DIGITAL ACCESS ORDERS – PROVIDING ADVICE AND EVIDENTIARY CONSIDERATIONS

Trudie Cameron, Principal Lawyer | Practice Leader – NSW & ACT Criminal Law, Armstrong Legal

Legal Wise – Criminal Law Conference 2025, March 2025

OVERVIEW

A Digital Access Order requires the person subject to the order to give police access to specified electronic devices and the data contained in them. In practice, this means that police can compel a person to provide any necessary passwords, passcodes, fingerprints, facial recognition or multifactor authentication to allow access to the device itself, as well as access to the data contained on it.

In some cases, this will involve multiple layers of access. For example:

1. a passcode may be required to unlock a mobile phone;
2. a password, facial recognition or multifactor authentification may be required to open and log into a certain application within that phone; and
3. a password or encryption key may be required to access communications or data within that application on the phone.

The NSW state based Digital Access Orders are similar in nature to "3LA Orders", the Commonwealth counterpart in s 3LA of the *Crimes Act 1914*.

While there was initially somewhat of a slow take up after the 1 February 2023 introduction of the power, there is now an increasing trend of NSW Police applying for and obtaining Digital Access Orders under Part 5, Division 4A of the *Law Enforcement (Powers and Responsibilities) Act* (hereafter "LEPRA").

This paper focuses on:

1. The application process;
2. What the order authorises police to do or request (and what it doesn't authorise);
3. What advice should be provided to clients who are subject to an order;
4. The consequences of non-compliance; and
5. Evidentiary considerations in proceedings in which a digital access order was made, and in particular, excluding admissions which fall outside the scope of the order.

LEGISLATION

On 1 February 2023 the legislative provisions relating to Digital Access Orders came into effect. The *Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Act 2022* inserted the provisions relating to Digital Access Orders, into Division 4A into Part 5 of LEPRA.

The amendments were made in order to provide police with a mechanism to compel a person to provide access to data held within electronic devices seized in conjunction with a search warrant. Prior to the introduction of the new powers police could seek a person's assistance or consent to provide passwords and access, however they could not force a person to provide them with passwords or access.

With the rise in use of electronic devices (and security measures on devices) Police were increasingly encountering difficulties in obtaining evidence in connection with investigations. While advanced forensic methods can sometimes be used successfully to get access to data on devices, such is not guaranteed. Furthermore, it's not instantaneous (causing delays in investigations and backlogs particularly in the Digital Forensics Unit) and consumes considerable resources. The legislative reform sought to cure this.

APPLICATIONS FOR ORDERS

The sections governing the making of an application for digital access orders are contained in ss 76AB to 76AH of the *Law Enforcement (Powers and Responsibilities) Act 2007*.

The Application Process

An application for a digital access order:

1. Can only be made by an 'eligible applicant' (s76AB(1) of LEPRA). With respect to who is an 'eligible applicant':
    a. the categories of 'eligible applicants' are prescribed in s 46 of LEPRA;
    b. there are numerous different 'eligible applicants' for digital access orders based on the type of warrant the digital access order is sought in relation to; and
    c. any NSW Police Officer is an eligible applicant for a digital access order in connection with a search warrant (see s 46(1) of LEPRA, specifically the interpretation of "eligible applicant" at (e)).
2. Can only be made in connection with a "search warrant" or a "crime scene warrant" (s76AB(1) of LEPRA, see also s 76AA of LEPRA for 'search warrant' and s 94 of LEPRA for 'crime scene warrant'). To be made "in connection with" a warrant, the digital access order:
    a. Can be applied for at the same time as the application for the warrant or after the warrant is issued (regardless of whether it has been executed or not); and
    b. Can't be made before the warrant is applied for, or if the application for the warrant has been refused.
3. Can be made:
    a. In person (s 76AC of LEPRA);
    b. By email or other electronic means (s 76AD of LEPRA);

    c. By phone (s 76AE of LEPRA), but only if it is not practicable for the application to be made in person or by email;

   and must be in the form prescribed by the regulations.

4. The form to be used for an application for a digital access order is Form 33 in Schedule 1 of the *Law Enforcement (Powers and Responsibilities) Regulations*.

Where the application is made in person or by email or other electronic means, the police officer applying for the order must verify the information in the application on oath or affirmation (before the eligible issuing officer) or by affidavit. It is an offence to knowingly give false or misleading information in such an application (s76AG of LEPRA).

If an application is refused, a further application can only be made:

1. To a Magistrate; or
2. To an eligible issuing officer, but only if the further application includes additional information that justifies the making of the further application (s76AH of LEPRA).

The legal test

An application for a digital access order can only be granted in circumstances where the requirements under s 76AJ of LEPRA are met. These include four limbs or questions:

1. The threshold question – that the order will:
    a. authorise an "executing officer";
    b. to issue a direction in accordance with s 76AM(1) of LEPRA (that is, the digital access order);
    c. in relation to a computer (which is defined as "an electronic device for storing, processing or transferring information" s 76AA of LEPRA);
    d. that has been found, or may be found;
    e. in the execution of a search warrant or crime scene warrant that has already been issued or will be issued at the same time as the order;
2. The reasonable grounds question – the eligible issuing officer must be satisfied:
    a. that there are reasonable grounds for suspecting evidential material is held in, or is accessible from, the computer;
3. The connection to the device question – the eligible issuing officer must be satisfied:
    a. that the specified person who will be subject to the order is:
        i. Reasonably suspected of having committed the offence stated in the warrant;
        ii. The owner or lessee of the computer (or is an employee of, or a person engaged under contract for services, of the owner or lessee of the computer;
        iii. A person who uses or has used the computer; or
        iv. A person who is or was a system administration for the system including the computer;

4. The relevant knowledge question – the eligible issuing officer must be satisfied that the specified person who will be subject to the order has relevant knowledge of:
    a. The computer or a computer network of which the computer forms or formed a part; or
    b. Measures applied to protect data held in, or accessible from, the computer.

When determining whether there are reasonable grounds to issue a digital access order, the eligible issuing officer must consider the reliability of the information on which the application is based, including the nature of the source of the information; s 76AI of LEPRA.

When a digital access order is granted:

1. It must be reduced to writing in the form prescribed by the regulations (which is form 35 of Schedule 1 of the *Law Enforcement (Powers and Responsibilities) Regulation*); s 76AK of LEPRA; and
2. It remains in force for 7 business days after issue (unless it is an order in connection with a covert search warrant in which case it is in force for 10 days after it is issued); s 76AL of LEPRA.

WHAT POLICE ARE AUTHORISED TO DO OR REQUEST

Section 76AM of LEPRA prescribes the effect of a digital access order as follows:

> *(1) The executing officer for a digital evidence access order may direct the specified person to--*
>
> > *(a) give the officer any information or assistance reasonable and necessary to enable the officer to access data held in or accessible from a computer specified in, or within the scope of, the order, or*
> >
> > *(b) give the officer any information or assistance reasonable and necessary to allow the officer to--*
> >
> > > *(i) copy data from a computer specified in, or within the scope of, the order to another computer, or*
> > >
> > > *(ii) convert the data into a documentary form or another form intelligible to a computer used by the officer.*
>
> *(2) Without limiting subsection (1), the executing officer may require the specified person to provide reasonable and necessary assistance in accessing data on a computer that is secured by biometric means, including, for example, fingerprints or retina scans.*
>
> *(3) To avoid doubt--*
>
> > *(a) information provided by a specified person under subsection (1) to access data held in or accessible from a computer may be used only for that purpose and no other purpose, and*

> *(b) this section is subject to any other provision of this Act or another Act that provides for how a police officer may take particulars that are necessary to identify a person*.

NON-COMPLIANCE

It is an offence to fail to comply with the order without reasonable excuse; s 76AO of LEPRA. The maximum penalty is 100 penalty units and/or imprisonment for 5 years.

It is not a reasonable excuse to not comply on the basis of a right against self-incrimination. Failure to remember a password (particularly if it is an automated or autogenerated password, or a password set a long time before) may well be an example of a reasonable excuse. However, if a person does not assist police to access the data by providing assistance such as answers to 'secret questions', access to email accounts to reset passwords or multifactor authentication it would appear unlikely that the 'reasonable excuse' defence would be made out.

ADVICE TO CLIENTS

When advising a client who is or might be the subject of a digital access order, the following topics should be canvassed:

1. What the order is;
2. What the order allows police to do (and doesn't allow the police to do);
3. What the order requires them to do;
4. The consequences of complying;
5. The consequences of not complying; and
6. What's likely to happen next.

What an order is and what it allows police to do

Explaining to a client what a digital access order actually is, is very important. Your client needs to understand the effect of the order in practice. You should explain that the order allows police to force them to:

1. give police access to their electronic devices;
2. give police access to the data contained on or in the device; and
3. give police access or assistance to allow them to copy or convert any of that data.

In some cases, this will involve multiple layers of access. For example:

1. a passcode may be required to unlock a mobile phone or a desktop computer;
2. a password, facial recognition and/or multifactor authentication (using another device) may be required to open and log into a certain application within that phone or computer; and
3. a password or encryption key may be required to access communications or data within that application on the phone.

Giving practical examples of what this means and what your client will need to do will often help illustrate the point. For example, you may ask the client if they have a pin code to open their phone, or facial recognition, or both. You'll need to explain that the order requires them to enter that pin, or present their face, to unlock the phone for police. You may need to explain that they need to also allow police to access any application, folders, files or data in the phone. For example, if the police wish to access an email application on the phone that is protected by a password and multifactor authentication, you should explain they will need to assist police by providing this password and/or using another device to complete the multi-factor authentication.

There may be instances where a client does not know, or cannot remember, a password. In these circumstances, they would be required to assist with retrieving a saved password (for example, if the person has passwords saved via a google account, they may need to log into that google account and enter the password for the google account), setting a new password to access the account or application, or providing answers to secret questions.

What an order doesn't allow police to do

Your client also needs to understand that the order does not allow police to force them to answer questions at large, or indeed, any questions beyond the scope of providing any information or assistance which is reasonable or necessary to allow police to access the device and the data contained within it (or copy it). Examples of questions police may ask clients, which they do not need to answer under the order include:

1. Where or when did you get this phone/computer/device;
2. What do you use this application for;
3. Why did you download this application;
4. When did you set this password;
5. When was the last time you logged in to this computer;
6. When did you make this note/enter this data;
7. Were you the person who sent this message;
8. Who is this person you're speaking to in this conversation; and
9. In an instance where a password has been forgotten – questions about why the person can't remember the password and/or questions designed to challenge the clients assertion that they've forgotten the password.

It also does not require the person to show or direct police to specific material they are looking for. For example, police can require a person to enter a password for an encrypted folder titled "teens", but they cannot require a person to identify where they have saved child abuse material onto their computer.

Consequences of complying

It is important to explain to clients not only that they must comply with the order (and what they need to do to comply), but also what may happen as a result of such. Clients should be told that giving police access to their phones or devices may (or likely will) result in:

1. Police obtaining evidence of the commission of an offence or offences;
2. Police charging them with one or more offences;

3. Police placing them under arrest;
4. That they may be bail refused by the police and/or court;
5. That they may be found guilty of one or more offences; and
6. That they may be sentenced to gaol as a result.

Consequences of not complying

The consequences of not complying with the order should also be explained.

It's important to note that you should explain that if they don't comply, they will almost certainly be charged with failing to comply pursuant to s 76AO of LEPRA (which carries a maximum penalty of up to 100 penalty units and/or 5 years imprisonment), and may be sentenced to gaol for that offence. However, you should also explain that if they don't comply:

1. Police may still obtain access to the devices in question and obtain relevant evidence of the commission of an offence (and arrest, charge, refuse bail in relation to such); or
2. The police may not ever be able to obtain access to the devices in question, and thus may never obtain relevant evidence of offences.

An ethical reminder – your paramount duty to the administration of justice

As a solicitor, your paramount duty is the duty to the court and the administration of justice; Rule 3, *Legal Profession Uniform Law Australian Solicitors Conduct Rules 2015*. You cannot ever advise a client to commit an offence, or to hinder a police investigation. You cannot and should not suggest or infer such. While your duty to act in your best interests of your client (and deliver legal services competently and diligently) does require you to provide your client with advice about digital access orders and the consequences of such, you cannot breach the paramount duty to the administration of justice in doing so.

It would be a breach of the rule, for example, to suggest that a client is 'better off copping' a charge of failing to comply with a digital access order than they are complying with the order and 'copping' various charges relating to supplying drugs or possessing child abuse material.

What's likely to happen next

It's good client management to explain the general process and what's likely to happen next, including:

1. That police will:
    - a. Film the entire interaction (and remind them that they should not say or do anything beyond complying with the order);
    - b. likely show them the order (and if they don't, they can and should ask for it);
    - c. explain the order;
    - d. 'place them under the order' and ask them to comply with the order;
    - e. usually either access the device and do a preliminary search and/or copy certain data and/or seize it;
    - f. conduct the rest of the primary search warrant; and

2. That they can ask police for an opportunity to get further legal advice if any questions at all arise (and you should urge them to do this if they think the police are asking them questions they're not allowed to or not required to answer).

If time permits (or in a later call) you may also wish to provide relevant advice about:

1. Arrest, charging and bail determinations;
2. Forensic Procedures;
3. What happens if they are refused bail and preparing for a bail application; and
4. Court procedure.

EVIDENTIARY CONSIDERATIONS

Provision of access and assistance – use of evidence

It is possible that the act of providing access to, or assistance to access a device and the data within will be sought to be used by the prosecution as further evidence of the commission of offences.

For example, if police obtain a search warrant and digital access order for your clients home and devices on the basis that there are reasonable grounds to suspect he or she is in possession of CAM, and your client assists by providing relevant passwords and access and the police locate CAM, the prosecution case may rely on:

1. Evidence of the CAM found on the device; and
2. Evidence that the client knew the relevant passwords, passcodes etc to access the device and material contained therein as evidence that they were knowingly in possession.

Inspection of records

If there are concerns about the validity of the making of the digital access order (or the accuracy/veracity of the information contained in the application), it may be appropriate to seek to inspect the application for the digital access order, any supporting affidavit or material and any records by the issuing officer as to why the application was granted (they are required to make a record of all relevant particulars of the grounds they've relied on to justify the issue of the order; s 76AP of LEPRA).

Reg 13 of the *Law Enforcement (Powers and Responsibilities) Regulations* provides for the keeping of these records for 6 years at the relevant Local Court Registry (and specifically refers to records relating to applications for digital access orders). Reg 13(7) provides for who may inspect the records and when. Digital access orders aren't specifically provided for, however there *may be* scope to argue that the records fall within reg 13(7)(a) "in the case of any warrant other than a warrant referred to in paragraph (b) or (c)—by the occupier of the premises to which the warrant relates or by any other person on behalf of the occupier", as the order is made in connection with such a warrant.

Applications based on false, misleading or improper information

Where the application for a digital access order was supported by information which was false, misleading or otherwise improper an application to exclude unlawful or improperly obtained evidence pursuant to s 138 of the *Evidence Act* can be made. If successful, it could result in relevant evidence being excluded from proceedings and offences being unable to be proven beyond reasonable doubt.

Where an order isn't sought

In the event police improperly or unlawfully force your client to provide access or assistance without having first obtained an order, the availability of the application process and the fact this process wasn't embarked on will be a relevant consideration to any application to exclude evidence pursuant to s 138 of the *Evidence Act*. Such an example may include circumstances where police seize a phone pursuant to a search warrant, and hold the phone up to your client's face to unlock it, without their consent.

Defects in orders

If an order suffers from a defect that affects the substance of the order in a material particular, then the order is invalid; s 76AQ of LEPRA. An application to exclude evidence pursuant to s 138 of the *Evidence Act* can be made.

Exclusion of unfair or improper admissions

Where a police officer, under the guise of or in connection with a digital access order, questions a person about matters beyond the ambit of an order, it may be appropriate to seek to exclude such evidence. Applications to exclude the evidence can be made pursuant to ss 90 and 138 of the *Evidence Act*.