

10 October 2019

Our ref: CrLC-BDS

Committee Secretary
Legal Affairs and Community Safety Committee
Parliament House
George Street
Brisbane Qld 4000

By email: lacsc@parliament.qld.gov.au

Dear Committee Secretary

Police Powers and Responsibilities and Other Legislation Amendment Bill 2019

Thank you for the opportunity to provide comments on the Police Powers and Responsibilities and Other Legislation Amendment Bill 2019 and the short extension of time in which to provide our submission. The Queensland Law Society (QLS) appreciates being consulted on this important piece of legislation.

QLS is the peak professional body for the State's legal practitioners. We represent and promote over 13,000 legal professionals, increase community understanding of the law, help protect the rights of individuals and advise the community about the many benefits solicitors can provide. QLS also assists the public by advising government on improvements to laws affecting Queenslanders and working to improve their access to the law.

This response has been compiled by the QLS Criminal Law Committee whose members have substantial expertise in this area.

1. Introductory comments

The Society acknowledges that an attempt is made in the *Police Powers and Other Legislation Amendment Bill 2019* (the **Bill**) to resolve the uncertainty in the present legislation governing the search of electronic devices. However, it is the view of the Society that the approach adopted by the Bill is unbalanced. The Bill grants police officers extraordinarily broad powers to pry into the private affairs of people who are not suspected of any offence, and into matters beyond the scope of any suspected offence under investigation. The Society is strongly opposed to the form of the amendments presented in the Bill.

Our commentary on the Bill follows.

2. No threshold for the standard order in a search warrant

A police officer may apply for a warrant to search a place to obtain evidence of the commission of an offence.¹ This is, and will be, the most frequent ground on which an

¹ Section 150(1)(a) *Police Powers and Responsibilities Act 2000*

application is made. A Justice of the Peace ("JP")² may issue the search warrant if satisfied that there are reasonable grounds to suspect the evidence is at the place.³ This is, and will be, the most frequent ground on which a search warrant is issued.

A JP may include in the search warrant a further order regarding electronic information (the standard order).⁴

Alarming, there is no threshold required for the order. That is, there is no requirement that a JP be satisfied of anything before making the order. The order may be included in the search warrant without any reason. It is submitted that, at a minimum, the legislation should require a JP to be satisfied that there is likely to be electronic information that is evidence of the commission of the offence.

3. People to whom the standard order applies

Once the order is made, it will apply to:

- a) every person in possession of any digital device at the place;
- b) every owner of a digital device at the place; and,
- c) every person who has ever used a digital device at the place.⁵

Suppose, for example, that Mr A is suspected of downloading child pornography, and Mr A is a public servant employed in the Department of Premier and Cabinet. He works in an open plan office. A search warrant including the order is obtained for the office in which Mr A works. When police officers arrive to execute the warrant, the standard order applies not only to Mr A, but to every person in the office who possesses a smartphone or a computer; which, in practice, will be every person in the office (including people not present, but whose devices are present).

4. Duties under the standard order

Every person to whom the order applies is compelled to give a police officer:

- a) access to their device;
- b) the password and other log-in information to their device; and,
- c) access to other information, not stored on the device, but accessible through the device, using the internet; including, for example: bank accounts, medical records, tax returns, dating, and match-making services.⁶

There is no requirement that a police officer's request for access to information have anything at all to do with the matter under investigation.

To continue with the example used above, the police officers would have unfettered access to the sensitive information belonging to Mr A's employer and accessible through his computer. Suppose Mrs B sits at the desk next to Mr A. She is not suspected of any involvement in the offence. A police officer is entitled to demand, not only the access code to Mrs B's smartphone, but also the details of her Facebook, Snapchat, and Tinder accounts. The police

² Or Magistrate, or Judge of the Supreme Court (Section 150(2)) but in practice most warrants will be issued by Justices of the Peace.

³ Section 151(a) *Police Powers and Responsibilities Act 2000*

⁴ Section 154 *Police Powers and Responsibilities Act 2000*

⁵ See the definition of "specified person" in the new s.149A inserted by clause 27 of the Bill.

⁶ See the definition of "device information" in the new s.149A inserted by clause 27 of the Bill.

officer is entitled to check the balance of her bank accounts, and to read the email correspondence between Mrs B and her husband.

5. Disconnection from place

The framework of the Act was designed in contemplation of searches of places. It was limited to places where evidence was suspected to be.

The proposed power is, in effect, a judicial order that a person give up the keys to their digital life. It bears little relationship to the place to be searched; so little that the artificial result has already been seen of a search warrant being issued for the police station at which a person or their device happens to be.

6. Conclusion

Such a broad power, unfettered by any checks and balances, has enormous implications for privacy and commercial confidentiality in the modern world. There is also the potential for abuse of this broad power.

The power is an exception to the general rule that a citizen is not required to assist the State to investigate. Whilst a person may not hinder a police investigation, neither are they obliged to assist.⁷ If a police officer demands to know the combination to a safe, or the location of a door key, a person is entitled not to answer. However, if the officer now demands the code to access a document saved on a computer, the person who uses the computer must give up the code. Failure to reveal the information is a crime.⁸ The privilege against self-incrimination is abolished.⁹

In those circumstances, the Society submits that such an extraordinarily invasive power should be restrained within limits to ensure that it is used only for its intended purpose. That would require, at a minimum, firstly, an obligation to satisfy the JP making the standard order that there are reasonable grounds to suspect digital evidence of the offence is likely to be found on a digital device. Secondly, an obligation should be imposed on the police officer to require access only to those devices and on-line accounts, which are reasonably suspected to contain evidence of the offence.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone on (07) 3842 5930.

Yours faithfully



Bill Potts
President

⁷ *O'Reilly v State Bank of Victoria Commissioners* [1983] HCA 47; (1983) 153 CLR 1, *Rice v Connolly* [1966] 2 QB 414, *Leonard v Morris* (1975) 10 SASR 528 – per Bray CJ at 530, *O'Hair v Killian* (1971) 1 SASR 1

⁸ Section 205A *Criminal Code 1899*

⁹ Section 154B *Criminal Code 1899*