Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
P 07 3842 5943 | F 07 3221 9329 | president@qls.com.au | qls.com.au

Office of the President

8 October 2021

Our ref: [KS: CrLC]

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

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

Dear Committee Secretary

Police Legislation (Efficiencies and Effectiveness) Amendment Bill 2021

Thank you for the opportunity to provide feedback on the Police Legislation (Efficiencies and Effectiveness) Amendment Bill 2021 (**the Bill**).

This response has been compiled with assistance from the Queensland Law Society's (**QLS**) Criminal Law Committee and Human Rights and Public Law Committee.

Access Orders for seized digital devices

Clause 8 amends s 154A by expanding the circumstances when a Magistrate or Supreme Court judge may grant an access order for a seized digital device.

Proposed section 154A(1)(b) expands the application of the section to include where the digital device is otherwise lawfully seized under the PPRA, other than under section 176(1)(j) where powers are exercised at a crime scene.

The proposed amendments to section 154A(3)(a) and (b) mean that an application may be made at any time after the digital device is seized, without the current requirement that device was seized under search warrant.

Where a digital device has been seized (other than by a search warrant), a judicial officer may make an order requiring a specified person to do a thing mentioned in section 154(1)(b) or (c) (including to give a police officer access information for the device or to allow a police officer to use access information for the device to gain access to device information from the device).

New section 154A(5) provides that a magistrate or judge may make such an order only if the judicial officer is satisfied that there are reasonable grounds for suspecting that *device information* from the digital device may be evidence of a crime scene threshold offence, that is an indictable offence with a maximum penalty of at least 4 years imprisonment, or an offence involving deprivation of liberty, or evidence of an offence under s 223 (Distributing intimate

images), s 227A (observations or recordings in breach of privacy) and s 227B (Distributing prohibited visual recordings) of the Criminal Code.

The PPRA currently defines **device information** as:

(a) information stored on the device; or

(b) information accessed, communicated or distributed by using the device, including by using an application on the device.

Examples—

- *images stored on a computer*
- *location data stored on or sent from a mobile phone*
- *emails or text messages sent from a smart phone*
- *messages or videos distributed from a social media application on a tablet computer*

An access order may facilitate access to information stored on the device or accessible by using the device.

The Society holds reservations about how these powers might be used in practice. Whilst we are supportive of the judicial oversight which has been implemented into the proposals, in our view, any expansion to the power to compel people to unlock electronic storage systems should be approached with caution.

It has been argued that "[e]xisting police powers need to be examined through a lens that considers mobile phones as akin to private homes"[1].It is important to recognise that access to a digital device facilitates access to the private information of third parties (who have no connection with any offending) and to information which may be privileged or subject to commercial confidentiality. Individual rights to privacy are also impacted. In this regard, we note the right to privacy is preserved in section 25 of the Human Rights Act 2019 where it states that a person has the right not to have their privacy, family, home or correspondence unlawfully or arbitrarily interfered with.

QLS submits that it is these competing interests which necessitate appropriate oversight, management of and restraints to police access to digital devices.

Whilst the current Bill seeks to expand access orders for lawfully seized digital devices (that is, those which are seized other than by a search warrant), it may also be appropriate for the Committee to consider whether a tighter framework is needed around the seizure of devices without a warrant to ensure that current laws reflect the depth of information which is now accessible via a device. It may be that a wider review is required in this regard.

Additional protections should also be considered within the legislation to limit access to the breadth of information which is accessible from a digital device. For example, to ensure cloud-based data is not accessed merely as a result of the device's connection to the internet rather than any connection to a relevant offence. It has also been suggested that detailed records should be kept of the data which is examined and that there should be additional

[1] Raj, Matthew and Marshall, Russ, 'Examining the Legitimacy of Police Powers to Search Portable Electronic Devices in Queensland' *University of Queensland Law Journal* 38 (1) <http://www8.austlii.edu.au/au/journals/UQLJ/2019/5.pdf>, at p 122.

constraints in the ability to make complete copies of device information which may (or may not be) relevant evidence but could still be accessible at a later date.[2]

We suggest that measures of this nature would more appropriately manage the competing interests involved in gathering evidence from devices with respect to any alleged offending by ensuring that there is transparency in the device information which is accessed and provide greater protection of unrelated data and device information.

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

Elizabeth Shearer
President

[2] Ibid at p 123.