COMMENT ON THE EXPOSURE DRAFT FOR THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018

Daniel Hochstrasser

September 2018

I am a final year PhD student and Teaching Fellow at Melbourne Law School. My thesis considers the role of the privilege against self-incrimination when law enforcement officials seek to compel a person to provide access to encrypted electronic data that may contain evidence of criminal conduct by that person.

Presently, the Commonwealth, Queensland, Victoria and Western Australia have each enacted a statutory mechanism to enable law enforcement officials to obtain an order compelling a person to assist law enforcement officials to access encrypted electronic data (**assistance order**). The exposure draft for the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**Assistance and Access Bill**) seeks to amend and expand existing Commonwealth provisions relating to assistance orders. Four comments on those proposed amendments are made below.

1. Abrogation of the privilege against self-incrimination

In Queensland, Victoria and Western Australia, the statutory power to obtain an assistance order is accompanied by the express abrogation of the privilege against self-incrimination without a grant of immunity for information obtained through the use of that order.[1] As presently drafted, the *Crimes Act 1914* (Cth) contains no similar express abrogation of the privilege and the amendments proposed to it do not include such a provision. The same is true of the proposed amendments to the *Surveillance Devices Act 2004* (Cth), the *Customs Act 1901* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth). It is my recommendation that this omission be rectified.

---

1 *Police Powers and Responsibilities Act 2000* (Qld) s 154B; *Criminal Investigation Act 2006* (WA) s 61(3); *Crimes Act 1958* (Vic) ss 465AA(6) and 465AAA(7). In South Australia, the proposed Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA) s 74BW(2) similarly abrogates the privilege with no grant of immunity.

The Explanatory Document to the Assistance and Access Bill 2018 (**Explanatory Document**) does not explain why the abrogation of the privilege is not expressly dealt with. However, when s 3LA of the *Crimes Act 1914* (Cth) was amended in 2009, it was noted in the accompanying Explanatory Memorandum that 'section 3LA (as it currently stands or as repealed or replaced by this item) does not impact on the privilege'.[2] That opinion is most likely wrong. In the United States of America, the decrypting of an encrypted electronic device pursuant to an assistance order has been found to infringe the privilege on the basis that the act of producing either the unencrypted documents or the encryption key constitutes a testimonial act that engages the protections afforded by the privilege.[3] In Canada, the compelled production of an encryption key constitutes the handing over of evidence to be used against the accused, an act that infringes the privilege. And in the United Kingdom, the courts have held that though an encryption key is pre-existing evidence that exists independently of the will of an accused – a fact that would normally render the privilege inapplicable – the act of producing that key may enliven the privilege.

There are reasons for believing the position to be the same in Australia. The privilege against self-incrimination in Australia protects a suspect not only from directly incriminating evidence, but also from producing evidence that leads to the discovery of incriminating derivative evidence.[4] Decrypting an encrypted electronic device that contains evidence of one's criminality falls squarely within the scope of that protection. Furthermore, there is judicial support for the argument that an assistance order implicates the privilege. In *Re Application under the Major Crimes (Investigative Powers) Act 2004*,[5] the Victorian Supreme Court identified evidence obtained from a computer through the use of an assistance order as an example of derivative evidence that would have been obtained in breach of the

---

2 Replacement Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009, 92.

3 Note, however, that where the contents of the encrypted drive are known to law enforcement with reasonable particularity and they are able to be authenticated other than through the act of encryption, an exception to the act of production doctrine known as the foregone conclusion doctrine will be satisfied. Where the requirements of the foregone conclusion doctrine are met, the act of production becomes one of surrender, not testimony, with the result that the privilege is no longer infringed by that act of production.

4 *Sorby v The Commonwealth* (1983) 152 CLR 281, 310 (Mason, Wilson and Dawson JJ).

5 (2009) 24 VR 415.

privilege. Finally, the inclusion by the legislatures of Queensland, Victoria and Western Australia of a clause expressly abrogating the privilege strongly evidences their belief that the privilege is engaged by an assistance order.

If it is accepted that assistance orders may infringe the privilege, abrogation of the privilege is necessary to ensure the assistance orders operate as intended. Abrogation can occur either through express words or implication,[6] though the latter can only occur where 'it appears from the character and purpose of the provision in question that the obligation was not intended to be subject to any qualification',[7] or where a failure to imply abrogation would undermine the purpose of the statute.[8] An example of a statutory power that has been held to abrogate the privilege by necessary implication is the power to require the owner of a motor vehicle to state who was driving the motor vehicle at a specified time. The failure to imply the abrogation of the privilege in respect of that power would, courts have found, have undermined the very purpose of the provision.[9]

In the case of a power to issue an assistance order, it is likely that abrogation by necessary implication is present. The solitary purpose of a statutory power to obtain an assistance order is to enable law enforcement officials to gain access to otherwise inaccessible encrypted material. To allow the recipient of an assistance order to refuse to comply with that order on the basis that to do so would infringe the privilege would render the order largely impotent. Despite this outcome, however, for purposes of certainty and consistency with State legislation it is preferable that the granting of a power to apply for an assistance order is accompanied by the express abrogation of the privilege against self-incrimination.

2. Alignment of sentences with the underlying offence

On page 98 of the Explanatory Documents, it states that there is a need to increase the penalty for non-compliance in s 3LA of the *Crimes Act 1914* (Cth) because 'there is no incentive for a person to comply with an order if they have committed an offence with a

---

6 *Sorby v The Commonwealth* (1983) 152 CLR 281, 289 (Mason, Wilson and Dawson JJ).
7 *Police Service Board v Morris* 156 CLR 397, 409.
8 *Mortimer v Brown* [1970] 122 CLR 493.
9 *Loges v Martin* 13 MVR 405, 409; *R v Hooper* 64 SASR 480, 486.

higher penalty and evidence is available on their device'. Similar sentiments are expressed in relation to s 201A(3) of the *Customs Act 1901* (Cth). The limited evidence that is available in both the United Kingdom and Australia bears this statement out. However, while the proposed amendments may improve compliance with assistance orders, there is an alternative measure with an arguably greater ability to achieve that goal.

I propose that the maximum sentence for non-compliance with an assistance order should match the maximum sentence for the offence that is being investigated. If multiple offences are being investigated, the maximum sentence for non-compliance will be that of the most serious offence under investigation. Such an approach seeks to achieve the same goals as the current proposals in the Access and Assistance Bill, but instead of providing just two sentencing thresholds for all manner of offences under investigation, the full range of sentences imposed for the underlying offences will be available. This will ensure that the sanction for non-compliance retains its ability to incentivise compliance where the underlying offending carries a term of imprisonment longer than ten years,[10] while also preventing the maximum sentence for non-compliance from exceeding the maximum sentence available for the underlying offending.[11]

3. Use of information obtained under the assistance provisions

In 2014, in *Riley v California*, the Supreme Court of the United States noted that 'it is no exaggeration to say that many of the more than 90% of the American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate'.[12] The ability to search that mobile phone, that computer, that electronic device brings with it the opportunity to examine almost every aspect of a person's life. In *Riley*, the court went on to note how electronic searches differ from other searches in two ways: the quantity of documents available for inspection far exceeds that which can be

---

10 After all, the concern expressed in the Explanatory Documents that 'there is no incentive for a person to comply with an order if they have committed an offence with a higher penalty and evidence is available on their device' remains a live concern for the most serious offences that might be investigated and which, like terrorism offences, carry maximum sentences greater than ten years' imprisonment.

11 As would be the case where the underlying offence was, for example, punishable by a term of imprisonment not exceeding five years.

12 *Riley v California* 134 S.Ct. 2473, 2490 (2014).

found and examined in the course of a physical search of documents or other evidence; and the type of information that is revealed is different. Most obviously, a mobile phone can reveal browsing habits, text messages, emails, call logs, app data and location data that divulges where a person has been and when they were there. The potential, therefore, for a search of an electronic device to turn into a largely untrammelled fishing expedition is boundless.

Section 74BW(3) of the Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA) provides that any evidence obtained during a search of an electronic device pursuant to an assistance order 'is not inadmissible in proceedings before a court in relation to a serious offence merely because the order under this Part was obtained in relation to a different serious offence'. That provision, it is submitted, goes too far. However, without being as explicit, the same position appears to be reflected in respect of searches conducted under the *Customs Act 1901* (Cth) and the *Crimes Act 1914* (Cth). Under both statutes, in s 199 of the former and s 3F of the latter, evidential material found during the execution of a search warrant that relates to an offence other than the one to which the warrant relates may be seized. No more is said in either statute about the use to which that evidence can be put.[13]

Given the scope of the evidence that can be revealed by an electronic search of a person's computer or mobile phone, it is appropriate that reasonable restrictions should be imposed on the use of that evidence. Specifically, only evidence relating to the underlying offence in

---

[13] It is noted that the amendments to the *Surveillance Devices Act 2004* (Cth) do not grant as much latitude. Under the proposed s 27A(1)(c), a computer access warrant may be granted if relevant offences are being investigated and 'access to data held in a computer (the **target computer**) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of: (i) the commission of those offences; or (ii) the identity or location of the offenders' (emphasis added). Section 27E(2) goes on to provide that a computer access warrant may authorise the obtaining of 'access to data (the **relevant data**) that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant'. Section 27E(4)(a) provides that data is covered by a warrant if '(a) in the case of a warrant sought in relation to a relevant offence – access to the data is necessary as described in paragraph 27A(1)(c)'. Similarly, under the *Australian Security Intelligence Organisation Act 1979* (Cth), when a computer access warrant is issued under s 25A, the warrant may specify that the target computer may only be used to obtain access to data 'that is relevant to the security matter and is held in the target computer at any time while the warrant is in force'. Section 25A(4)(b) does, however, allow the copying of any 'data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act'.

respect of which the assistance order was obtained should be admissible in criminal proceedings against that person. For example, where child exploitation material is being investigated, any evidence of possession, production or distribution of that material would be admissible; evidence of tax fraud, however, would not be. Such an outcome has two virtues.

First, it provides a better balance between the need for law enforcement to be able to investigate offending and the right to privacy held by community members. While the right to privacy cannot be used to defeat a search on reasonable grounds, it should be expected to restrain what could otherwise evolve into an almost limitless search. Indeed, that a person's privacy is identified as one of the considerations to be taken into account in determining whether to grant a computer access warrant under the proposed s 27C(2)(c) of the *Surveillance Devices Act 2004* (Cth) demonstrates the importance of this right. Secondly, it prevents abuse of the use of assistance orders. In addition to the existing evidence requirements that need to be satisfied before an assistance order can be made, limiting the use to which evidence unrelated to the stated underlying offending can be put prevents the use of an assistance order for a collateral purpose. For example, if the applicant for an assistance order has insufficient evidence to obtain an assistance order in respect of the primary offending that is being investigated, but has sufficient evidence in respect of a less serious offence, the applicant cannot circumvent the lack of evidence in respect of the more serious offending by obtaining an assistance order based on the less serious charge and utilising it to search for evidence of the more serious offending.

For these reasons, it is my recommendation that the assistance provisions under both the *Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth) should provide that only evidence relating to the offending in respect of which the assistance order was granted may subsequently be admitted in criminal proceedings against the recipient of the assistance order. Note that this will not prevent the use of that unrelated but incriminating material against persons other than the recipient of the assistance order.

4. The problem of the destruction of evidence

The inability to access encrypted material is not the only problem posed by the use of encryption. In the second reading speech for the Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA) in the Legislative Council, it was said by the government that

> contemporary technology is such that an individual could purport to comply with a court order and provide his or her password or other means of access but in reality this could destroy (or conceal or alter beyond recovery) all the encrypted records subject to that order. It is becoming common practice for persons with sophisticated IT knowledge to have these second or 'false' passwords for their devices. Once this password is entered, no-one can recover the data, not even the person whose device it is.[14]

In order to address that issue, the South Australian Bill makes it an offence to deliberately delete, conceal or alter the contents of the encrypted device which is the subject of an assistance order.[15] Engaging in such conduct – either by entering the password oneself or be providing it to law enforcement officials to (unwittingly) enter into the electronic device – is to be subject to a maximum term of imprisonment of ten years, more than twice the maximum term for non-compliance with the order. The South Australian Bill also creates a third offence in respect of the remote deletion of the contents of the encrypted drive by an acquaintance of the recipient of the assistant order, at the recipient's request.[16]

The addition of similar provisions in the Assistance and Access Bill would complement the existing assistance provisions. While the intentional deletion of the encrypted material would be punishable under the existing sanction for non-compliance, there remains a fundamental difference between existing material that remains in an encrypted state and material that has been irretrievably deleted. In the case of the former, that material remains susceptible to further assistance orders or the possibility of defeating the encryption with the passage of sufficient time or technological innovation; in respect of the latter, that material can never be recovered. Addressing the possibility of this conduct in the manner suggested by the South

---

14 South Australia, *Parliamentary Debates*, Legislative Council, 18 October 2017, 7973.

15 Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA), s 74BX(2) and (3).

16 Statutes Amendment (Child Exploitation and Encrypted Material) Bill 2017 (SA), s 74BX(1).

Australian parliament could assist in ensuring that such a practice does not develop. For these reasons, I recommend inserting provisions of this nature into the Assistance and Access Bill.