Crime and Corruption Commission
QUEENSLAND

October 2015

Accessing electronically stored evidence of child exploitation material offences

An examination of the legislative limitations of section 154 of the *Police Powers and Responsibilities Act 2000*

Background

In 2006, the Queensland Parliament introduced a legislative provision to ensure police officers had sufficient powers to investigate criminal activities that may involve electronically stored evidence.[1] An "access order" obtained under section 154 of the *Police Powers and Responsibilities Act 2000* gives a police officer the power to require a person to give them the information that is necessary to access material stored electronically on a computer or other storage device.[2] This power was considered necessary for police to properly investigate a range of offences, including drug trafficking, identity fraud and offences involving child exploitation material (CEM), the investigation of which also fall within the remit of the Crime and Corruption Commission (CCC).

It has been nearly ten years since the introduction of the section 154 access order provision. Significant developments in technology have occurred over this time, constraining the effectiveness of the power. To ensure the power can operate effectively in this rapidly adapting technological environment, and to generally improve the operation of the power, the CCC's submission to the 2015 Parliamentary Crime and Corruption Committee review recommended that a number of amendments be made to section 154, and that this amended power also be inserted into the *Crime and Corruption Act 2001* (CCC 2015, pp. 44–5).

This paper, which supplements the CCC's earlier submission, examines how these legislative limitations manifest in the investigation of offences involving CEM and identifies options for legislative reform. Readers will detect significant similarity to the issues identified and recommendations made in the Queensland Organised Crime Commission of Inquiry report, which was published on 30 October 2015.[3]

---

1 Explanatory Notes, Police Powers and Responsibilities and Other Acts Amendment Bill 2006, p. 4.

2 The provision was originally numbered s. 71A.

3 Queensland Organised Crime Commission of Inquiry 2015.

Section 154 access orders

Section 154 of the *Police Powers and Responsibilities Act 2000* (PPRA) provides that an access order can be made in a search warrant. An access order requires a person to, among other things, give a police officer the information that is necessary to access material stored electronically on a computer or other storage device (see Textbox 1). This may include login details, passwords and encryption keys.[4] Access orders can only be made by a magistrate or judge (not a justice of the peace) and only when issuing a search warrant.

Textbox 1: Section 154, *Police Powers and Responsibilities Act 2000*

Order in search warrant about information necessary to access information stored electronically

(1) If the issuer is a magistrate or a judge, the issuer may, in a search warrant order the person in possession of access information for a storage device in the person's possession or to which the person has access at the place—

(a) to give a police officer access to the storage device and the access information necessary for the police officer to be able to use the storage device to gain access to stored information that is accessible only by using the access information; and

(b) to allow a police officer given access to a storage device to do any of the following in relation to stored information stored on or accessible only by using the storage device—

(i) use the access information to gain access to the stored information;

(ii) examine the stored information to find out whether it may be evidence of the commission of an offence;

(iii) make a copy of any stored information that may be evidence of the commission of an offence, including by using another storage device.

(2) In this section—

access information means information of any kind that it is necessary for a person to use to be able to access and read information stored electronically on a storage device.

storage device means a device of any kind on which information may be stored electronically.

stored information means information stored on a storage device.

Electronically stored child exploitation material

Child exploitation material (CEM) is material that, in a way likely to cause offence to a reasonable adult, describes or depicts a person, or a representation of a person, who is, or apparently is, a child under 16 years:

(a) in a sexual context, including for example, engaging in a sexual activity; or

(b) in an offensive or demeaning context; or

(c) being subjected to abuse, cruelty or torture.[5]

In Queensland, it is an offence to make, distribute, possess or involve a child in making CEM.[6]

There is growing international concern that technological advancement is facilitating the online exploitation of children (Australian Crime Commission 2015). It is common for CEM to be stored electronically, and offenders are becoming increasingly skilled in data encryption and secure data storage to conceal evidence of their involvement in these offences.[7] Encryption and other security measures make it virtually impossible for law enforcement to access evidence of suspected CEM on an electronic storage device without information such as

4 An encryption key is used to decrypt encrypted data so that it can be read.

5 Section 207A *Criminal Code Act 1899* (Qld).

6 Sections 228A–D Criminal Code Act.

7 Encryption involves converting data into a coded form so that only authorised people can read it. Data is encrypted using an encryption key, which a person must have to decrypt the data. The encryption key can be password protected.

login details and passwords that are necessary to access the device or its files.[8] An inability to access this information means that evidence of these offences remains concealed and may be destroyed. Further, police are unable to identify, locate and remove from harm the children involved in the CEM. Being able to access protected storage devices suspected of containing electronic evidence of CEM is therefore critical to police efforts to tackle child exploitation.

Legislative limitations of section 154 of the PPRA

The frequency with which CEM is concealed on storage devices protected by encryption and other security mechanisms means that Queensland police officers make considerable use of section 154 in CEM investigations. Between 2010 and 2014, more than 80 per cent of search warrants executed by QPS officers in relation to suspected CEM offences included an access order.[9]

Although section 154 is used frequently, limitations in the provision present challenges for police investigating CEM offences and prevent section 154 from fully achieving its intended purpose. More specifically, the limitations mean that:

- Police encounter situations where an access order is not available.
- The scope of an access order is not always sufficient to enable police to obtain required access information or access protected storage devices.
- Access orders are not always complied with.

These challenges and the legislative limitations of section 154 that give rise to them are discussed further below, along with possible reforms. Any reforms will need to balance the community's interest in investigating and prosecuting CEM offences, with the protection of individual human rights and liberties, including those of offenders.

Police encounter situations where an access order is not available

As noted previously, being able to access protected storage devices is critical in CEM investigations. Any barriers that police encounter when trying to obtain an access order therefore need to be examined.

Police officers investigating CEM offences sometimes encounter situations where they are seeking an access order but cannot obtain one because of constraints around when and how orders can be issued. Specifically:

- Access orders can only be issued at the time of the search warrant application.
- Access orders can only be issued by magistrates and judges, who are not always available.

Access orders can only be issued at the time of the search warrant application

Under section 154, access orders can only be issued when police apply for a search warrant. After the search has been completed and the search warrant is finalised, the access order expires and police can no longer require a person to provide access information. This creates problems for police investigating CEM offences in circumstances where:

- it only becomes apparent to investigators after the search warrant is finalised that a storage device found at the warrant premises cannot be accessed without access information

8 In some situations, police are able to access protected data in other ways (e.g. by using key loggers that remember the sequencing of key strokes for a particular keyboard), but this requires advanced preparation time that is not always available in situations where a child may be at risk.

9 The CCC received data from QPS Statistical Services on 1245 search warrants executed between 1 January 2010 and 31 December 2014 where the suspected offences related to CEM. Resource constraints prevented all search warrants from being examined to determine if they included an access order under section 154. The CCC therefore selected a random sample of 223 search warrants and was able to find a copy of the signed search warrant on QPRIME (Queensland Police Records and Information Management Exchange) in 54 cases. Of these 54 search warrants, 83 per cent (n = 45) included an access order. Warrants from the QPS regions were less likely to contain an access order than were warrants from Task Force Argos — 80 per cent of warrants from the regions (n = 33), compared with 92 per cent of warrants from Argos (n = 12).

- additional storage devices or accounts (for example, email accounts, online file storage services and social media profiles) are identified after the search warrant is executed. Although police perform a preliminary triage of storage devices when the search warrant is executed, more sophisticated forensic examinations conducted at a later time can identify additional accounts.

Compounding this issue, a person is only required to provide access information that is specifically requested by police when executing the search warrant. Given that some CEM offenders are proficient at hiding files and storage devices and that preliminary triage of devices during the search does not always reveal this information, it is inevitable that police executing the warrant may not always be aware of the full extent of a suspect's CEM collection and where it is stored. In this instance police would need to obtain and execute an additional search warrant that includes an access order to require a person to provide the access information related to the newly discovered devices or accounts. Once again, this delay provides the offender with an opportunity to destroy evidence.

Police responding to an immediate threat by using "emergent search" powers are unable to obtain an access order at all. An emergent search occurs where police determine that evidence is likely to be concealed or destroyed if they do not take immediate action.[10] In such instances, there is no time to apply to a magistrate for a search warrant that includes an access order, and the search warrant powers that can be used during an emergent search do not include the power to require access information.[11] Police therefore have no power to require the provision of access information during the search, and there is no ability for police to later require access information for devices seized during the search.[12]

Legislative reforms

To solve these problems, it should be possible for police to obtain an access order at times other than when applying for a search warrant. In Victoria, for example, police can apply for an access order "at the same time as an application is made for the warrant… or at any time after the issue of the warrant".[13] Even where police seize a computer or storage device pursuant to a search warrant that included an access order, the Victorian provision allows police to apply for a second access order after the warrant has been executed.[14] Such an amendment in Queensland would ensure that police are able to obtain an access order for storage devices and online accounts seized during a search, whether conducted with a warrant or under emergent search provisions.

Even if an access order was available after a search is conducted, there may be strategic value in police also being able to require access to information at the time of the search. Police who investigate CEM offences have indicated that people are most likely to provide access information at the time of the search; this approach may also help to ensure people do not have time to hide access information or make up an excuse as to why they cannot provide it. One option that would enable police to require access information when a search is conducted would be to extend the search warrant powers police have under section 157 of the PPRA.[15] Specifically, adding the power to require the provision of access information to section 157 would mean that police automatically have this power when a search warrant is issued (without having to apply for an additional order under section 154) and would also be able to use this power during an emergent search.

---

10 Sections 160–162 PPRA.

11 Search warrant powers are defined in s. 157 of the PPRA. Section 160(3) PPRA provides that a police officer conducting an emergent search may exercise search warrant powers (under s. 157) as if they were conferred under a search warrant.

12 An access order cannot be included in the "post-search approval order" that is issued by a magistrate to authorise an emergent search.

13 Section 465AA(4) *Crimes Act 1958* (Vic). See Explanatory Memorandum, Justice Legislation Amendment (Confiscation and Other Matters) Bill 2014 (Vic) for a discussion on the scope of s. 465AA of the Crimes Act. See also s. 3LA(1),(3) *Crimes Act 1914* (Cwlth).

14 Section 465AA(7) Crimes Act (Vic). See also s. 3LA(1),(3),(4) Crimes Act (Cwlth); s. 58(3)(e) *Criminal Investigation Act 2006* (WA).

15 Current search warrant powers include powers to search the place [s. 157(1)(c)], open anything at the place that is locked [s. 157(1)(d)] and seize and take photographs of evidence or other relevant property [s. 157(1)(h), (j)].

Access orders can only be issued by magistrates and judges, who are not always available

Although a search warrant application can usually be made to any justice of the peace (except in certain situations where it must be made to a magistrate or Supreme Court judge),[16] only a magistrate or judge can issue a search warrant that includes an access order.[17] Police involved in CEM investigations have found that a magistrate or judge is not always available when a search warrant is required, which means that police have to conduct the search without an access order or delay the search. A delay may leave a child at risk of harm, as well as present an opportunity for evidence to be destroyed.

Legislative reform

This problem would diminish with the implementation of either of the legislative reforms suggested previously on page 4 — allowing police to obtain an access order after a search is conducted, or including the requirement for a person to provide access information as a search warrant power.[18] If these reforms were not introduced, another solution would be to amend the legislation so that any justice of the peace could issue an access order.

The scope of an access order is not always sufficient to enable police to obtain required access information or access protected storage devices

To be useful to police, access orders must be able to cater to the range of circumstances that may arise in a CEM investigation. In particular, access order provisions should be broad enough to target all people who may have access information, and to allow police to obtain access information in a range of formats. They should also extend to various forms of storage devices and facilities and be adaptive to constantly evolving technology in this area.

The CCC identified three elements of section 154 that mean the scope of an access order may not always be sufficient to enable police to obtain required access information or access protected storage devices:

- The parties to whom an access order applies may not be broad enough.
- The definition of “access information” may not be broad enough in some situations.
- It is unclear whether access orders apply to information stored at physical locations outside of the search warrant premises.

The parties to whom an access order applies may not be broad enough

In Queensland, police are currently able to use access orders to require a range of people to provide access information. Unlike the equivalent provision in Western Australia,[19] the Queensland provision is broad in that it is not limited to suspects. However, it does not explicitly clarify whether the provision covers system administrators who may have access information relating to the accounts of other people in the network. In the event that section 154 does not cover these circumstances, police officers could execute another search warrant on the system administrator, but this requirement would prolong the investigation process.

Legislative reform

To address this ambiguity, the definition of access information should be clarified to explicitly cover the range of people who could provide access information, including system administrators. The wording of the Commonwealth and Victorian provisions may provide a useful example.[20]

16 Section 150(2)–(4) PPRA. For example, a search warrant application must be made to a Supreme Court judge if police intend to do anything that may cause structural damage when entering and searching a place [s. 150(4)].

17 Section 154(1) PPRA.

18 Evidence could potentially be destroyed between the execution of a search warrant and a later access order.

19 Section 58(3)(h) Criminal Investigation Act.

20 Section 3LA(2)(b) Crimes Act (Cwlth); s. 465AA(5)(b) Crimes Act (Vic).

The definition of “access information” may not be broad enough

Section 154 requires that a person give police the “access information” necessary to access a storage device and any stored content. Access information is defined as:

> information of any kind that it is necessary for a person to use to be able to access and read information stored electronically on a storage device.[21]

It may be argued that this definition is limited to information such as passwords and encryption keys and does not extend to other kinds of assistance that are sometimes necessary to access a storage device, such as providing information to reset or recover passwords (for example, answers to secret questions, recovery email addresses), enabling access to devices via access cards or fingerprint technology, or helping police to identify the person with relevant access information. Without assistance of this kind, there are situations where police may not be able to access material stored on a device.

Legislative reform

Although the validity of the above argument has not been tested in the courts, the definition of access information should be clarified to ensure that it includes other kinds of assistance. The comparable Commonwealth and Victorian provisions, which refer to “any information or assistance that is reasonable and necessary” to allow a police officer to access content on a storage device,[22] may provide useful examples. This would help to cover situations where a person may not have the specific access information police require but may be of help in acquiring it.

It is unclear whether access orders apply to information stored at physical locations outside of the search warrant premises

CEM is increasingly stored online at offsite storage facilities — for example, cloud storage services. This means that the information police are seeking to access is not always physically located at the search warrant premises, but is instead held on servers that may even be located in other jurisdictions. Under section 154, it is not clear whether access orders apply to these kinds of offsite storage facilities. Currently, an access order:

- applies to a person “in possession of access information for a storage device in the person’s possession or to which the person has access *at the place*” [emphasis added][23]
- requires the person to give a police officer access information that will allow the officer to access “stored information *stored on or accessible only* by using the storage device” [emphasis added].[24]

Given this, it is arguable that the use of access orders is limited to information stored on devices at the search warrant location and therefore do not extend to offsite storage facilities. This would mean that any material stored at a physical location outside of the search warrant premises would not come within the ambit of the access order, potentially preventing police from accessing evidence of CEM that may be critical to an investigation.

Legislative reform

To address this problem, the legislation should be amended to include reference to data “held in, or accessible from,” a storage device. This is consistent with the Commonwealth and Victorian provisions, and would clarify that access orders extend to situations where information is stored at a physical location outside of the search warrant premises but can be accessed from a computer or other device at the premises.[25]

---

21 Section 154(2) PPRA.

22 Section 3LA(1) Crimes Act (Cwlth); s. 465AA(2) Crimes Act (Vic).

23 Section 154(1) PPRA.

24 Section 154(1)(b) PPRA.

25 Section 3LA(1)(a) Crimes Act (Cwlth); s. 465AA(3)(a) Crimes Act (Vic). See also Explanatory Memorandum, Justice Legislation Amendment (Confiscation and Other Matters) Bill 2014 (Vic), which notes that an access order should extend to situations where a data server is located outside of Victoria but accessed by a person using a computer or data storage device within Victoria.

Access orders are not always complied with

Access orders are only useful to police investigating CEM offences when they are complied with. Non-compliance with access orders may result in evidence of CEM remaining concealed and, in turn, perpetrators of CEM offences may escape prosecution and the children involved may continue to be exploited. It is therefore desirable that there be a high rate of compliance with access orders.

Consultations with police officers indicated that compliance with access orders varies depending on the nature of the offender and their offences. In some situations, offenders willingly give police access. This is more often the case with low-level offenders, or where police have already accumulated substantial evidence against the person and gaining access to the devices merely verifies evidence obtained elsewhere. On the other hand, police reported that high-level offenders with extensive involvement in the CEM community are often well-informed of the law and law enforcement methods and of technologies used to hide evidence and conceal their involvement in CEM offences. These offenders are less likely to give access information to police, and it is in these situations that an access order must operate most effectively.

Police investigators perceive that certain characteristics of section 154 contribute to non-compliance with access orders. Specifically:

- Failure to comply with an access order is not an offence under section 154 of the PPRA.
- The penalty for failing to comply with an access order is substantially less than the penalty for a CEM offence.

Another characteristic of section 154 that may lead to non-compliance is that the privilege against self-incrimination (assuming it is available) has not been limited or abolished by statute.

Failure to comply with an access order is not an offence under section 154 of the PPRA

A person who fails to comply with an access order (without a reasonable excuse) can only be charged with disobeying a lawful order issued by a statutory authority under section 205 of the *Criminal Code Act 1899*.[26] This is because section 154 of the PPRA does not include an offence provision.

Consultations with investigators from specialist CEM units revealed that people who fail to comply with an access order are rarely charged with the general offence under section 205 of the Criminal Code. An analysis of Queensland Wide Inter-linked Courts (QWIC) data supports this. Since 1 January 2010, 23 people have had court matters finalised for a charge under section 205 for non-compliance with an access order.[27] Only two of these matters were related to suspected CEM offences, and in both cases the person was found not guilty. The low number of charges against people in suspected CEM cases who fail to comply with access orders is indicative of a perception among police officers that doing so is not an effective use of resources, especially because the penalty is seen to be insufficient to deter non-compliance (see further discussion on page 8).

Legislative reform

The utility of access orders would probably be improved if failure to comply with an order was an offence under section 154 of the PPRA. This would ensure the elements of the offence specifically relate to the conduct of failing to comply with an access order, rather than being encompassed by the general section 205 provision that applies to a wide range of circumstances. In turn, the penalty could better match the specific conduct of non-compliance with an access order (discussed further below). Comparable access order provisions in the Commonwealth, Victoria and Western Australia all include a specific offence for non-compliance.

26 Section 156(3) PPRA.

27 Correct as at 16 June 2015.

In contemplating reform in this area, legislators may consider the extent of the offence, including whether there should be any exceptions or defences for non-compliance with an order. A common exception in comparable access order provisions in other jurisdictions is to include an exemption from liability where a reasonable excuse exists — for example, see section 61(2) of the *Criminal Investigation Act 2006* (Western Australia) in Textbox 2.[28]

Textbox 2: Section 61, *Criminal Investigation Act 2006* (Western Australia)

61 Data access order, effect of

(1) A data access order has effect according to its contents.

(2) A person who is served with a data access order and who, *without reasonable excuse* (the onus of proving which is on the person), does not obey it commits a crime.

Penalty: imprisonment for 5 years.

Summary conviction penalty: a fine of $24 000 and imprisonment for 2 years.

(3) It is *not a defence* to a charge of an offence under subsection (2) that information required to be given under the data access order *would or may have incriminated the accused* [emphasis added].

The penalty for failing to comply with an access order is substantially less than the penalty for a CEM offence

A person may refuse to comply with an access order knowing that the penalty for failing to comply with the order is substantially less than the penalty for the CEM offence that the information contained on the storage device may be evidence of. The maximum penalty for failing to comply with an access order is one year's imprisonment, compared with a maximum penalty of 14 years' imprisonment for a CEM offence.[29]

Analysis of the sentences handed down in finalised court matters for a charge under section 205 of the Criminal Code for non-compliance with an access order revealed that actual penalties are often much less than the maximum penalty. Although the defendants in both matters related to suspected CEM offences were found not guilty (see above on page 7), the penalties given in other matters are indicative of possible outcomes. Of the 18 people found guilty of the section 205 offence, 44 per cent (n = 8) were fined, with the value of the fines ranging from $50 to $1000. A further 22 per cent of people (n = 4) received no punishment.

On this basis, a person with even a rudimentary understanding of the legal system would be unlikely to give police access information to storage devices they know contain evidence of CEM, considering the penalty for the CEM offence would be significantly greater than the penalty for failing to comply with the access order. This is a major impediment to police investigating CEM offences.

Legislative reform

The legislation should provide greater disincentive for a person being investigated for CEM offences to refuse to comply with an access order. Possible options include:

- increasing the maximum penalty for failing to comply with an access order
- linking the penalty for failing to comply with an access order to the offence being investigated
- introducing a mandatory minimum penalty for failing to comply with an access order.

Where a person is sentenced to a term of imprisonment, a court could also have the power to order the person's early discharge from prison where the person has subsequently complied with the access order.[30]

---

28 See also s. 465AA(9) Crimes Act (Vic).

29 Sections 205, 228A–D Criminal Code Act.

30 The provision could be modelled on the contempt provisions in the *Crime and Corruption Act 2001*, see in particular s. 199(8F).

Increasing the maximum penalty for failing to comply with an access order

Increasing the maximum penalty for failing to comply with an access order may decrease non-compliance by helping to deter people from opting for the lesser penalty associated with this offence compared with a CEM offence. Compared with Queensland, other Australian jurisdictions have higher penalties for failing to comply with provisions comparable to section 154 — from two years' imprisonment in the Commonwealth, to five years' imprisonment in Victoria, Western Australia and the Australian Capital Territory.[31] In Western Australia, this penalty is commensurate with that for offences relating to the possession of CEM. This ensures that a person being investigated for such offences who disobeys an access order faces a serious penalty.[32]

A similar approach — where the penalty for non-compliance with an order is commensurate with the offence that compliance with the order may prove — exists in Queensland with respect to random breath testing. The maximum penalty for non-compliance with a request for a breath specimen (6 months' imprisonment) is equivalent to the maximum penalty for the offence of driving while over the middle alcohol limit (0.100).[33] This is intended to overcome situations where a person refuses to supply a specimen for a breath test to avoid being detected driving under the influence of alcohol.

Linking the penalty for failing to comply with an access order to the offence being investigated

Another way to deter non-compliance with access orders may be to link the maximum penalty for failing to comply with an order to the offence being investigated, as in other jurisdictions. For example, in the United Kingdom the maximum penalty for non-compliance with an access order is two years' imprisonment, but increases to five years' imprisonment in child indecency cases.[34] By linking the penalty for non-compliance to the offence being investigated, an access order can be uniquely responsive to certain types of offences. In serious matters concerning the protection of children from abuse, including CEM investigations, a higher penalty may be required to deter non-compliance with access orders and ensure that police can conduct effective investigations.

Introducing a mandatory minimum penalty for failing to comply with an access order

Consultations with police revealed a common perception that a mandatory minimum penalty is required to elicit compliance with access orders among high-level CEM offenders. Mandatory sentencing is not used extensively in Queensland.

The privilege against self-incrimination has not been limited or abolished by statute

The common law privilege against self-incrimination provides that a person cannot be compelled to answer any question if doing so may tend to incriminate them in a criminal offence.[35] This extends to making disclosures that may lead to the discovery of real evidence of an incriminating character.[36]

It is arguable that requiring a person to provide access information to a storage device that may contain evidence of an offence infringes the privilege against self-incrimination. A person could potentially refuse to give access information to police investigating CEM offences on these grounds. Although the argument that disclosing access information breaches the privilege against self-incrimination has been rejected in the United

31 Section 3LA(5) Crimes Act (Cwlth); s. 465AA(10) Crimes Act (Vic); s. 61(2) Criminal Investigation Act (WA); s. 116Q(3) *Crimes (Child Sex Offenders) Act 2005* (ACT).

32 Explanatory Notes, Criminal Investigation Bill 2005.

33 Sections 80(5A), 79(1F) *Transport Operations (Road Use Management) Act 1995*. Note that the maximum penalty for the lesser offence of driving over the general alcohol limit (0.050) but not over the middle alcohol limit is three months' imprisonment [s. 79(2)].

34 Section 53(5A) Regulation of Investigatory Powers Act 2000.

35 *Sorby v The Commonwealth* (1983) 152 CLR 281 per Gibbs CJ at 288.

36 *Sorby v The Commonwealth* (1983) 152 CLR 281 per Gibbs CJ at 310.

Kingdom,[37, 38] it has not been tested in relation to section 154 of the PPRA or equivalent provisions in other Australian jurisdictions.

Legislative reform

To reduce the risk of a person failing to comply with an access order on the above grounds, the privilege against self-incrimination with respect to access orders should be removed by statute as in Western Australia and Victoria. In these jurisdictions, a person is not excused from complying with an access order on the grounds that it might incriminate them and there is no restriction on the use of any evidence obtained (see Textbox 2 on page 8 for the WA legislation).[39] A different approach taken to access orders in child protection matters in the Australian Capital Territory is to limit the use of evidence obtained to proceedings under the *Crimes (Child Sex Offenders) Act 2005*.[40]

Conclusion

The access order provision in section 154 of the PPRA was intended to provide police with sufficient powers to investigate a range of serious crimes that are facilitated by technology, including those involving CEM. To remain an effective tool in police investigations, it is important that the power evolves to reflect the rapidly changing technological environment and any elements undermining the general operation of the power are eliminated.

In 2015 the CCC recommended a number of amendments to section 154 to address legislative limitations. To highlight the significance of these legislative deficiencies, this paper has examined the possible impact of these deficiencies in the context of investigations involving CEM offences. In summary, if not addressed, these deficiencies may mean that police are unable to secure evidence to prosecute offenders, and to identify and remove children involved in CEM from harm.

The legislative reforms discussed here will ensure that:

- police are able to obtain access orders in all of the situations where they require access information, including after property is seized
- the scope of access orders is sufficient to enable police to obtain required access information, and to access data accessible from but not physically located at the search warrant premises (for example, data in cloud storage services)
- the likelihood of non-compliance with access orders is reduced.

These reforms are best considered in concert with Chapter Four of the Queensland Organised Crime Commission of Inquiry (2015) report, which delivers a detailed examination of online child sexual offending and CEM.

37 Section 49 Regulation of Investigatory Powers Act (notice requiring a person to provide keys to protected information).

38 It was held that the key to protected information is independent of a person's will and that, although the contents of the device may tend to incriminate a person, the key itself is neutral (*R v S & Anor* [2008] EWCA Crim 2177).

39 See also s. 465AA(6) Crimes Act (Vic).

40 Section 116Q(4) Crimes (Child Sex Offenders) Act.

References

Australian Crime Commission 2015, *Organised crime in Australia 2015*, ACC, Canberra, viewed 29 October 2015, <https://www.crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf>.

CCC — *see* Crime and Corruption Commission.

Crime and Corruption Commission 2015, *Submission to the PCCC review of the Crime and Corruption Commission*, CCC, Brisbane, viewed 29 October 2015, <http://www.parliament.qld.gov.au/documents/committees/PCCC/2015/five-year-review/submissions/014.pdf>.

Queensland Organised Crime Commission of Inquiry 2015, *Queensland Organised Crime Commission of Inquiry*, viewed 30 October 2015, <https://www.organisedcrimeinquiry.qld.gov.au/__data/assets/pdf_file/0017/935/QOCCI15287-ORGANISED-CRIME-INQUIRY_Final_Report.pdf>.

Legislation and associated material cited in this report

Crime and Corruption Act 2001 (Qld)

Crimes Act 1914 (Cwlth)

Crimes Act 1958 (Vic)

Crimes (Child Sex Offenders) Act 2005 (ACT)

Criminal Code Act 1899 (Qld)

Criminal Investigation Act 2006 (WA)

Explanatory Memorandum, Justice Legislation Amendment (Confiscation and Other Matters) Bill 2014 (Vic)

Explanatory Notes, Criminal Investigation Bill 2005 (WA)

Explanatory Notes, Police Powers and Responsibilities and Other Acts Amendment Bill 2006 (Qld)

Police Powers and Responsibilities Act 2000 (Qld)

Regulation of Investigatory Powers Act 2000 (UK)

Transport Operations (Road Use Management) Act 1995 (Qld)

Legal cases

R v S & Anor [2008] EWCA Crim 2177

Sorby v The Commonwealth (1983) 152 CLR 281

Data sources

To identify the legislative limitations of section 154 of the PPRA and determine how they could be addressed, the CCC:

- analysed data from the QPS's QPRIME database to examine the use of section 154 orders in CEM matters
- examined equivalent legislative provisions in all Australian state and Commonwealth jurisdictions and select international jurisdictions (the United Kingdom and New Zealand)
- consulted with QPS officers to understand the practical use of section 154 during CEM investigations, the challenges for police that arise from the limitations of section 154 and options for reform
- analysed QWIC data to examine court outcomes for people charged under section 205 of the Criminal Code with failing to comply with an access order
- examined legislative provisions in other jurisdictions to identify options for reform of section 154.

List of abbreviations

CCC	Crime and Corruption Commission
CEM	child exploitation material
PPRA	*Police Powers and Responsibilities Act 2000* (Qld)
QPRIME	Queensland Police Records and Information Management Exchange
QPS	Queensland Police Service
QWIC	Queensland Wide Inter-linked Courts
section 154	section 154 of the *Police Powers and Responsibilities Act 2000* (Qld)
section 205	section 205 of the *Criminal Code Act 1899* (Qld)

Crime and Corruption Commission
QUEENSLAND

Information on this and other CCC publications can be obtained from:

Crime and Corruption Commission

Level 2,
North Tower Green Square
515 St Pauls Terrace,
Fortitude Valley QLD 4006

GPO Box 3123, Brisbane QLD 4001

Phone: 07 3360 6060
(Toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

www.ccc.qld.gov.au