CDPP
Australia's Federal Prosecution Service

Submission by the Commonwealth Director of Public Prosecutions

Parliamentary Joint Committee on Law Enforcement: The capability of law enforcement to respond to cybercrime

December 2023

Introduction

1. The Office of the Commonwealth Director of Public Prosecutions (**CDPP**) welcomes the opportunity to provide a submission to assist the inquiry into the capability of law enforcement to respond to cybercrime.

2. This submission draws on the CDPP's experience prosecuting both cyber-dependent crime contrary to Part 10.7 of the *Criminal Code* (Cth) (**the Criminal Code**), being crimes directed at computers or other information communications technologies; and cyber-enabled crime, being offences which are facilitated through the use of computers and other forms of information communications technologies.

Role of the CDPP

3. The CDPP is an independent prosecution service established by Commonwealth Parliament to prosecute offences against Commonwealth law. The CDPP aims to provide an effective, ethical, high quality and independent criminal prosecution service for Australia in accordance with the Prosecution Policy of the Commonwealth.

4. The CDPP receives briefs of evidence from investigative agencies for assessment as to whether a prosecution should commence or continue. The CDPP undertakes any resulting prosecution. The CDPP received referrals from both Commonwealth, State and Territory agencies. The CDPP is a prosecution agency and has no legislative remit to conduct criminal investigations.

5. The work of the CDPP is divided into four prosecution Practice Groups.[1] All four practice groups prosecute or otherwise deal with cyber-enabled crime. This reflects the increasing role that digital technology plays in facilitating the commission of all crime types. Cyber-dependent crime is generally prosecuted by the Human Exploitation and Border Protection Practice Group.

Legislative Background and Offences

6. Criminal offences which capture cyber-offending are contained in a mixture of Commonwealth, State and Territory offences.

7. At the Commonwealth level, Part 10.7 of the Criminal Code entitled "*Computer offences*", contains cyber-dependent offences, being offences directed at computers or other information communications technologies; or in more technical terms, offences for which a core element is the unauthorised access to, modification of, or impairment of data.

8. While Part 10.7 of the Criminal Code contains cyber-dependent offences, there are a myriad of other Commonwealth offences which are facilitated using computers and other forms of information communication technologies, but for which a cyber aspect is not an element of the offence itself. To provide some examples, it might be the case that the commission of a Part 7.3 fraud offence or a Division 400 money laundering offence involved the use of computers to facilitate the offences. It might also be the case that the commission of online child sex exploitation offences involved the use

[1] The CDPP's prosecution Practice Groups are Human Exploitation and Border Protection, Organised Crime and National Security, Serious Financial and Corporate Crime, and Fraud and Specialist Agencies. The CDPP's four prosecution Practice Groups are supported by a fifth Practice Group, being the Legal Capability and Performance Practice Group.

of information communications technologies, for example, using a carriage service to access and transmit child abuse material. These are examples of cyber-enabled crimes.

9. Beyond Commonwealth offences, State and Territory legislation also contains an array of cyber-dependent and cyber-enabled offences. The ambit of those offences overlap to varying extents with the Commonwealth offences. The maximum penalties vary between the jurisdictions. The content of State and Territory offences are beyond the scope of this submission.

Prosecution trends and statistics

10. This section will solely deal with the CDPP's experience in prosecuting Part 10.7 cyber-dependent offences.

11. The prosecution of cyber-dependent offences against Part 10.7 of the Criminal Code have been limited in number. In the period 1 July 2018 to 30 November 2023, the CDPP commenced prosecutions against **34** defendants for at least one Part 10.7 offence. As at 30 November 2023, **one** prosecution remains ongoing, **six** defendants are awaiting sentence, **one** matter was discontinued and withdrawn, and the remaining **26** defendants were convicted of at least one offence.[2]

12. The following table sets out the number of charges for each offence provision that proceeded to sentence during that period.

Prosecutions which proceeded to sentence between 1 July 2018 to 30 November 2023 by charge

Offence provision	No. of charges
Section 477.1(1)	2
Section 477.2(1)	5
Section 477.3(1)	6
Section 478.1(1)	41
Section 478.2(1)	0
Section 478.3(1)	1
Section 478.4(1)	1
TOTAL	**56**

13. The limited number of cyber-dependent offences prosecuted by the CDPP to date means that there is presently insufficient sentencing data available to draw meaningful conclusions about sentencing trends. That being the case, the CDPP observes that the most significant sentence for a cyber-dependent crime was for two years and three months' imprisonment, with the offender to be released on a recognizance after 16 months.[3] That sentence was imposed on an offender who had been convicted of one offence contrary to s 477.1 of the Criminal Code, one offence contrary to s 478.4(1) of the Criminal Code, and one offence contrary to s 192E of the *Crimes Act 1900* (NSW). The relevant offending involved the offender, in short, engaging in an extensive and elaborate internet/computer fraud. The particulars of the fraud involved him unlawfully accessing sensitive personal information and possessing that information with the intent of committing fraud, and also phishing to obtain further sensitive personal information. This case was the only one involving a sentence of imprisonment exceeding 12 months in duration.

[2] Please note that it is not necessarily the case where a defendant was convicted of at least one offence, that that offence was a Part 10.7 cyber-dependent crime.
[3] The recognizance release order was fixed with reference to an aggregate sentence, rather than being solely referable to the specified count which involved an indicative sentence of two years and three months' imprisonment.

International co-operation

14. Cybercrime often occurs across international borders, which means that the successful prosecution of cybercrime offences requires effective cooperation between law enforcement agencies at the international level.

15. The CDPP's experience has been that the successful prosecution of cybercrime often requires a close working relationship between Australian law enforcement agencies and their international counterparts. The CDPP supports the continued strengthening of those partnerships. The CDPP notes, for example, that prosecutions involving an Australian and United States nexus have benefited from effective partnerships between Australian and United States law enforcement agencies (including the Federal Bureau of Investigations and the United States Department of Justice). Serious and organised crime is increasingly undertaken on a global scale without regard to international borders.

16. The CDPP further notes that where evidence has been received on a police-to-police basis, a successful prosecution will often only be possible where the evidence is subsequently obtained pursuant to the provisions of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (**MA Act**). Formal evidence gathering using the provisions of the MA Act help to ensure that any evidence gathered is admissible in courts in Australia. The CDPP supports any amendments or other policy reform that would help to streamline and accelerate the obtaining of admissible evidence from foreign entities. The CDPP notes, by way of example, that it is hoped that the introduction of the *Australia-US Cloud Act Agreement*[4] will aid in achieving these ends for some evidence as between Australia and the United States.

Challenges caused by the voluminous amounts of digital evidence in cybercrime

Resourcing challenges for investigative agencies

17. The proliferation in the use of technology to facilitate criminal offending presents resourcing challenges for prosecution and investigative agencies. Encrypted communications may limit the ability of agencies to access relevant communications or may delay agencies obtaining access to such communications. It is not uncommon for digital devices, such as mobile phones and computers, to be seized when a defendant is arrested and charged with a criminal offence. However, it may take many months for investigating agencies to be able to gain access to all of the data on those devices. This can delay the progress of a criminal prosecution.

18. Even after access is achieved, the devices might contain such a large volume of evidential material s to present resourcing challenges for investigators and prosecutors tasked with reviewing that material to determine its relevance and evidentiary value. It is also not uncommon for such devices to contain evidence of further uncharged offences. For example, in the context of child sex exploitation matters, such a review process can sometimes result in the discovery of significant amounts of child abuse material, which leads to the laying of further charges.

19. Increasing data volumes present challenges to all parties in the justice system, including police, prosecutors, defendants, defence legal representatives, and the courts. At the same time, new technology also offers the prospect of being able to interrogate and sort large data sets more quickly to identify relevant information.

[4] Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.

Disclosure

20. The Prosecution's "duty of disclosure" is a fundamental legal obligation which helps to ensure that every accused receives a fair trial. The CDPP's disclosure obligations are set out in the CDPP's Statement on Disclosure[5] and are also sourced within State and Territory statutes. These disclosure obligations generally require the Prosecution to disclose to the defendant material that will be relied on by the Prosecution to prove its case, material that can be seen on a sensible appraisal as running counter to the Prosecution case, material that might reasonably be expected to assist the defendant in advancing a defence, and material that might reasonably be expected to undermine the credibility or reliability of a material witness. Whereas it was once possible for prosecutors to meet these obligations by manually reviewing each item seized by investigators, the proliferation of digital technology and the exponential growth in data volumes means that such an approach is no longer possible. Increasingly, prosecutors and investigators must work closely together to leverage technology to ensure that all disclosable material is identified and provided to a defendant.

Limiting the disclosure of personal information

21. The CDPP's experience in prosecuting cybercrime is that investigative agencies will often seize a large amount of sensitive personal information. By way of example, where a defendant has allegedly caused a data breach, any devices seized from the defendant may contain large amounts of sensitive personal information obtained through that data breach.

22. Where an instance of cybercrime involves the unlawful dealing with personal information, that personal information may need to be included in the Prosecution's brief of evidence to establish elements of the relevant offence. Whilst investigators and prosecutors may be required to consider individual redactions to that material to protect the privacy of victims whose personal information has already been compromised, in some instances, the personal information itself may be relevant to the prosecution case and access to that information must be provided to the defendant.

Cybercrime: A Prosecution perspective on legislative gaps and opportunities for reform

Deepfakes and the offence in s 474.17A of the Criminal Code

23. The CDPP has received referrals from investigative agencies in relation to 'deepfakes', being cases where individuals have created media which depict victims in certain poses or saying or doing things, where those victims have not in fact said or done those things individual. For example, an individual might create a deepfake image or video which superimposes a victim's face on another body so as to depict the victim engaging in a sexual act, in circumstances where the victim was never in fact involved in that sexual act.

24. It is observed that the federal offences under ss 474.17 and 474.17A of the Criminal Code may not capture this conduct.

25. Section 474.17(1) of the Criminal Code makes it an offence for an individual to use a carriage service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing, or offensive. The maximum penalty for that offence is three years' imprisonment.

26. Section 474.17A(1) of the Criminal Code is an aggravated form of the offence in s 474.17(1), and provides that where the offence in s 474.17(1) is committed in a way that involves the transmission, making available, publication, distribution, advertisement or promotion of *private sexual material*, the

[5] https://www.cdpp.gov.au/system/files/Disclosure%20Statement-March-2017.pdf

offender will be liable for the offence in s 474.17A(1) which is punishable by a maximum of five years' imprisonment.

27. While an individual's transmitting of deepfakes using a carriage service may constitute an offence contrary to s 474.17(1),[6] the CDPP considers that such conduct is unlikely to constitute an offence contrary to s 474.17A(1). That is, *even if* the deepfakes being transmitted depict a victim engaging in a sexual activity or purport to depict the victim's sexual organ, anal region, or breast region,[7] such conduct is unlikely to contravene s 474.17A(1). This is because deepfakes of such a nature will not constitute "*private sexual material*" as defined in s 473.1.

28. The definition of "*private sexual material*" in s 473.1 can be satisfied in two ways – *first* where the material depicts the victim engaging in a sexual pose or sexual activity in circumstances that reasonable persons would regard as giving rise to an expectation of privacy; and/or *second* where the material depicts the victim's sexual organ, anal region, or breast region, in circumstances that reasonable persons would regard as giving rise to an expectation of privacy. The issue that arises is that, as the victim was not involved in the creation of the fictional 'deepfake' version of themselves, it cannot be said that any expectation of privacy attaches to the depiction of the victim.

29. The consequence of the above is that where an individual engages in conduct relating to deepfakes using a carriage service, the most likely available Commonwealth offence will be that available under s 474.17(1) of the Criminal Code. The CDPP observes that the maximum penalty for an offence against s 474.17(1) is three years' imprisonment.

Dealing with unlawfully obtained data

30. In some cases, an individual may misuse data that has been unlawfully obtained by another person. By way of example, the CDPP prosecuted an offender who downloaded data that had been obtained unlawfully by another individual, and then used that data in an attempt to extort the victims of the data breach. In that matter, the individual pleaded guilty to two counts of using a telecommunication network with intention to commit a serious offence contrary to s 474.14(2) of the Criminal Code, with the serious offence being a State blackmail offence.

31. However, given the anecdotal accounts of stolen data being obtained and/or used for improper purposes, there may be no available offence to cover an individual who has knowingly or recklessly dealt with unlawfully obtained data but may not yet have engaged in further criminal conduct by using that unlawfully obtained data in the commission of a criminal offence.

Maximum penalties

32. The maximum penalties for ss 478.1 to 478.4 offences range between two and three years' imprisonment.

33. Maximum penalties must be carefully considered, *firstly*, because the legislature has legislated for them; *secondly*, because they invite comparison between the worst possible case and the case before the court at the time; and *thirdly*, because in that regard they do provide, taken and balanced with all of the other relevant factors, a yardstick.[8] The maximum penalty signifies to sentencing judges (and to

[6] The CDPP observes that it is not necessarily the case that in each case where deepfakes are transmitted that the individual will have committed an offence contrary to s 474.17. It remains the case that the individual's conduct must otherwise be menacing, harassing, or offensive, and the use of deepfakes is just one consideration that may be relevant to this determination.
[7] Criminal Code s 473.1.
[8] *Markarian v R* (2005) 228 CLR 357, [30]-[31]; *Elias v R* (2013) 248 CLR 483, [27].

the community and to offenders) the seriousness with which the legislature regards offences of the kind in question.[9]

34. The maximum penalty for an offence is one of many factors to be taken into account to determine the appropriate sentence for an offender and can underscore the relevance of general deterrence[10] and serves as a basis of comparison between the case before the Court and the worst category of case.[11]

35. Given the increasing scale of modern cyber-dependent crime, the assessment of what is considered to fall within the "*worst possible case*" is likely to also increase.

Conclusion

36. The CDPP is available to provide further information to the Committee if required.

[9] *Markarian v R* (2006) 228 CLR 357 [31] (Gleeson CJ, Gummow, Hayne, and Crennan JJ); see also *Rex v Taylor* [2022] NSWCCA 256 [60]; *Muldrock v The Queen* (2011) 244 CLR 120 [31].
[10] *R v Lambert* (1990) 51 A Crim R 160.
[11] *Markarian v R* (2005) 228 CLR 357, [39]; *Lodhi v R* [2007] NSWCCA 360.