LAW ENFORCEMENT (POWERS AND RESPONSIBILITIES) AMENDMENT (DIGITAL EVIDENCE ACCESS ORDERS) BILL 2022

STATEMENT OF PUBLIC INTEREST

Need: Why is the policy needed based on factual evidence and stakeholder input?

As communications in society are increasingly being undertaken online, so too are criminal communications. When investigating crime in NSW, it is increasingly common for key evidence of criminal activity to be digital in nature. This can include communications via digital means (such as messages and emails) and activity on electronic applications or digital files such as documents, photos or videos.

The legislative framework concerning search warrants in NSW already envisages the examination of 'digital devices' in searches authorised by warrant. For example, s75A and s75B of the *Law Enforcement (Powers and Responsibilities) Act 2002* include a range of powers available in respect of the examination of computers in the execution of search warrants. However, the framework does not currently provide clear powers for law enforcement to access where digital devices under the warrant may have access controls aimed to prevent access, such as passwords, PIN codes, encryption keys or biometric security features (e.g. fingerprint access controls).

NSW law enforcement faces ongoing challenges in accessing the information on such devices where a person refuses to provide assistance to access these devices during a search. One factor contributing to this is the lack of NSW legislative power that enables police to compel a person to assist them in accessing a device. In limited circumstances, police may be able to use technology and expert services to bypass the access control. However, even when this is available, this can take valuable investigatory time and resources to access data on the device.

Other Australian law enforcement jurisdictions have also been challenged by this issue resulting in legislative amendments. For example, the Commonwealth inserted section 3LA into the *Crimes Act 1914* in 2018 which provides for a constable to apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to access data within a device. The proposed "Digital Evidence Access Orders" will address this issue in NSW by providing a mechanism for law enforcement officers to obtain an order that can require a person to assist law enforcement in accessing device within the scope of the order. An offence will apply if a person does not comply with such a direction.

Objectives: What is the policy's objective couched in terms of the public interest?

When a criminal offence has occurred, there is public interest in ensuring that law enforcement can identify the extent of offending, the perpetrators of the offence and determine whether legal actions can be brought against the perpetrators. There is also public interest in ensuring that all evidence relevant to the offending can be identified and put before the court in any criminal proceedings.

This is particularly pertinent in respect of criminal offences where NSW legislation already provides for premises searches under a search warrant and crime scene warrant. When a law enforcement officer encounters a digital device in these searches, it is important that they are able to examine data on these devices to ensure that all evidence of criminal offending can be identified.

The introduction of Digital Evidence Access Orders will ensure the NSW legislative framework encapsulates evidence collection requirements in the modern era and addresses the current challenge between accessing digital information versus hard copy. It is expected the reforms

will provide long term benefits to law enforcement to effectively investigate crimes and therefore assist in keeping the community safe.

Options: What alternative policies and mechanisms were considered in advance of the bill?

The reforms can only be achieved through legislative amendment.

However, various options for providing "digital evidence access" powers could be considered. Key options include:

1. No reform.

2. Introduce a new power for police to give a "Digital Evidence Access Direction" in respect of devices without the need for applications to an authorised officer.

3. Introduce "Digital Evidence Access Orders" available in connection with search warrants and crime scene warrants (the approach in the Bill).

Analysis: What were the pros/cons and benefits/costs of each option considered?

1. ***Option 1: No reform.***

Current powers available to law enforcement under the *Law Enforcement (Powers and Responsibilities) Act 2002* do not include a clear power that enables police to compel a person to assist them in accessing a device by providing a password or access code.

If no reform is progressed, NSW law enforcement will continue to have challenges in accessing digital devices encountered when executing search warrants and crime scene warrants, where access is not voluntarily provided by the person

Failing to progress reform would also send a message to the community that criminals can frustrate investigations and potentially evade successful prosecution by undertaking criminal communications and conduct online using complex security codes.

2. ***Option 2: Introduce a new power for police to give a "Digital Evidence Access Direction" in respect of devices without the need for applications to an authorised officer.***

Under this option, a new power could be included in the *Law Enforcement (Powers and Responsibilities) Act 2002* that enables police officers to give, in the course of any investigation, a direction to a specified person to require the person to give the officer any information or assistance reasonable and necessary to enable the officer to access data held in or accessible from a device (a "digital evidence access direction").

This option would require no application to a court or other body to authorise the direction and the new power would be available to all police officers as a 'standard' power available to them under the law.

This option would meet the law enforcement objectives of the reforms. However, this approach would not provide for court-based scrutiny and the additional safeguard this affords.

The model in the Bill adopts a court based approach with approval of the proposed directions by authorised officers. The appropriateness of this approach can be explored as part of the proposed statutory review after two years of operation.

3. ***Option 3 (adopted in the Bill): Introduce Digital Evidence Access Orders" in connection with search warrants and crime scene warrants.***

This option is the reform proposed in the Bill. It provides for a new "Digital Evidence Access Order" that can be applied for and issued in connection with a crime scene warrant or a search warrant. When issued by an appropriate authorised officer, these Orders will authorise a direction to a specified person to require the person to give the officer any information or assistance reasonable and necessary to enable the officer to access data held in or accessible from the device.

This option provides law enforcement with a new mechanism that can assist in accessing electronic data in search warrants. It achieves this by including a new order that can be integrated within the existing application framework for search warrants and crime scene warrants that are provide for within the *Law Enforcement (Powers and Responsibilities) Act 2002*. This provides for scrutiny of the applications by authorised officers and allows for existing features of the search warrant application scheme to be adopted within the digital evidence access order framework.

It is noted that the authority of a search warrant and crime scene warrant already envisages examination of electronic devices. It is therefore appropriate to introduce "Digital Evidence Access Orders" in this context to provide additional mechanisms that ensure searches conducted in accordance with these warrants can operate as effectively as possible.

The proposed approach will also limit the resource impact of the new orders by providing for the possibility of a significant proportion of digital evidence access orders to be applied for and dealt with at the same time as the 'underlying' warrant application.

After Digital Evidence Access Orders have been introduced to the NSW legislative framework, it will be necessary to identify whether any improvements can be made to their operation. This will be explored as part of the statutory review after two years of operation. The appropriateness of the proposed context in which these Orders are available can also be reviewed at this time.

Pathway: What are the timetable and steps for the policy's rollout and who will administer it?

The Bill is proposed to commence on 1 February 2023. This will provide adequate lead time for key agencies within the NSW criminal justice system to implement necessary arrangements for the reforms.

The amendments will be made to the *Law Enforcement (Powers and Responsibilities) Act 2002*, which is administered by the Attorney General and the Minister for Police.

Consultation: Were the views of affected stakeholders sought and considered in making the policy?

Yes. When developing these reforms, NSW government agencies such as the Department of Communities and Justice, NSW Police Force, NSW Crime Commission and the Office of the Director of Public Prosecutions were consulted.

Prior to introducing the Bill, the NSW Government considered the views of key stakeholders by providing an opportunity for targeted stakeholders to provide written comment on draft legislative instruments and discussion papers.

External stakeholders who were approached to provide comment on the Bill include representatives from the Legal Sector.

All stakeholder comments were considered as part of the finalisation of the Bill.