## 7.0 CHALLENGES TO ENFORCEMENT

Enforceability of current legislation in the Northern Territory is problematic, and these problems are likely similar throughout other Australian jurisdictions. The key challenge in evidence gathering is the ability to gain access to the evidence in a timely way. The nature of the evidence is both the data on the source device used to originally capture the images and, more importantly, the websites where these images or videos are posted and subsequently accessed. As many social media services and devices are moving to cloud storage of data, there needs to be some lawful authority to obtain this information and to present it at hearing. The scope of the information required by investigators is limited to that information that is normally available to the user of the device.

Given the likely increase in the number of such offences, there needs to be available mechanisms that facilitate their ready execution and yield quick results. At present, there appear to be two main ways in which this information is obtained, both of which are problematic. The first approach is to contact the service provider directly and request the information and the second is to apply for a warrant under the *Crimes Act 1914* (Cth). Applications under the *Crimes Act 1914* (Cth) are problematic and open to criticism where they are used to enforce State legislation. Additionally, the process of obtaining such a warrant is burdensome and would need to be streamlined as it becomes increasingly relevant to more offences (for example, breach of a domestic violence order by Facebook Messenger). Applications to service providers have proven to be long and drawn out and often involve multiple agencies.

Considerations for reform of police powers include:

- the ability to use a device to access data stored online that would normally be available to the user of that device (e.g. web based email; Facebook feeds; Twitter; Snap Chat, etc.);

- the power to require biometric and password unlocking of devices (e.g. PIN; fingerprint; facial recognition, etc.); and

- the power to compel the provision of passwords for accounts in the same way as personal particulars.

In evaluating these proposals, consideration would also need to be given to the balancing of personal rights and freedoms, which is beyond the scope of this report. Examples of these challenges include:

- the potential for additional offences to be identified unrelated to the original reason for exercising the power and protections against its use;

- the risk of data loss if the device is set to remote wipe; and

- the potential to infringe the rights of innocent third parties.