New York Harbor*, 378 US 52, 54, 79 (Goldberg J) (1964) 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'.

5 See, eg, *Miranda v Arizona*, 384 US 436, 491–2 (Warren J) (1966).

6 *Doe v United States*, 487 US 201, 210 (Blackmun J) (1988) ('*Doe*'). Stated differently, '[the] content itself must have testimonial significance': at 211 n 10. Later in his opinion, Blackmun J spoke of how the privilege against self-incrimination ('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': at 213.

7 *Holt v United States*, 218 US 245 (1910) (accused could be compelled to wear a specific item of clothing); *Schmerber v California*, 384 US 757, 761 (Brennan J) (1966) (the privilege was not applicable to blood tests); *United States v Wade*, 388 US 218, 222 (Brennan J) (1967) (voice exemplars can be compelled); *United States v Dionisio*, 410 US 1 (1973) (voice exemplars can be compelled); *Gilbert v California*, 388 US 263, 266–7 (Brennan J) (1967) (handwriting exemplars can be compelled); *United States v Mara*, 410 US 19 (1973) (handwriting exemplars can be compelled).

8 425 US 391 (1976) ('*Fisher*').

9 Ibid 402 (White J).

incriminating testimonial communication.[10] Simply, the documents had been voluntarily prepared by someone other than Fisher and as such the privilege did not attach to them.[11]

However, the Court further held that independently of the content of a document, the act of producing a document can have 'communicative aspects' if it 'concedes the existence of the papers demanded and their possession or control by the taxpayer'.[12] The act of production can also authenticate the evidence.[13] 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.[14]

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,[15] and the state is able to establish the authenticity of the documents independently of information provided by the defendant.[16] In such instances, the production of the documents is a matter of surrender, not testimony.[17] This exception is known as the foregone conclusion doctrine.

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.[18] 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.[19] 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.[20] There was therefore no testimonial component in producing the documents.

---

10 Ibid 408–9. But see the statements by Brennan J at 423 in which he rejects this analysis.

11 Ibid 409. See also at 397 where it was said that '[the] 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'.

12 Ibid 410. See also *United States v Doe*, 465 US 605, 614 (Powell J) (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.

13 *Fisher* (n 8) 410 (White J). For a discussion of this case and the act of production doctrine, see Phillip R Reitinger, 'Compelled Production of Plaintext and Keys' [1996] (1) *University of Chicago Legal Forum* 171, 180–6.

14 *Fisher* (n 8) 411 (White J). 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.

15 Ibid.

16 See *United States v Bright*, 596 F 3d 683, 693 (Fisher J) (9th Cir, 2010), 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 n 125.

17 *Fisher* (n 8) 411 (White J), quoting *Re Harris*, 221 US 274, 279 (Holmes J) (1911).

18 Ibid 411.

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

20 Ibid 413.

Later decisions have clarified the scope of the act of production doctrine. In *Doe v United States*, 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'.[21] 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.[22] In the later decision in *United States v Hubbell*, the Supreme Court spoke of the act of production doctrine being enlivened when a defendant is required to make 'extensive use of "the contents of his own mind"' to identify the requisite documents, thereby rendering the act of production testimonial.[23] 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.

B How the Privilege Has Been Applied to Compelled Production Orders

Before analysing how the courts of the US have applied the principles discussed above, it is necessary to briefly note the source of the courts' authority to grant a compelled production order. While, as will later be seen, Australia and England and Wales have enacted statutory provisions to grant the necessary authority, in the US, authority in federal courts is given under the *All Writs Act* ('*AW Act*'),[24] which provides that 'the Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law'.[25]

The primary area of disagreement that has arisen in the courts of the US is in the application of the act of production and foregone conclusion doctrines, which have been relied upon in almost all cases involving compelled production orders. This is significant as the courts of the US have accepted that the compelled production of a password is a testimonial act that engages the privilege, a conclusion based on the finding that the act of production doctrine is engaged by the production of a

21 *Doe* (n 6) 210 (Blackmun J). In *United States v Hubbell*, 530 US 27, 35 (Stevens J) (2000) ('*Hubbell*'), the Court spoke of communications that related 'either express or implied assertions of fact or belief'.

22 *Doe* (n 6) 210. The Supreme Court made similar statements in its later decision in *Hubbell* (n 21) 35.

23 Ibid 43.

24 *All Writs Act 1789*, 28 USC § 1651 ('*AW Act*').

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

password.[26] The result of that conclusion is that a compelled production order can only be granted if the foregone conclusion doctrine is satisfied.[27]

While the discussion in the remainder of Part II(B) is based on the finding that the foregone conclusion doctrine can be *applied* to compelled production orders,[28] a recent case has held that the foregone conclusion doctrine is a narrow one that was never intended to be used for compelled production orders. In *Commonwealth v Davis*, a decision of the Supreme Court of Pennsylvania, the Court, by a 4:3 majority, held that the foregone conclusion doctrine was 'inapplicable to compel the disclosure of a defendant's password'.[29] This conclusion was based on the majority's earlier finding that the doctrine is 'an extremely limited exception to the Fifth Amendment privilege against self-incrimination'.[30] In a similar vein, in *Seo v State*, a 3:2 majority of the Indiana Supreme Court opined that there were reasons for not applying the foregone conclusion doctrine to an application to compel a suspect to decrypt an encrypted device.[31] For now, however, these decisions – both delivered by the narrowest of majorities – remain a minority view against a broad consensus that the foregone conclusion doctrine can be applied to compelled production orders.

When courts apply the foregone conclusion doctrine to compelled production orders, two issues in particular arise: what evidence must the applicant have regarding the suspect's knowledge of the password; and what evidence must the applicant have about the contents of the encrypted drive? As Australian courts have also raised concerns with the evidentiary burden that must be satisfied before a compelled production order can be made,[32] how the courts of the US have resolved these issues may be of assistance.

---

26 See, eg, *State v Andrews*, 234 A 3d 1254, 1285 (Solomon J) (NJ, 2020) ('*Andrews*') ('the cases agree that an act of production is involved in compelling disclosure of a passcode'); *Commonwealth v Davis*, 220 A 3d 534, 548 (Todd J) (Pa, 2019) ('*Davis*'); *Grand Jury Subpoena* (n 25); *Apple MacPro Computer* (n 25) 247–8 (Vanaskie J) (3rd Cir, 2017). See also Orin S Kerr, 'Compelled Decryption and the Privilege against Self-Incrimination' (2019) 97(4) *Texas Law Review* 767, 779.

27 There is a further, secondary debate in the United States ('US') about the significance of the form of the order that is sought. Two possible orders have been considered by the courts: an order to compel the suspect to enter the password into the encrypted device; and an order to compel the suspect to disclose the password. That discussion is beyond the scope of this article. Overwhelmingly, the courts of the US recognise that the act of production and foregone conclusion doctrines apply regardless of the form of order. As the form of order is not relevant in Australia, there is limited utility in entering that debate here. While there is some recent case law that argues that the foregone conclusion doctrine does not apply to compelled production cases, those cases remain outliers for now: see *Davis* (n 26) in respect of a compelled entry order; *Seo v State*, 148 NE 3d 952, 962 (Rush CJ) (Ind, 2020) ('*Seo*') in respect of compelled disclosure.

28 Note that this does not refer to the doctrine being satisfied on the facts; it only refers to the finding that the foregone conclusion doctrine is applicable to compelled production orders regardless of whether it is made out on the facts.

29 *Davis* (n 26).

30 Ibid 549 (Todd J).

31 *Seo* (n 27). The majority's statements on this issue were obiter as the foregone conclusion was not enlivened on the facts.

32 See, eg, *Luppino v Fisher [No 2]* (2019) 278 A Crim R 550 ('*Luppino [No 2]*').

1 Knowledge of the Password

In order to satisfy the foregone conclusion doctrine, the prosecution must satisfy the court that the suspect knows the password. At times, this question is easily answered due to the overwhelming, or underwhelming, nature of the evidence. For example, in *United States v Apple MacPro Computer*, in which the court found that this knowledge was present, the government was able to establish that the suspect possessed and owned the devices;[33] 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.[34] By contrast, in *Commonwealth v Jones*,[35] 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.[36]

Where the facts lie between these extremes, however, the case law shows at times substantial differences in what evidence needs to be led to satisfy that requirement. At its most lenient, several courts have found this element to be satisfied where the electronic device in question belongs to the suspect and is in that person's possession or control.[37] Other courts, however, have required more. In *Re Grand Jury Subpoena to Sebastian Boucher*, for example, Neidermeier J found that it was 'not without question' that Boucher knew the encryption key despite the laptop being found in Boucher's possession and Boucher acknowledging ownership of it.[38] This approach has been endorsed by other courts.[39]

To date, regrettably, there is no consistent approach as to what is required to satisfy this evidentiary burden.

---

33 *Apple MacPro Computer* (n 25) 248 (Vanaskie J).

34 Ibid 249. See also *People v Johnson*, 90 NE 3d 634, 637 (Pierce PJ) (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 (Blackburn J) (D Colo, 2012) ('*Fricosu*') where the defendant was heard admitting to a fellow suspect that she was storing the information sought by the Federal Bureau of Investigation on her computer, and that it was protected through encryption.

35 *Commonwealth v Jones*, 34 Mass L Rptr 287 (Mass, 2017) ('*Jones*'). Although, the decision was overturned on appeal once further information had been provided.

36 Ibid slip op 4.

37 See, eg, *Andrews* (n 26) 1275 (Solomon J) where the Court found that the doctrine was satisfied where 'the cellphones were in Andrews' possession when seized and that he owned and operated the cellphones'; *United States v Gavegnano*, 305 Fed Appx 954, 956 (Moon J) (4th Cir, 2009) ('*Gavegnano*') where it was sufficient that Gavegnano was 'the sole user and possessor of the computer'; *State v Stahl*, 206 So 3d 124, 134 (Black J) (Fla Ct App, 2016) ('*Stahl*') where it was sufficient to establish that the phone in question belonged to Stahl, who had possession and control of it; *Re the Search of a Residence in Aptos, California 95003* (ND Cal, No 17-mj-70656-JSC-1, 20 March 2018) where it was sufficient that the phone was found in the suspect's possession.

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

39 *Grand Jury Subpoena* (n 25) 1344 (Tjoflat J); *Seized Data Storage System* (n 25); *State v Trant* (Me Super Ct, No 15-2389, 22 October 2015) ('*Trant*').

2 Knowledge of the Contents of the Encrypted Drive: Control v Contents Test

It is this element that is the most contentious of the two, one that has given rise to two competing interpretations of the foregone conclusion doctrine.[40] Those competing approaches can be described as the control test and the contents test. Under the control test, the applicant must produce evidence that the suspect has possession or control of the electronic device and that they know what the password is. The contents test adds a further requirement to those: the applicant must provide evidence that they know with reasonable particularity what is contained on the encrypted drive.[41] What the reasonable particularity test demands is that although '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'.[42]

The two competing approaches have arisen 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).

(a) The Contents Test

The leading case adopting the contents test is *Re Grand Jury Subpoena Duces Tecum* ('*Grand Jury Subpoena*'), delivered by the Court of Appeal for the Eleventh Circuit. In this matter, law enforcement officials sought to compel the accused to decrypt several electronic devices that were found in his possession in his hotel room. In considering whether the privilege had been infringed, the Court noted

---

40 Several writers have recognised these two competing understandings of what is required under the foregone conclusion doctrine. See, eg, Orin Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106(4) *Georgetown Law Journal* 989, 1002–3 <http://dx.doi.org/10.2139/ssrn.2938033> though the authors note that at the time of writing the courts have not resolved this question; Kerr (n 26) 767; Dan Terzian, 'Forced Decryption as a Foregone Conclusion' (2015) 6 (May) *California Law Review Circuit* 27, 27. See also Jamil N Jaffer and Daniel J Rosenthal, 'Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge' (2014) 24(2) *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.

41 The reasonable particularity standard has been adopted by most courts hearing compelled production orders: *Grand Jury Subpoena* (n 25) 1344 (Tjoflat J); *Boucher I* (n 38) slip op 3–4; *United States v Pearson* (ND NY, No 1:04-CR-340, 24 May 2006); *Commonwealth v Gelfgatt*, 11 NE 3d 605, 621 (Lenk J, dissent) (Mass, 2014); *Seized Data Storage System* (n 25) slip op 8; *Apple MacPro Computer* (n 25) 247 (Tjoflat J); *Stahl* (n 37) 135 (Black J); *Trant* (n 39) slip op 3; *Seo v State*, 109 NE 3d 418, 436 (Mathias J) (Ind Ct App, 2018) ('*Seo II*'); *Jones* (n 34); *GAQL v Florida*, 257 So 3d 1058 (Fla App 4 Dist, 2018) ('*GAQL*'). 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 Kerr (n 26) 775 where the author discusses the application of the reasonable particularity standard.

42 *Stahl* (n 37) 135–6 (Black J), citing *United States v Greenfield*, 831 F 3d 106 (2nd Cir, 2016). In *Grand Jury Subpoena*, the Court spoke of the need for the government to be able to demonstrate that the files were present on the encrypted drive: *Grand Jury Subpoena* (n 25) 1348–9 (Tjoflat J).

that while the files to which access was sought were not testimonial evidence (as they were pre-existing), 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.[43] For the foregone conclusion doctrine to be satisfied, the government needed to know with reasonable particularity that the files to which access was sought were on the encrypted drive,[44] which required more than a mere suspicion that the documents existed.[45]

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'.[46] As for the foregone conclusion doctrine, the Court held that it had not been enlivened. The government, the Court found, did not know what, if anything, was contained on the hard drives, and could not demonstrate that Doe could access the drives.[47] This finding was made despite the fact that as part of their 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, and the encrypted drives were found in his possession while staying at a hotel.[48] The Court contrasted this finding with the appeal decision in *Re Grand Jury Subpoena to Sebastian Boucher*,[49] in which the government knew of the existence of file names indicative of child pornography.[50] 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]'.[51]

A further important finding of the Court concerned bodily samples. After reviewing *Fisher*[52] and *Hubbell*,[53] the Court held that the privilege is not engaged through the compulsion of a merely physical act that does not require the defendant

43 *Grand Jury Subpoena* (n 25) 1342 (Tjoflat J).
44 Ibid 1343.
45 Ibid 1344.
46 Ibid 1346. Most cases that adopt the contents test use similar language. See, eg, *Fricosu* (n 34) 1236 (Blackburn J); *Seized Data Storage System* (n 25); *Trant* (n 39) slip op 3.
47 *Grand Jury Subpoena* (n 25) 1346 (Tjoflat J).
48 Ibid 1339.
49 (D Vt, No 2:06-mj-91, 19 February 2009) ('*Boucher II*').
50 *Grand Jury Subpoena* (n 25) 1349 (Tjoflat J). 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.
51 *Seo II* (n 41) 434 (Mathias J). See also *GAQL* (n 41) 1063 (Levine J). 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.
52 *Fisher* (n 8).
53 *Hubbell* (n 21).

to use the contents of his mind as it does not engage the act of production doctrine.[54] This finding is particularly relevant to decryption through the use of a biometric feature, such as a fingerprint, and on this question the courts of the US have been relatedly consistent in holding that decryption through such means does not engage the privilege as providing a fingerprint does not require a suspect to communicate any knowledge or make a factual assertion.[55]

Sacharoff, writing in support of the contents test, argues that using a password to unlock an encrypted device reveals not only knowledge of the password, but 'that the device likely belongs to the person and that the person possesses, perhaps knowingly, the files on the device'.[56] He reaches this conclusion for two reasons. First, because the act of production doctrine as applied to physical documents asks whether the government knows that the documents exist and that the suspect possesses them.[57] The focus, therefore, is on the documents, not on the act. Arguably, what is overlooked in this comparison, however, is that what is requested in the document scenario are the actual documents; what is requested in the compelled production scenario, however, is the password. Sacharoff appears to disregard 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. Secondly, Sacharoff argues that all act of production testimony is inferential.[58] The act of production doctrine is not concerned with verbal statements made by the suspect but with the inferences that can be drawn from an act by the suspect. So understood, any attempt to distinguish between inferences and testimony – as Kerr, a proponent of the control test seeks to do – is not possible; rather, we are left to ask which implied assertions 'accompany the act'.[59] For advocates of the contents test, knowledge of the contents of the device is an implied assertion that necessarily accompanies the act of decryption.

As to what level of evidence is required to satisfy the reasonable particularity test, the strict approach adopted in *Grand Jury Subpoena* has been applied by other courts, including one decision where a court held that there was insufficient evidence that the suspect used a particular messaging app despite the existence of a witness who could testify that she had messaged the suspect on the suspect's phone using the messaging app in question.[60] Other courts, however, have been satisfied by evidence that files with filenames indicative of child pornography, or

54 *Grand Jury Subpoena* (n 25) 1345 (Tjoflat J). The Court noted the 'famous' example of the key to the lock of a safe as an example of such compulsion.

55 *Commonwealth v Baust*, 89 Va Cir 267 (2014); *Stahl* (n 37) 135 (Black J); *State v Diamond*, 890 NW 2d 143, 150 (Smith J) (Minn App, 2017); *State v Diamond*, 905 NW 2d 870, 872 (Chutich J) (Minn, 2018) ('*Diamond*'); *Re Search Warrant Application for [Redacted Text]*, 279 F Supp 3d 800, 803 (Chang J) (ND Ill, 2017); Kerr and Schneier (n 40) 1002.

56 Laurent Sacharoff, 'What Am I Really Saying when I Open My Smartphone: A Response to Orin S Kerr' (2019) 97 *Texas Law Review Online* 63, 67.

57 Ibid 68.

58 Ibid 69.

59 Ibid 70.

60 *GAQL* (n 41).

hash values that correspond with known child pornography,[61] are found to have been received, distributed or stored on the electronic device in question.[62]

More broadly, 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.

(b) The Control Test

As noted previously, 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*,[63] the Court stated that

> [t]he 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 'foregone conclusion'.[64]

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.[65]

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 *United States v Apple MacPro Computer*,

---

61 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.

62 *Apple MacPro Computer* (n 25) (in this matter there was also evidence from a witness that she had seen child pornography on the computer in question); *Seized Data Storage System* (n 25).

63 11 NE 3d 605 (Mass, 2014).

64 Ibid 615 (Spina J).

65 Kerr made this same argument in a recent article: Kerr (n 26) 782–3. See also *United States v Spencer* (ND Cal, 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; *Re the Search of A Residence in Aptos* (ND Cal, No 17-mj-70656-JSC-1, 20 March 2018) slip op 6 where the Court held 'that the testimony inhering to the act of decryption is that Mr Spencer knows the encryption password. The act of decryption requires nothing more'. One further case makes the same point, though it is unclear from that decision whether the order sought the act of decryption or some other form of order: *Stahl* (n 37) 134 (Black J) (producing the password does not involve an acknowledgement that one knows the contents of the device).

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*"'.[66] 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.

In endorsing the control test, Kerr, the leading academic proponent of the control test, rejects the argument of Sacharoff that the act of decrypting an encrypted device implicitly communicates that the person has knowledge of the contents of the device.[67] The key distinction, Kerr argues, is between the testimonial statement actually made by the suspect (which is that the suspect knows the password) and the inferences that can be drawn from that statement (which include that the suspect knows what is on the encrypted device). It is only the former that is relevant to the foregone conclusion doctrine as 'the ability to draw an inference from testimony does not amount to testimony about that inference'.[68]

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.[69] 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 content test imposes its further evidentiary burden, but the control test does not.[70]

Thus, the burden imposed under the control test differs from that imposed under the contents 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 of the subpoena to search and seize the electronic device is issued (rather than at the stage that the compelled production order is sought).

---

66 *Apple MacPro Computer* (n 25) 248 (Vanaskie J) (emphasis added).

67 Kerr (n 26) 780.

68 Ibid.

69 Note, however, that the probable cause requirement will ordinarily be satisfied without difficulty: Laurent Sacharoff, 'Unlocking the Fifth Amendment: Passwords and Encrypted Devices' (2018) 87 *Fordham Law Review* 203, 214.

70 This process is demonstrated in *Grand Jury Subpoena*, in which 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: *Grand Jury Subpoena* (n 25) 1339 (Tjoflat J). To search the encrypted devices, however, a compelled production order was required. On the facts of *Grand Jury Subpoena*, that order was not issued partly because the applicant failed to satisfy the knowledge requirement concerning the contents of the encrypted devices. See also *Trant* (n 39); *Stahl* (n 37); *Diamond* (n 55).

III ENGLAND AND WALES AND THE EUROPEAN COURT OF HUMAN RIGHTS

A Background on the Privilege

In England and Wales, the application of the privilege is governed by article 6 of the *Human Rights Act 1998* (UK), which guarantees the right to a fair trial. Though the privilege is not mentioned in the text of article 6, 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'.[71] Importantly, the interpretation of article 6 is guided by the decisions of the European Court of Human Rights under the *Convention for the Protection of Human Rights and Freedoms* (commonly known as the *European Convention on Human Rights* or '*ECHR*').[72]

Unlike the US, the privilege is not absolute and may be abrogated by statute, either expressly or by necessary implication.[73] Where a statute compels 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.[74] The privilege does not ordinarily apply to pre-existing evidence,[75] but where such evidence was obtained through coercion or oppression, it would be a breach of the privilege.[76] Improper coercion or oppression of that nature will be present where a suspect faces a threat of sanction if they do not comply,[77] or physical or psychological pressure that breaches article 3 of the *ECHR* is applied to the suspect.[78]

---

71 *Saunders v United Kingdom* (1997) 23 EHRR 313, 337 [68] ('*Saunders*').

72 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) ('*ECHR*'). Under section 3 of the *Human Rights Act 1998* (UK), English courts are required to take account of any decision of the European Court of Human Rights that relates to a *ECHR* right.

73 *Beghal v Director of Public Prosecutions* [2016] AC 88, 118 [63] (Lord Hughes). 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* [2009] EWCA Crim 1640, [19] (Moore-Bick LJ); *Phillips v News Group Newspapers Ltd* [2013] 1 AC 1, [11] (Lord Neuberger MR); *R v Mushtaq* [2005] UKHL 25, [49] (Lord Rodger).

74 *Beghal v Director of Public Prosecutions* [2016] AC 88, 118 [63] (Lord Hughes).

75 See, eg, *Saunders* (n 71) 337–8 [69] where it was said that

> *[t]he 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* (emphasis added).

76 *Volaw Trust and Corporate Services Ltd v The Office of the Comptroller of Taxes* [2019] UKPC 29, [43] (Lord Reed) ('*Volaw Trust*').

77 See, eg, *JB v Switzerland* (European Court of Human Rights, Chamber, Application No 31827/96, 3 May 2001).

78 *Volaw Trust* (n 76) [43] (Lord Reed).

B How Have the Courts of England and Wales Resolved Applications to Produce a Password?

1 Does the Privilege Apply to a Compelled Production Order?

Compelled production orders are authorised under Part III of the *Regulation of Investigatory Powers Act 2000* (UK) ('*RIPA*'). Under section 49, a notice may be issued to a suspect requiring that person to disclose the encryption key to an encrypted device. The leading decision on these provisions and the role of the privilege is that of the Court of Appeal in *R v S (F)*.[79] The defendants were served section 49 disclosure notices requiring them to produce the encryption keys to a computer on which one of the defendants was caught part way through entering the encryption key (which he did not thereafter enter in full once the police entered the room he was in). The defendants refused to comply with the notices on the basis that they were incompatible with the privilege against self-incrimination.

At first instance, Stephens J 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'.[80] 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.[81] 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 … 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.[82]

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.[83] That conclusion notwithstanding, Lord Judge CJ proceeded

79 [2009] 1 WLR 1489 ('*R v S (F)*').
80 Ibid 1494 [15] (Lord Judge CJ, Penry-Davery and Simon JJ).
81 Ibid 1495–6 [18] (Lord Judge CJ, Penry-Davery and Simon JJ), citing *Saunders* (n 71); *Attorney General's Reference (No 7 of 2000)* [2001] 2 Cr App R 19; *R v Kearns (Nicholas Gary)* [2003] 1 Cr App R 7.
82 *R v S (F)* (n 79) 1496 [20] (Lord Judge CJ, Penry-Davery and Simon JJ).
83 Ibid 1497 [21].

to note that 'the fact of the defendant's *knowledge* of the keys may itself be an incriminating fact'.[84] This, Lord Judge CJ noted, was the approach adopted in the US in *Boucher I*. His Lordship thus adopted an approach broadly consistent with the act of production doctrine in the US, one in which the privilege 'may' be engaged by a requirement to provide an encryption key.[85]

2 Abrogation of the Privilege

As a suspect's knowledge of the encryption key may engage the privilege, does *RIPA* have the effect of abrogating the privilege? Although *RIPA* does not expressly provide for the abrogation of the privilege, the Court of Appeal has found that the statutory provisions have that effect. In *R v S (F)*, 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*,[86] his Lordship noted that some curtailment of the privilege was necessary and accepted as being 'indispensable to the stability of society'.[87] The privilege was, accordingly, subject to 'numerous statutory exceptions which limit, amend or abrogate [it] in specified circumstances' provided the limitation did not compromise the fairness of the trial under article 6 of the *ECHR*.[88] 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'.[89]

After finding that a requirement to provide an encryption key implicated the privilege where the data discovered using that encryption key was incriminating,[90] his Lordship stated that the determinative question was whether any interference with the privilege imposed by a disclosure notice was 'proportionate and permissible'.[91] 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

84 Ibid (emphasis in original).

85 Ibid 1498 [24]. This approach was followed in the later decision of *Greater Manchester Police v Andrews* [2011] EWHC 1966 (Admin) ('*Greater Manchester Police*') where it was held that the privilege had been engaged by the requirement to provide the encryption key as doing so revealed 'the fact of the defendant's knowledge of the keys': at [17] (McCombe J).

86 [1993] AC 1.

87 *R v S (F)* (n 79) 1494–5 [17] (Lord Judge CJ, Penry-Davery and Simon JJ), citing *R v Director of Serious Fraud Office; Ex parte Smith* [1993] AC 1, 31 (Lord Mustill).

88 *R v S (F)* (n 79), 1494–5 [17] (Lord Judge CJ, Penry-Davery and Simon JJ).

89 Ibid. His Lordship proceeded to quote a passage from Lord Bingham in *Brown v Stott* 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': ibid, citing *Brown v Stott* [2003] 1 AC 681, 704 (Lord Bingham).

90 *R v S (F)* (n 79) 1498 [24] (Lord Judge CJ, Penry-Davey and Simon JJ).

91 Ibid 1498 [25].

> 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 … and in relation to any subsequent trial, the powers under section 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 defendant's knowledge of the key or means of access, remain. Neither the process, nor any subsequent trial can realistically be stigmatised as unfair.[92]

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 section 78 of the *Police and Criminal Evidence Act 1984* (UK).[93] Notably, to date, no court decision has found that compelled production orders under *RIPA* destroy the essence of the privilege. Thus, while the existence of article 6 regulates the use of *RIPA*, it does not prohibit the granting of orders under it.

3 The Level of Knowledge Required for an Order to Be Issued

Unlike their counterparts in the US, the courts of England and Wales have shown a reluctance to be unduly hampered by the evidentiary burdens required to be satisfied before a compelled production order can be granted. With regards to knowledge of the contents of the encrypted drive, in *R v S (F)* orders were made in respect of three separate encrypted drives found at different locations. One defendant, S, owned two of the drives; the third was owned by the second defendant. On one of the drives owned by S, illegal material was found. On the basis of that material, the orders were granted in respect of the second device owned by S and the device owned by the second defendant. The granting of the order in respect of the second defendant shows a relatively generous approach to the level of evidence required as the only evidence that illegal material was on his computer was the second defendant's relationship with S.

The same is true of evidence of knowledge of the password. In *Greater Manchester Police v Andrews*, the defendant, a convicted sex offender, was arrested on suspicion of having breached a Sexual Offences Prevention Order

92 Ibid. This passage was cited with approval by McCombe J in *Greater Manchester Police* (n 85) [16].

93 Section 78 of the *Police and Criminal Evidence Act 1984* (UK) 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'.

which prohibited him from looking at photographs of children.[94] 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 section 49 of the *RIPA* for the defendant to provide the encryption key to the memory sticks. After the application failed at first instance, an appeal was brought before the High Court. Hearing the appeal, McCombe J found that it was 'a perfectly legitimate inference to draw'[95] 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.[96] May P agreed and, in overturning the lower court decision, he held that 'the facts of the present case falls so far in favour of a disclosure requirement that the judge's decision must be wrong'.[97] In England and Wales, then, ownership or possession of the device in question is sufficient to satisfy the evidentiary burden. This shows a fairly marked departure from one line of authority in the US, in which more than mere possession is required before the court will be satisfied that the suspect knows the password to the encrypted device (or, indeed, what is contained on it).[98]

IV CANADA

A Background on the Privilege

Like the US, Canada grants the privilege constitutional protection in the *Canadian Charter of Rights and Freedoms*.[99] One consequence of this is that any statutory abrogation of the privilege requires a grant of immunity that operates in the same manner as the privilege that it displaces.[100] As the purpose of the privilege is to prevent a person from being conscripted to provide evidence against themselves,[101] 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

94 *Greater Manchester Police* (n 85) [2] (McCombe J). 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.

95 Ibid [21].

96 Ibid [3]–[4].

97 Ibid [28] (May P). This decision is to be preferred to that in *Grand Jury Subpoena* (n 25). There is no evidence in the *Grand Jury Subpoena* 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.

98 See, eg, *Seized Data Storage System* (n 25) slip op 8; *Grand Jury Subpoena* (n 25) 1346 (Tjoflat J). In both cases, possession of the devices was insufficient to satisfy the evidentiary burden concerning knowledge of the encryption key.

99 *Canada Act 1982* (UK) c 11, sch B pt I ('*Canadian Charter of Rights and Freedoms*'). In the context of compelled production cases, that protection is primarily found in section 7, though at least one court has also considered section 11(d): *R v Talbot* [2017] ONCJ 814.

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

101 Ibid [88].

disclosure'.[102] Where evidence has been obtained in breach of the privilege, its exclusion from trial is determined under section 24(2) of the *Canadian Charter of Rights and Freedoms*. That requires the court to assess:

> (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.[103]

Under that test, statements made by an accused in breach of the privilege remain presumptively inadmissible;[104] physical evidence such as bodily samples, however, 'are not communicative in nature', thereby 'weakening self-incrimination as the sole criterion for determining their admissibility'.[105]

B A Prohibition on Compelling the Production of a Password in the Absence of a Targeted Statutory Framework

Under current Canadian case law, compelled productions orders are not permitted on the basis that they constitute an infringement of the privilege. Arguably, the leading Canadian decision on this issue is that of the Court of Appeal of Quebec in *R v Boudreau-Fontaine* ('*Boudreau-Fontaine*').[106] In this matter, the accused had been arrested in his motor vehicle for allegedly breaching the terms of his parole which prohibited him from accessing the internet. The suspect was using his computer at the time of arrest, which he turned off upon arrest. Police obtained a warrant to compel the accused to produce the password to encrypted files on the computer, with which he complied. Subsequently, the accused sought to exclude evidence found through the use of the password on the basis that his privilege had been infringed. He was successful at trial and the Crown failed to overturn that finding on appeal. The Court of Appeal held that the order to provide the password 'was commanding the appellant to give essential information with the specific intent of having him incriminate himself'.[107] The law, the Court further noted, 'will not allow an order to be joined compelling the respondent to self-incriminate'.[108] As such, the evidence found through the use of the password was to be excluded from trial notwithstanding its very high reliability.[109]

Importantly, the Court further identified a concern with the source of the power for the warrant. The warrant purported to authorise the computer search on the basis of sections 487(2.1) and 487(2.2) of the *Criminal Code*, which provided a general power to 'use or cause to be used any computer system' found during a

102 Ibid [170].
103 *R v Grant* [2009] 2 SCR 353, [71] (McLachlin CJC and Charron J).
104 Ibid [92].
105 Ibid [105].
106 [2010] QCCA 1108.
107 Ibid [39] (Doyon JA, Pelletier and Léger JJA agreeing at [3]).
108 Ibid.
109 Ibid [71].

search.[110] 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'.[111]

Subsequent lower court decisions have, however, held that the power to order a compelled production order could be found in the *Criminal Code*. In *R v Talbot,* a single judge of the Ontario Court of Justice held that a compelled production order fell within the scope of section 487.02 of the *Criminal Code*, but that such an order nevertheless infringed the privilege.[112] The same conclusion was reached by a single judge of the same court in *R v Shergill* ('*Shergill*').[113] While both of those decisions applied to the entry of a passcode into the encrypted device, a different conclusion has been reached in respect of the use of a fingerprint to unlock an encrypted device. In *Re Impression Warrant Application (s. 487.092)*,[114] the Crown sought to compel the suspect to use his fingerprint to unlock his phone. It relied on section 487.092(1) of the *Criminal Code* for authority to do so, which authorised the taking of a bodily sample such as a fingerprint.[115]

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.[116] It did not, however, authorise the taking of a fingerprint to continue a search.[117] On that basis the application was denied.[118] Furthermore, in a brief obiter, Conacher JP noted the 'residual concern' that providing the fingerprint would require the suspect to assist the police in their

110 *Criminal Code*, RSC 1985, c C-46 ('*Canadian Criminal Code*'):

> (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 …

111 *R v Boudreau-Fontaine* [2010] QCCA 1108, [46] (Doyon JA, Pelletier and Léger JJA agreeing at [3]).

112 [2017] ONCJ 814, [15], [38] (Applegate J).

113 [2019] ONCJ 54, [8] (Downes J) ('*Shergill*').

114 [2016] ONCJ 197 ('*Re Impression Warrant Application*').

115 *Canadian Criminal Code* (n 110):

> 487.092 (1) 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.

116 *Re Impression Warrant* (n 114) [11] (Conache JP).

117 Ibid [12].

118 Ibid [14].

investigation in a manner that appeared to infringe the privilege. His Honour further noted, however, that he did not need to decide that issue.[119]

While these decisions suggest some level of certainty about the Canadian position, such an impression may be deceiving. In the first place, with the exception of *Boudreau-Fontaine*, the issue of compelled production orders has been discussed in the various provinces' lower courts. A thorough appellate court discussion of this issue remains outstanding. Secondly, there is reason to believe that the introduction of a statutory response specifically addressing compelled production orders may result in a different outcome. In *Re Impression Warrant Application (s. 487.092)*, the absence of a specific statutory provision authorising such an order was fatal to the Crown's application for a compelled production order. A statutory response would remedy that failing. Perhaps more important though is the idea, expressed in *Shergill*, that '[i]t may be that a different approach to this issue is warranted, whether through legislative initiatives or modifications to what I see as jurisprudence which is binding on me'.[120] This statement followed from the Court's earlier recognition that 'the current digital landscape as it relates to effective law enforcement and the protection of privacy presents many challenges'.[121] With the Canadian approach proving less receptive to compelled production orders than any of the comparative jurisdictions, the Court in *Shergill* appears to recognise that the current Canadian position may require a response from either the legislature or the country's highest court. Until such time as this issue is addressed by the legislature or the Canadian Supreme Court, the primary lesson to be taken from the Canadian jurisprudence may be the importance of having this issue resolved either by statute or the country's highest court.

V AUSTRALIA

A Background on the Privilege

Though the Australian High Court has stated that the privilege against self-incrimination is a right that is 'deeply ingrained in the common law',[122] one that acts as '[a] fundamental bulwark of liberty',[123] its operation in Australia is markedly different to that in Canada and the US. This is because the privilege in Australia rests on different moorings to the comparator jurisdictions as it does not

119 Ibid [15].

120 *Shergill* (n 113) [51] (Downes J).

121 Ibid.

122 *Sorby v Commonwealth* (1983) 152 CLR 281, 309 (Mason, Wilson and Dawson JJ) ('*Sorby*'); *Reid v Howard* (1995) 184 CLR 1, 5 (Deane J), 11 (Toohey, Gaudron, McHugh and Gummow JJ) ('*Reid*'). See also *Environmental Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 532 (Deane, Dawson and Gaudron JJ) ('*Caltex Refining*'); *X7 v Australian Crime Commission* (2013) 248 CLR 92, 136–7 [104] (Hayne and Bell JJ) (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).

123 *Pyneboard Pty Ltd v Trade Practices Commission* (1983) 152 CLR 328, 340 (Mason ACJ, Wilson and Dawson JJ) ('*Pyneboard*').

have constitutional – or in the case of England and Wales, quasi-constitutional – recognition. This means that the privilege can be abrogated with relative ease as 'the constitutional nature of this question [in the US] is materially different from the statutory question of construction which arises' in Australian law.[124] Given the importance of the privilege, however, it is presumed that the legislature does not intend for its abrogation.[125] Nevertheless, abrogation can occur by statute, through express words or by implication.[126]

While the privilege affords protection against both direct-use and derivative-use evidence,[127] where the privilege has been abrogated there is ordinarily no requirement for immunity to be provided.[128] 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.[129] In instances where the privilege has not been abrogated, it only applies to testimonial disclosures.[130] Notably, however, the privilege can be engaged through the production of pre-existing documents under threat of criminal sanction.[131] The High Court has held, however, that the privilege does not apply to bodily samples, and that '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

124 *A v Boulton* (2004) 207 ALR 342, 358 [64] (Kenny J) ('*Boulton II*'). See also *Caltex Refining* (n 122) 490 (Mason CJ and Toohey J).

125 *Sorby* (n 122) 289 (Gibbs CJ).

126 Ibid 289 (Gibbs CJ), 309 (Mason, Wilson and Dawson JJ); *Police Service Board v Morris* (1985) 156 CLR 397, 409 (Wilson and Dawson JJ) (where the court held that 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'); *Pyneboard* (n 123) 341 (Mason ACJ, Wilson and Dawson JJ); *Mortimer v Brown* (1970) 122 CLR 493 (where the Court recognised that abrogation may be implied if a failure to do so undermines the purpose of the statute). See also *R v Hooper*, in which the Full Court of the South Australian Supreme Court found that a motor vehicle reporting obligation impliedly abrogated the privilege for reasons that included: the questions that were capable of being asked of the suspect were strictly limited; 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; and it would be impractical to expect a police officer to adjudicate on whether a claim of privilege was reasonable: *R v Hooper* (1995) 64 SASR 480, 486 (Cox J) ('*Hooper*').

127 *Reid* (n 122) 6 (Deane J); *Sorby* (n 122) 310 (Mason, Wilson and Dawson JJ).

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

129 See, eg, *Sorby* (n 122) 316 (Brennan J); *Hamilton v Oades* (1989) 166 CLR 486 (in respect of the *Companies (New South Wales) Code 1981* (NSW)); *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* (2016) 263 A Crim R 503 (the *Crime and Misconduct Act 2001* (Qld)); *Boulton I* (n 128); *Boulton II* (n 124) (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, December 2015) 324 where a list of Commonwealth legislation abrogating the privilege is discussed.

130 *King v McLellan* [1974] VR 773, 776 (Gowans, Nelson and Anderson JJ).

131 Sorby (n 122) 288 (Gibbs CJ).

identified, or to speak or to write so that the jury or another witness may hear his voice or compare his handwriting'.[132]

B Compelled Production Orders in Australia

Compelled production orders are provided for under legislation enacted by the Commonwealth, South Australia, Queensland, Victoria and Western Australia. In the Parts that follow this article briefly describes those statutory provisions, before considering several issues that have arisen from their operation.

1 The Statutory Framework in Australia

At the federal level, section 3LA of the *Crimes Act 1914* (Cth) provides a mechanism through which access to encrypted material can be compelled. Section 3LA applies to computers and data storage devices that are seized pursuant to a warrant issued under section 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'.[133] Offences with a federal aspect include those involving an electronic communication,[134] which further includes any communication of information in the form of text, data or visual images.[135]

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 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, sections 154 and 154A of the *Police Powers and Responsibilities Act 2000* (Qld) ('*Police Powers Act*') 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 section 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 section 465AAA providing for a compelled production order to be included in a search warrant.[136] In Western Australia, section 59 of the *Criminal Investigation Act 2006* (WA) provides for the issuing of a data access order that can require a person to

132 Ibid 292. See also *Grollo v Bates* (1994) 53 FCR 218, 250 (Einfeld J) 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.

133 *Crimes Act 1914* (Cth) s 3C.

134 Ibid s 3AA(3)(e).

135 Ibid s 3AA(5).

136 Both provisions are materially identical.

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.

2 The Statutory Powers Infringe the Privilege

We have already seen that each of the comparator jurisdictions understand compelled production orders to infringe the privilege. The same is true of Australia. With regards to alphabetic and numeric passwords, in *Luppino v Fisher*,[137] a compelled production order was made using the specific powers provided under section 3LA of the *Crimes Act 1914* (Cth) ('*Crimes Act*'). 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.[138] The power to make the interlocutory orders was said to reside in section 23 of the *Federal Court of Australia Act 1976* (Cth), which provides that the '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'.[139] This power, then, is the equivalent of that granted to courts in the US by the *AW Act*.[140] Luppino opposed the interlocutory order on the grounds that it infringed the privilege.

White J had little hesitation in refusing the interlocutory relief. At the outset, his Honour noted that unlike section 3LA of the *Crimes Act*, the provision sought to be relied upon did not abrogate the privilege.[141] 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)'.[142] Such action was an infringement of the privilege.[143] With regard to the first order, White J held that

137 [2018] FCA 2106 ('*Luppino*').
138 Ibid [3]–[12] (White J).
139 Ibid [18].
140 *AW Act* (n 24).
141 *Luppino* (n 137) [22].
142 Ibid [28].
143 Ibid [27]. This finding is supported by reference to the Explanatory Memorandum and statement of compatibility to the Justice Legislation Amendment (Confiscation and Other Matters) Bill 2014 (Vic), which introduced section 465AA of the *Crimes Act 1958* (Vic) ('*Vic Crimes Act*') and which provide respectively that the compulsory powers 'expressly limit the right to self-incrimination' and 'arguably limit' the privilege: Explanatory Memorandum, Justice Legislation Amendment (Confiscation and Other Matters) Bill 2014 (Vic) 31 (Amended Print); Victoria, *Parliamentary Debates*, Legislative Council, 17 September 2014, 3096 (Martin Pakula). See also the Victorian Scrutiny of Acts and Regulations Committee, in commenting on the operation of section 465AAA, expressed the view that 'clause 9

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.[144] 'Given the fundamental nature of the common law privilege against self-incrimination', his Honour held, 'that course would be inappropriate'.[145] 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.[146]

While no cases have yet involved the use of a biometric encryption key, it is to be expected that decryption through such means will not infringe the privilege given the High Court's decision in *Sorby v Commonwealth* ('*Sorby*') that the privilege did not apply to evidence of the condition of a person's body, and that a person may be required to give a fingerprint or a voice or handwriting sample.[147] 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.[148]

3 Courts Have No Inherent Jurisdiction to Order a Compelled Production Order

Luppino provides a second finding of note: White J's finding that the Federal Court was not empowered by section 23 of the *Federal Court of Australia Act 1976* (Cth) to grant the interlocutory relief sought.[149] As such, the Court lacks a general subpoena power to issue a compelled production order. This is a notable distinction from the position adopted in the US; there, the *AW Act* 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*.[150] The result is that where a compelled production order is sought outside the terms of the specific

---

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)': Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Alert Digest* (Digest No 9 of 2015, 18 August 2015) 9.

144 *Luppino* (n 137) [32] (White J).

145 Ibid.

146 Ibid [33]. This same conclusion was reached by the Queensland Court of Appeal in *Wassmuth v Commissioner of Police*, in which North J found that compelling a person to reveal the encryption key to an electronic device implicated the privilege: *Wassmuth v Commissioner of Police* [2018] QCA 290, 312 [29] ('*Wassmuth*').

147 *Sorby* (n 122) 292 (Gibbs CJ).

148 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).

149 *Luppino* (n 137) [33]. In a recent article in the *Alternative Law Journal*, Adam and Barns conflate the question of the order under section 3LA and the order under section 23 of the *Federal Court of Australia Act 1976* (Cth): Lisanne Adam and Greg Barns, 'Digital Strip Searches in Australia: A Threat to the Privilege against Self-incrimination' (2020) 45(3) *Alternative Law Journal* 222, 225 <https://doi.org/10.1177/1037969x20923073>. The former is permissible because, as White J held, section 3LA abrogates the privilege; the latter order cannot be made either due to a 'lack of power, or as a matter constituting a bar on the exercise of the power, or as a matter of general discretion': at [33].

150 *AW Act* (n 24).

statutory provisions authorising such orders, there does not appear to be another statutory power under which such an order can be made.

This finding by White J finds support in *R v Ford*.[151] 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 that the applicant was involved in drug dealing.[152] 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 found, with reference to the powers under sections 154 and 154A of the *Police Powers Act*, that the constables were not 'exercising a power under any Act which required the applicant to give information or answer questions'.[153] As a result, it was open to Ford to lawfully refuse to provide the PIN.[154] This finding means that the lawful exercise of stop, search and arrest powers does 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.[155]

4 Abrogation of the Privilege

As compelled production orders raise the issue of the privilege, each of the statutes seek to abrogate the privilege. In Queensland and Victoria, that abrogation engages state-based human rights statutes in those jurisdictions. In the following Parts, this article examines how the privilege is abrogated in each of the local jurisdictions.

---

151 [2017] QSC 205.

152 Ibid [6]–[9] (Flanagan J).

153 Ibid [25].

154 Ibid [50].

155 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 2000* (Qld) s 157 ('*Police Powers Act*'). Note, too, that the only oral information that a police officer can ordinarily require of a suspect is their name and address: at 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 (Kyam Maher). 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.

(a) Jurisdictions with No Human Rights Statute

Of the Australian jurisdictions without a human rights statute, Western Australia and South Australia expressly abrogate the privilege by providing that the privilege cannot be relied upon to refuse to answer a disclosure notice.[156] Furthermore, they do so without giving any express immunity in exchange for that compliance.[157]

By contrast, at the federal level, the *Crimes Act 1914* (Cth) provides no such express abrogation. That does not preclude the possibility, however, that the privilege has been abrogated by necessary implication.[158] 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'.[159] It is, therefore, a question of what purpose the statute seeks to achieve. In the case of section 3LA, allowing a suspect to rely on the privilege would entirely defeat the purposes of the provision. Unsurprisingly, therefore, the Federal Court has held that section 3LA has the effect of abrogating the privilege. In *Luppino*, White J expressly held that '[section] 3LA of the *Crimes Act* is a statutory abrogation of the privilege'.[160]

Notably, White J further 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'.[161] The result is that if the use of biometrics is found to be an infringement of the privilege, the compulsory use of a biometric feature would still be permissible under the federal legislation as those statutory provisions abrogate the privilege.

(b) Jurisdictions with a Human Rights Statute

Victoria and Queensland are the only enacting jurisdictions in Australia with human rights statutes, and in both cases they expressly abolish the privilege when

---

156 *Criminal Investigation Act 2006* (WA) s 61(3); *Statutes Amendment (Child Exploitation and Encrypted Material) Act 2019* (SA) s 74BW(2).

157 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] (Hall J) ('*Sumption*') where the Court notes that the privilege is not a defence to a data access order.

158 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 this privilege': Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No 2) 2009 (Cth) 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.

159 *Pyneboard* (n 123) 341 (Mason ACJ, Wilson and Dawes JJ concurring). See also *Loges v Martin* (1991) 13 MVR 405, 408 (Nathan J) ('*Loges*'); *Hooper* (n 126).

160 *Luppino* (n 137) [26]. This finding is consistent with how courts have dealt with motor vehicle reporting obligations, which were found to impliedly abrogate the privilege: *Loges* (n 159) 409 (Nathan J); *Hooper* (n 126) 486 (Cox J). Compare, however, the decision in *Wassmuth* (n 146) in which North J found that the equivalent – though differently worded – provisions in the *Police Powers Act* (n 155) did not abrogate the privilege. The effect of his Honour's finding was, of course, to denude the provisions of their force, rendering them entirely otiose by reducing them to little more than the ability to request access to the device in question with no power to compel such access.

161 *Luppino* (n 137) [27] (White J).

granting a compelled production order.[162] How, though, do those acts of abrogation sit with the protection given to the privilege in the *Charter of Human Rights and Responsibilities 2006* (Vic) ('*Victorian Charter*') and the *Human Rights Act 2019* (Qld)? That question can be answered by reference to the existing case law under the *Victorian Charter*, as it has a far larger body of case law on which to draw than does Queensland and the provisions of the two statutes are, for present purposes, sufficiently similar.

The *Victorian Charter* provides, in section 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'.[163] However, section 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.[164] Importantly, if a limitation is found to be unreasonable, that finding does not invalidate the provision in question. Instead, the court is limited to issuing a declaration of inconsistent interpretation.

The question thus arises whether sections 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 section 7 of the *Victorian Charter*. Guidance can be sought from the section 7 analysis performed by the Victorian Supreme Court in *Re an Application under Major Crime (Investigative Powers) Act 2004*.[165] The case concerned section 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 answer questions. The abrogation of the privilege required by that provision was accompanied by a direct-use immunity, but not a derivative-use one. The Court, after considering the section 7 factors, read a derivative-use immunity into the provision on the grounds that such immunity was required under section 25(2)(k) of the *Victorian Charter*.[166]

At the outset of her section 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 they receive a fair trial. The standard of proof required to be met to satisfy a court that a limitation is reasonable

---

162 *Vic Crimes Act* (n 143) ss 465AA(6), 465AAA(7); *Police Powers Act* (n 155) s 154B.

163 The comparable provision in the *Human Rights Act 2004* (ACT) is section 22(2)(i).

164 *Charter of Human Rights and Responsibilities 2006* (Vic) s 7(2) ('*Victorian Charter*') 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.

165 (2009) 24 VR 415 ('*Major Crime*').

166 The legislature subsequently amended the legislation to remove the derivative-use immunity that had been read in by the Court.

is high.[167] 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'.[168] 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'.[169] Allowing its use could 'provide a "back-door" to prosecuting authorities to use compelled incriminating testimony against the [testifier]'.[170] 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'.[171] 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'.[172]

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 section 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.[173] 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.[174]

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

167 *Major Crime* (n 165) 448 [177] (Warren CJ).
168 Ibid 448 [146]. Note, though, that in England it is recognised that a breach of the privilege does not automatically render a trial unfair.
169 Ibid 435 [84]. Note, though, that a password itself is not ordinarily incriminating.
170 Ibid 437 [95].
171 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.
172 Ibid 450 [153].
173 Ibid 450 [155].
174 Ibid 451 [156].

definition criminal conduct involving more than one person.[175] 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 it 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.[176] US 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 relevant to a prosecution against the possessor of the electronic device.[177]

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 section 7 *Victorian Charter* analysis performed on sections 465AA and 465AAA of the *Crimes Act 1958* (Vic) would find the infringement to be reasonable. Importantly, too, even in the event that the relevant statutory provisions are held to infringe the privilege, that finding does not render the statutory provisions invalid.[178]

5 The Evidentiary Burden Concerning Knowledge of the Password

Australian decisions are consistent in applying a relatively low evidentiary threshold to satisfy knowledge of a password. In *Luppino v Fisher [No 2]* ('*Luppino [No 2]*'),[179] this issue was specifically raised by the defendant. 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.[180]

Support for this position can be found in several decisions of the Supreme Court and Court of Appeal of Western Australia. In *Garbellini v Western Australia*,[181] 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 *Western Australia v Doyle*,[182] 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

175 *Major Crime (Investigative Powers) Act 2004* (Vic) s 3AA(1)(b).
176 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.
177 See, eg, *Boucher II* (n 49); *Apple MacPro Computer* (n 25); *Gavegnano* (n 37); *Stahl* (n 37).
178 *Victorian Charter* (n 164) s 36(5).
179 *Luppino [No 2]* (n 32).
180 Ibid [196] (White J).
181 [2017] WASC 93 ('*Garbellini*').
182 [2017] WASCA 207.

was found in the suspect's possession. In *Lenton v Western Australia*,[183] 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 which were password protected.[184] A data access order was granted in respect of those devices.[185]

That Australia and England and Wales have adopted a more lenient standard than that applied in the US is clear. In *Grand Jury Subpoena*, 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 *Re the 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 US. 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 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 ordinarily remembered because of the frequency with which it is used. It is therefore, as the English Court of Appeal held, a perfectly legitimate conclusion to draw that the suspect will know the password.

6 The Evidentiary Burden Concerning Knowledge of the Contents of the Encrypted Drive

In Australia, courts have held that the prosecution has established sufficient evidence of the accused's knowledge of the contents of the encrypted drive in circumstances where: encrypted files were found on a computer that had been used

183 (2017) 82 MVR 447 ('*Lenton*').

184 Ibid [10]–[18] (Buss P, Beech JA and Hall J).

185 See also *Dias v Western Australia* [2017] WASCA 49 ('*Dias*') in which 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 *Chadburne v Western Australia* [2017] WASCA 216 ('*Chadburne*') in which a mobile phone found in the appellant's vehicle was made the subject of a data access order.

186 *Grand Jury Subpoena* (n 25) 1346 (Tjoflat J).

187 *Seized Data Storage System* (n 25) slip op 8.

to view terrorist propaganda and websites;[188] an order for access to email accounts was sought after child pornography had been found in the accused's possession;[189] a hard drive was found in the possession of a person who was a customer of a child pornography website;[190] an iPhone was found in the possession of a person at the same time as drugs were found hidden on him;[191] and an iPad and mobile phone were found in a suspect's house during a search that found drugs.[192]

Importantly, however, in *Luppino [No 2]* White J identified an additional requirement that is imposed on a magistrate when they issue a search warrant that includes a compelled production order. His Honour held that a section 3LA warrant 'contemplates an order being made in respect of a particular computer or data storage device (or particular computers or devices)'.[193] On the facts, two mobile phones and one laptop were seized from the accused.[194] However, in issuing the warrant, the magistrate stated that he was satisfied that evidentiary material would be found on 'the' computer or storage device.[195] That left open which of the three devices that level of satisfaction related to; it also meant that 'the s 3LA order did not inform the plaintiff of the particular device in respect of which he was required to provide the information or assistance'.[196] This failure in the warrant led White J to find that section 3LA did not authorise the order granted by the magistrate. Note, however, that this finding by White J does not increase the evidentiary burden required to be satisfied under section 3LA. What it does do, though, is to require the evidentiary burden to be satisfied in respect of each electronic device that is sought to be searched under a section 3LA warrant.

Unfortunately, there are reasons to be dissatisfied with White J's approach. As White J noted, section 3LA allows an order to be made prior to the execution of a search warrant;[197] it can also be issued after the devices have been seized. White J's approach thus achieves nothing more than to require law enforcement officials to obtain a second section 3LA warrant after seizure of the devices which will rely on precisely the same information that was sufficient to obtain the first warrant. That first warrant having been obtained in reliance on that information, it follows that the second must also be issued as the evidentiary burden will not have changed.

---

188 *K v Children's Court of Victoria* [2015] VSC 645, [9]–[10] (Forrest J).

189 *R v SW* [2008] NSWDC 148, [2]–[4] (Knox DCJ). Compare this to *Securities and 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.

190 *R v Monaghan* [2014] ACTSC 278, [28]–[29] (Murrell CJ).

191 *R v Ford* [2017] QSC 205, [6]–[8] (Flanagan J). See also *Lenton* (n 183) [11]–[18] (Buss P, Beech JA and Hall J) (drugs and mobile phones found in person's backpack).

192 *Garbellini* (n 181) [9] (Hall J); *Western Australia v Doyle* [2017] WASCA 207, [7] (Buss P, Mazza JA and Hall J). See also *Dias* (n 185) [3]–[9] (Newnes and Mazza JJA), *Chadburne* (n 185) [15]–[18] (Martin CJ, Mazza and Mitchell JJA) and *Sumption* (n 157) [7]–[8] (Hall J), all of which involved drugs and mobile phones found in the suspect's motor vehicle while the suspect was in the vehicle.

193 *Luppino [No 2]* (n 32) [161] (White J).

194 Ibid [165].

195 Ibid [161].

196 Ibid [165].

197 Ibid [160].

White J's ruling thus merely adds unnecessary costs and time to the execution of the section 3LA order.

The above findings with regards to the evidentiary burden are consistent with the approach taken in England and Wales. Moreover, it is also similar to the evidentiary requirement imposed under the control test in the US. The outlier is therefore the evidentiary burden imposed under 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 US decisions that have applied the contents test, as *Grand Jury Subpoena* 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 English or Australian case law.[198]

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 electronic device must be shown.[199] 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 sees compelled production orders subject to a more onerous evidentiary standard, a standard that even in the US has not been accepted by several courts, including the Supreme Court.[200]

Notably too, the burden imposed by the contents test is not there to protect a suspects' privacy, as the ordinary warrant requirements perform that function; nor do proponents of the contents test provide a 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. The contents test stands

198 See also *GAQL* (n 41) 1064 (Levine J) in which the reasonable particularity standard for access to the Snapchat messages of the suspect was not satisfied despite the state informing the court that it had a witness who had shared messages with the witness by phone that day using the Snapchat messaging app. The court held that the state could not 'say with reasonable particularity that the Snapchat and text [message] files are located on the phone': at 1064.

199 The probable cause threshold is imposed by the Fourth Amendment when a warrant is sought. That burden will apply when law enforcement officials seek a warrant to search an encrypted device. This process is demonstrated in *Grand Jury Subpoena* (n 25) 1339 (Tjoflat J). See also *Trant* (n 39); *Stahl* (n 37); *Diamond* (n 55).

200 Mohan and Villasenor (n 41) 20 where the authors note that the Supreme Court was 'specifically presented with the "reasonable particularity" standard in *Hubbell* and chose not to adopt it'.

alone among the three jurisdictions in imposing so onerous a burden, and it does so with no compelling argument supporting its onerous terms.[201]

In light of that analysis, Australian courts can find significant comfort in the fact that their interpretation of the evidentiary burdens imposed by a compelled production order find substantial support in the comparator jurisdictions.

7 The Application of Section 3LA to Smartphones

The decisions in the *Luppino* cases raises one outstanding issue: does section 3LA apply to smartphones? This question was raised by Luppino, who challenged the applicability of section 3LA to smartphones on the basis that a smartphone was not a computer or data storage device, as required by the statute. In *Luppino [No 2]*, White J, while expressing the view that this argument had 'some force', refused to express a concluded view on this issue.[202] 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 section 3LA, as drafted at the time the order was made, was intended to apply to smartphones. This question, however, has become moot since the Luppino decisions were handed down. With the passage of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ('*Assistance and Access Act*') in December 2018, section 3LA has been amended to insert a new subsection (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 section 3LA applies to smartphones. As is stated in the Explanatory Memorandum to the *Assistance and Access Act*, because section 3LA prior to amendment did 'not envision people carrying smartphones in their pockets … [t]he Bill will resolve this gap'.[203]

VI CONCLUSION

As the prevalence in Australia of cases involving compelled production orders grows, several conclusions can be drawn from the preceding analysis. First, where a compelled production order is sought under the federal or a state statute, the

---

201 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] (Ricchetti J).

202 *Luppino [No 2]* (n 32) [184] (White J).

203 Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 22 [101]–[102]. The Explanatory Memorandum notes, in full, that

> [t]he current section 3LA predates the existence and common usage of smartphones – it refers to accessing data held in, or accessible from, a computer or data storage device that is on a warrant premises, has been moved from a premises or seized. Those provisions do not envision people carrying smartphones in their pockets. The Bill will resolve this gap by allowing law enforcement agencies to compel persons to assist in providing access to a device under a person-based warrant.

The Explanatory Memorandum states that these amendments will allow law enforcement agencies 'to access portable technology devices': at [107].

privilege cannot bar the granting of that order and the order does not require a commensurate grant of immunity. In Australia, the High Court has stated that 'the privilege … does not prohibit the giving of evidence, against the will of a witness, as to the condition of his body'.[204] The same position is adopted in England and Wales and the US, notwithstanding that the latter grants constitutional protection to the privilege, and the former protects the privilege through the *Human Rights Act 1998* (UK). Suggestions, then, that the privilege is inadequately protected in Australia when such orders are sought due to the absence of a federal human rights statute are misplaced.[205]

What is retrieved from the encrypted device is pre-existing evidence of the type that has, until the widespread availability of encryption, always been retrievable under a search warrant. The purpose of a compelled production order is not to broaden law enforcements' powers; it is to restore them to the position they were in little more than a decade ago. In a recent article, Adam and Barns ask: 'If an individual cannot be compelled to answer questions put to them by police officers, why would it be appropriate to compel an individual to unlock their electronic device?'[206] The question is misconceived. All jurisdictions examined in this article recognise the distinction between real, pre-existing evidence such as fingerprints, breathalyser samples and DNA tests on the one hand, and testimonial evidence that is created through compulsion, such as oral testimony, on the other hand. An encryption key is not created when it is spoken by a suspect – it already exists. So much has been recognised by the Court of Appeal of England and Wales.[207] It is for that reason that the Court of Appeal has upheld the lawfulness of compelled production orders. Unfortunately, the question asked by Adam and Barns appears to ignore this distinction.

Secondly, such orders can only be granted where a statutory framework is in place. If a jurisdiction has not enacted specific legislation to address this issue, then it is unlikely to have a general power that authorises such measures. Thirdly, as the court in *Luppino* found, even absent an express statutory abrogation of the privilege, that abrogation will be implied. Were that not the case, the ability to rely on the privilege would fatally undermine the sole purpose of the legislation, rendering the provisions entirely impotent.

Fourthly, the approach adopted by the Australian courts regarding the evidentiary burden is consistent with that of the courts of England and Wales, and also those courts of the US that have adopted the control test. This article supports that approach. Where a suspect is the owner or possessor of an electronic device that is found on his or her possession or in his or her house, it is, as the High Court of England and Wales noted, 'a perfectly legitimate inference to draw' that the suspect knows the password.[208] It is one that is consistent with the evidentiary burden that is imposed for any other search warrant, and it provides sufficient rigor to prevent

204 *Sorby* (n 122) 292 (Gibbs CJ).
205 Adam and Barns (n 149) 227.
206 Ibid.
207 *R v S (F)* (n 79) 1496 [20] (Lord Judge CJ, Penry-Davey and Simon JJ).
208 *Greater Manchester Police* (n 85) [21] (McCombe J).

law enforcement officials from engaging in fishing expeditions. 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 *Grand Jury Subpoena* 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 by a subpoena to the relevant internet service provider. If it has, then finding that device in the possession of its owner would render any assertion by that same owner that they do not know the password unsustainable. While these additional measures may not frequently be required, in cases where there is doubt about the suspect's knowledge of the password they may provide sufficient evidence to remove that doubt.

Finally, where decryption is to occur through the use of a biometric feature such as a fingerprint, the privilege is not engaged. So much has been overwhelmingly recognised by the courts of the US, and it is a position that is consistent with long standing authority on the scope of the privilege in Australia.

In Australia, this issue need not be overcomplicated. The statutory measures enacted by the federal government and various states are effective in abrogating the privilege and allowing the granting of a compelled production order. What judicial dispute exists concerns the penumbra of such orders and does not alter the conclusion that such orders can validly be made provided the statutory provisions are complied with. This outcome is appropriate and entirely consistent with the position in England and Wales, which, like Australia, has been able to chart a clear path with such orders, one that has resulted in broad judicial certainty about their operation.