Cyber-Dependent and Cyber-Enabled Crime: Legal Responses and Challenges

Chapter 5

Cyber-Dependent and Cyber-Enabled Crime: Legal Responses and Challenges

Monique Cormier and Simon McKenzie*

Introduction

[5.10] The term "cybercrime" is any crime committed using computers or online networks.[1] It is more constructive, however, to consider cybercrime in two categories: cyber-dependent crime and cyber-enabled offences. Cyber-dependent crimes (sometimes called "pure" cybercrime) are those offences that can only be committed using communication and information technologies. They are crimes that are directed against computers and networks and include such illicit activities as hacking, spreading malware or ransomware and causing distributed denial of service attacks.[2] Cyber-enabled offences are continuations or varieties of existing types of offences, committed using digital technologies, such as online fraud, cyberstalking or harassment. The risk of not recognising the difference between pure cybercrime and cyber-enabled crime is that there is the potential to miss how cyber-enabled crime fits into existing patterns of offending. We should avoid fetishising the technology and instead focus on the most prevalent forms of cybercrime, and the perpetrators responsible for it. It is important to recognise when the internet is a "new medium for

* Monique Cormier is a Senior Lecturer in the School of Law at the University of New England, Armidale, New South Wales; and Simon McKenzie is a Research Fellow in the School of Law at the University of Queensland, Brisbane, Queensland. The authors would like to thank Robert Brown and Isabelle Peart for their excellent research assistance during the preparation of this chapter

1 Australian Cyber Security Centre, "ReportCyber" <cyber.gov.au/acsc/report>.

2 C Teunissen, I Voce and R Smith, "Estimating the Cost of Pure Cybercrime to Australian Individuals" (Statistical Bulletin No 34, Australian Institute of Criminology, 2021).

'old' practices; and where in other cases it facilitates actions that would not be perpetrated 'offline' ".[3]

First, a note of caution: any categorisation and assessment of the legal responses to cybercrime should account for the reality of how cyberspace forms part of everyday life.[4] Most people in the developed world have ongoing internet access through their phones, their computers, as well as through their televisions, tablets, even sometimes fridges and vehicles. In addition to revolutionising work, business and commerce, people carry out their most intimate and important personal tasks through the internet. Relationships are formed, sustained and ended via digital means; if a person is sick, a common first step is to search the internet for explanations or book a doctor's appointment online; banking and shopping online is now routine. Our online and offline lives are thoroughly and – at least for some of us – irretrievably intertwined. We are not disembodied in digital spaces "because digital life is in fact lived through our bodies in the way we use and engage with technology".[5]

This means that while it is useful to differentiate between cyber-dependent and cyber-enabled crimes, it is also important to recognise that the boundaries between online and offline spaces is blurred. We should be attentive to the fact that thinking of cyberspace as a separate, alternative, disembodied space does not accurately reflect digital technologies which are "very real, very material, and very grounded geographies".[6]

With such caveats in mind, this chapter explores legal responses to cybercrime using two distinctly different types of cyber offending to demonstrate the diversity under the umbrella concept of cybercrime. It focuses on the cyber-dependent crime of deploying ransomware and the suite of cyber-enabled crimes that facilitate family violence and digital coercive control. Ransomware and family violence are in many ways opposite ends of the spectrum of cyber offending, but they provide diverse examples to demonstrate how digital technologies are facilitating, transforming and escalating the commission of criminal offences. They also provide examples of the various challenges that cybercrime presents for law and law enforcement, and demonstrate why a one-size-fits-all response to different types of cyber offending is problematic.

3 B A Harris and D Woodlock, "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies" (2019) 59(3) *British Journal of Criminology* 530, 532.

4 A Powell and N Henry, *Sexual Violence in a Digital Age* (Palgrave Macmillan UK, 2017) 52.

5 Powell and Henry, n 4, 60.

6 M Graham, "Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?" (2013) 179(2) *Geographical Journal* 177, 181.

This chapter begins with an overview of how cyber-dependent crime is conceptualised, in broad terms, before turning to the specific example of ransomware attacks. Ransomware has wide-ranging scope and the potential for devastating real-world impact. It is categorised as a cyber-dependent crime because it is, at its core, an attack on a computer system or network, but it can have significant consequences for individuals, business and industry, public infrastructure and national security. In this first part, the chapter provides a snapshot of both the international and Australian legal frameworks that deal with cyber-dependent crime and examines how and why the problem of ransomware has proven to be almost immune to legal responses.

The chapter then turns to the example of cyber-enabled crime, exploring how the internet has provided a new means for committing old crimes of family violence. Focusing on the example of family violence, it demonstrates how perpetrators use digital technologies in a variety of ways – some crude, some creative – to perpetuate ongoing abuse and control against their family members. This second part reviews Australian legal responses to cyber-enabled family violence (including conduct such as image-based sexual abuse and online harassment) and emphasises the importance of recognising the real harm caused by such conduct.

This chapter concludes by identifying common shortcomings of the legal responses to both cyber-dependent and cyber-enabled crime. It also considers some of the current policy responses to cybercrime and suggests that a more holistic approach is needed.

Cyber-Dependent Crimes

[5.20] "Computer crimes", "pure cybercrimes" or "cyber-dependent crimes" are various labels for the type of cybercrime that targets computers or networks. It includes computer access crimes and computer disruption crimes.[7] Access crimes include those in which a perpetrator unlawfully accesses (hacks) a computer or network for the purposes of removing, acquiring or otherwise using information or data that they have no right to access. Disruption crimes are those which prevent the computer or network from functioning properly. Common disruption crimes include distributed denial of service attacks, circulation of computer viruses and deployment of ransomware. This section explores international and domestic legal responses to cyber-dependent crime, using ransomware as the primary example. It demonstrates how the ever-increasing volume of cyber-dependant crime and the transborder nature of

7 Teunissen, Voce and Smith, n 2, 2–3.

such activities provide particular challenges for criminal prosecution of this type of cybercrime.

What is ransomware?

[5.30] Ransomware is a type of malware that works by encrypting files on a user's machine as well as files on any connected devices. It displays an image on the screen with instructions for the user to pay a ransom to have their files decrypted. If the user does not pay by a certain time, their files are usually destroyed or their systems remain otherwise inaccessible.[8] Thanks to the proliferation of what is called "ransomware-as-a-service", someone wanting to perpetrate a ransomware attack does not have to possess any particular technical skills. Ransomware specialists offer their code and expertise to novice hackers for either a nominal fee or a cut of the ransom, meaning that ransomware-as-a-service is quite readily available and easily accessible.[9]

Ransomware is deployed by a range of actors: individuals, organised criminal groups, loosely affiliated criminal networks and states.[10] There is also a long and growing list of victims of ransomware attacks, including individuals, small businesses, large corporations, hospitals, banks, utilities, schools and government departments. Ransomware is now a multi-billion-dollar industry, with estimates that by 2020 it had cost the global economy more than US$1 trillion.[11] The use of ransomware has grown to become one of the top global cybercrime concerns, fuelled no doubt by its ease of use and its success rate.

There are reportedly well over a thousand different variants of ransomware, most are deployed indiscriminately and some can spread rapidly by self-replicating. Others are highly targeted; flooding the internal systems inside a particular organisation and effectively grinding all operations to a halt until a bulk ransom is paid to decrypt all the systems of that organisation. Other strains of ransomware are clearly deployed for non-financial purposes, and maliciously delete data or release it even after the ransom is paid.[12]

8 M Harkins and A M Freed, "The Ransomware Assault on the Healthcare Sector" (2018) 6(2) *Journal of Law & Cyber Warfare* 148, 151.

9 Harkins and Freed, n 8, 152.

10 This chapter mostly focuses on the legal issues relating to cybercrimes committed by individuals or criminal groups. For legal analysis of cyberattacks attributable to states, see, for example, N Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 17 *Journal of Conflict and Security Law* 229.

11 "New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion", *McAfee* (7 December 2020) <mcafee.com/en-au/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629>.

12 Australian Cyber Security Centre, *Ransomware in Australia* (Report, 2 October 2020) 6.

While relatively small-scale ransomware incidents continue to plague individuals and small businesses or organisations, cybersecurity experts are concerned that ransomware is increasingly being used to "hunt big game entities" which are those targets perceived as "high profile, high value, and/or those that provide critical services".[13] In May 2021, for example, there was a significant ransomware attack on critical infrastructure in the United States, when cybercriminals targeted Colonial Pipeline, operator of the US's largest fuel pipeline system. Colonial Pipeline was forced to shut down the fuel delivery system which caused petrol shortages to the east coast for several days. It led to panic buying and gasoline price surges and had flow on effects for the transport and aviation industries. The company reportedly paid US$4.4 million dollars in ransom to resume normal operations,[14] and it has since been labelled "the largest attack on the US energy system in history".[15]

The ability of ransomware to disrupt critical infrastructure and essential services makes it significantly more dangerous than "ordinary" crimes relating to blackmail or extortion. The added component of cyber enables criminals to increase the stakes of the threat, which in turn increases the odds that the ransom will be paid. The fact that so many public and private services rely on networked systems to function mean that they are vulnerable to hacking and malware, and a prime target for ransomware. The nature of cybercrime also allows for criminal activity to be coordinated across national borders and have increasingly wide-reaching and transnational effects.

One of the most infamous global ransomware incidents to date was the 2017 Wannacry ransomware attack. Wannacry was a self-replicating ransomware cryptoworm that spread rapidly and indiscriminately, eventually infecting at least 200,000 computers in over 150 countries.[16] Of particular concern was the fact that Wannacry infected parts of the National Health Service (NHS) network in the United Kingdom, locking patient databases and shutting down medical equipment. The NHS estimated nearly 20,000 patient appointments

13 Australian Cyber Security Centre, *ACSC Annual Cyber Threat Report 2020–21* (Report, 15 September 2021) 31 (*ACSC Annual Cyber Threat Report 2020–21*); K Keneally and T Watts, *Beyond the Blame Game* (Policy Paper, February 2021) <timwatts.net.au/media/187357/beyond-the-blame-game-ransomware-discussion-paper.pdf>.

14 *ACSC Annual Cyber Threat Report 2020–21*, n 13, 33.

15 J Bardoff, "The Colonial Pipeline Crisis Is a Taste of Things to Come", *Foreign Policy* (17 May 2021) <foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/>.

16 L J Trautman and P C Ormerod, "Wannacry, Ransomware, and the Emerging Threat to Corporations" (2019) 86(2) *Tennessee Law Review* 503, 505.

including surgeries were cancelled, ambulances had to be diverted and 1,200 pieces of diagnostic equipment were infected.[17] There were no reported cases of physical harm to patients caused by this disruption, but one can imagine how this could quite easily have contributed to patients' deaths or exacerbation of medical conditions. While the NHS might have been the most high profile victim of Wannacry, there were many, many others including companies in Japan, universities in Canada, ministries in Russia, police departments in India and individuals all over the world.[18] In 2021, it is still considered "the most notorious ransomware attack of all time".[19]

In Australia, ransomware is a growing cybersecurity concern, with the Australian Cyber Security Centre labelling ransomware as "one of the most significant threats" facing the Australian cybersecurity landscape.[20] Millions of dollars are reportedly being paid in ransom by Australian organisations,[21] and cybercriminals are now ramping up their hunt of big game in Australia. In March 2021, for example, Eastern Health, one of Melbourne's public health services which runs several hospitals, was the victim of a ransomware attack which caused the postponement of elective surgeries and prevented staff from accessing patient medical histories for weeks.[22] While ransomware incidents remain a relatively small proportion of cybercrime in Australia, ransomware is considered the most serious type of cybercrime "due to its high financial impact and disruptive impacts to victims and the wider community".[23]

The escalating threat presented by cyber-dependent crime more broadly, and ransomware specifically, has arguably reached a tipping point. Ciaran Martin,

17 O Hughes, "WannaCry Impact on NHS Considerably Larger than Previously Suggested", *Digital Health* (27 October 2017) <digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/>.

18 Trautman and Ormerod, n 16.

19 P Haskell-Dowland and A Woodward, "Is Australia a Sitting Duck for Ransomware Attacks? Yes, and the Danger Has Been Growing for 30 Years", *The Conversation* (13 July 2021) <theconversation.com/is-australia-a-sitting-duck-for-ransomware-attacks-yes-and-the-danger-has-been-growing-for-30-years-161818>.

20 *ACSC Annual Cyber Threat Report 2020–21*, n 13, 9.

21 J Purtill, "Australian Organisations Are Quietly Paying Hackers Millions in a 'Tsunami of Cyber Crime' ", *ABC News* (16 July 2021) <abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542>.

22 M Cunningham, "Staff Unable to Access Patient Files after Eastern Health Cyber Attack", *The Age* (29 March 2021) <theage.com.au/national/victoria/staff-unable-to-access-patient-files-after-eastern-health-cyber-attack-20210329-p57eyj.html>.

23 *ACSC Annual Cyber Threat Report 2020–21*, n 13, 16.

the former director of the UK's National Cyber Security Centre articulated the urgency of this matter:

> It's time to do something because we're getting cleaned out left, right and centre. Services are being disrupted and millions of pounds are being lost … We need to do something to catapult ransomware up the priority ladder for cybersecurity agencies, governments and industry people who care about cybersecurity.[24]

With such high global stakes, there is a concerted push for both a coordinated international and targeted domestic response. The next section evaluates both the international and Australian legal responses to cyber-dependent crime.

Legal responses to cyber-dependent crime

[5.40] At present, the most pressing challenges created by ransomware are seen to be technological: how to protect against such attacks, how to minimise damage when they occur, how to identify who is behind them. But legal responses are also needed and given the unprecedented transborder effects of ransomware, it needs to involve both international and domestic actors. This section first provides an overview of the current international legal framework for addressing cybercrime, before demonstrating that Australia's criminal laws are *prima facie* sufficient to deal with cyber-dependent offences such as ransomware attacks.

The international legal response to cyber-dependent crime

[5.50] It goes without saying that the internet and digital technologies have created an unprecedented level of transnational connectivity. This shrinking of geographical distance and the borderless nature of cyberspace has fostered innovation in commerce, science and education. It has also become a playground for enterprising criminals, with the territorial reach of criminal activity only being limited by the extent of internet connectivity, necessitating an international approach to combat cybercrime. While there is no global cybercrime treaty at present, there are several regional cybercrime instruments, the most comprehensive of which is the Council of Europe Convention on Cybercrime, also known as the *Budapest Convention*.[25]

Although regional in origin, the *Budapest Convention* is open to all states and is the closest thing the world has to a comprehensive international

24 M Gooding, "Pay Ransom, Face Sanctions? US Treasury Warning Divides Industry", *Tech Monitor* (15 October 2020) <techmonitor.ai/cybersecurity/ransomware-sanctions-treasury>.

25 *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004).

cybercrime treaty. In recognising "the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks", the aim of the *Convention* is to pursue "a common criminal policy aimed at the protection of society against cybercrime".[26] To that end it requires parties to criminalise certain cybercrime activities, and it sets out a relatively comprehensive framework on cyber investigations, international cooperation and jurisdiction – including an obligation on parties to extradite or punish alleged offenders found on their territory.

The *Budapest Convention* has several shortcomings, however, including the fact that, at the time of writing, it only has 66 states parties and only 21 of those are from outside Europe. Australia ratified the *Budapest Convention* in 2015, but is one of only four countries in the Asia-Pacific region to have done so.[27] The *Convention* does not provide a model law, and gives states significant leeway in how they implement the legal framework. The *Convention* also gives states the right to require that the proscribed conduct must result in serious harm and leaves it to states to determine what constitutes "serious harm".[28] The *Convention* recommends that states criminalise the following:

- illegal access to any part of a computer system;
- illegal interception of private transmission of computer data;
- interference with computer data or a computer system;
- misuse of devices;
- computer-related forgery and fraud;
- use of a computer system in relation to child pornography; and
- copyright infringement.[29]

None of these provisions explicitly mention ransomware or cyber extortion of any kind. It is conceivable that an offence of illegal access to a computer system and a prohibition on data interference (which includes the suppression of computer data) would be applicable. But it does not address the "ransom" aspect of ransomware attacks, nor does it acknowledge the potentially debilitating indirect effects that suppressing data can have. The fact that the *Convention*'s

26 *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004), Preamble.

27 The only other parties in the Asia-Pacific region are Japan, Tonga and the Philippines.

28 *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004), Art 4(2).

29 *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004), Arts 2–10.

substantive law is underinclusive and not sufficiently particularised, and the fact that it only has 66 states parties has led some commentators to argue for an entirely new cybercrime convention developed by international consensus.[30] But developing new multilateral treaties can take decades, which is time the world does not have when facing rapid, widespread and increasingly destructive cybercriminal activity. The *Budapest Convention* provides a good starting point for developing a more comprehensive transnational cybercrime framework. What it does need, however, is a model law, and there may already be a solution to this issue.

The International Telecommunication Union's (ITU) Toolkit for Cybercrime Legislation is essentially a ready blueprint for such a model law. Developed in consultation with technical experts, various industry and government representatives, and the American Bar Association, the toolkit was produced with the aim of helping "to advance a harmonized global legal framework, facilitate international cooperation, resolve jurisdictional and evidentiary issues and deter cyber-criminal behaviour".[31] It provides what it calls "sample language" for a raft of cyber offences including multiple provisions that would apply to ransomware. To give a few examples, there are provisions that makes it an offence to use computers to extort money;[32] that makes it a crime to interfere with or impair medical care,[33] another one that deals with unauthorised access to critical infrastructure.[34] Most specify the mental element of intention, but for some it is sufficient that the perpetrator has "knowledge that such conduct could cause" the particular harm, which is akin to the mental element of recklessness.[35] This would cover ransomware

30 See, for example, J Hakmeh, "Building a Stronger International Legal Framework on Cybercrime", *Chatham House* (6 July 2017) <chathamhouse.org/2017/06/building-stronger-international-legal-framework-cybercrime>. In December 2019, the UN General Assembly adopted a resolution in which it decided "to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes". This represents a first step towards a possible global cybercrime treaty: *Countering the Use of Information and Communications Technologies for Criminal Purposes*, GA Res 74/247, UN GAOR, UN Doc A/RES/74/247 (20 January 2020, adopted 27 December 2019).

31 International Telecommunications Union, "Toolkit for Cybercrime Legislation" (Report, February 2010) 8 <https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf>.

32 International Telecommunications Union, n 31, s 9.

33 International Telecommunications Union, n 31, s 6(f).

34 International Telecommunications Union, n 31, ss 2(c), 3(d).

35 For example, s 4(c), (d) and (e).

deployed indiscriminately; hackers could not claim that they did not intend for their ransomware to hit any particular target. It would also cover situations like the Colonial Pipeline attack in which the group responsible claimed that it did not mean to "[create] problems for society" its only goal was "to make money".[36] There are also provisions in the ITU Toolkit that make it an offence to "produce, sell or procure" a computer program intended primarily for committing various cyber offences,[37] which would apply to those providing ransomware-as-a-service. In addition, there are a comprehensive range of procedural provisions that deal with issues of jurisdiction, expedited mutual assistance and due process.

Without a model law, the *Budapest Convention*'s *laissez-faire* approach to defining cybercriminal acts reflects the variable state of domestic laws. A 2013 survey of cybercrime legislation conducted by the UN Office on Drugs and Crime found that laws relating to illegal access to computer systems differed widely with respect to both the physical and fault elements of the offences. Some specify that illegal access must be for a particular objective – for example, to damage, delete, alter, suppress or transfer data. Some laws criminalise mere access to a computer system, others require criminal intent to cause a particular harm.[38]

As the next section demonstrates, however, a comprehensive domestic legal framework on cyber-dependent crime is never going to be sufficient in and of itself to ensure that such offending is prosecuted. The complexity of criminal investigation and difficulty of transnational enforcement require a multifaceted response to the challenge of cyber-dependent crime.

The Australian legal response to cyber-dependent crime

[5.60] Criminal law in Australia is largely a matter for the states and territories, but there is also a separate Australia-wide Commonwealth criminal jurisdiction. This means that there are nine different criminal law regimes in Australia, any of which may be applicable to cybercrime with or without some kind of jurisdictional connection to the offence.[39] This section provides a brief overview of the types of criminal offences codified in various Australian

36 M A Russon, "US Fuel Pipeline Hackers 'Didn't Mean to Create Problems' ", *BBC News* (10 May 2021) <bbc.com/news/business-57050690>.

37 International Telecommunications Union, n 31, s 6(b).

38 United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (Draft Report, February 2013) Ch 4.

39 The relevant legislation will usually specify jurisdiction. In the *Criminal Code Act 1983* (NT), for example, computer offences in Pt VII Div 10 require there to be a territorial nexus to the Northern Territory (s 276F). See Chapter 3 on "Jurisdiction".

jurisdictions that may be appropriate for prosecuting cyber-dependent crimes, including ransomware. It then turns to discuss the considerable challenges for enforcing such laws.

As Australia is a party to the *Budapest Convention*, its suite of dedicated Commonwealth cyber offences complies with the broad requirements of that treaty. Part 10.7 of the *Commonwealth Criminal Code* criminalises certain "computer offences" including:

- unauthorised access to, or modification of, data held in a computer;[40]
- unauthorised impairment of electronic communication;[41] and
- possession or control of data, or producing, supplying, or obtaining data, with intent to commit a computer offence.[42]

Under such offences the computer itself, and/or the data it contains, is the target of the criminal activity. These laws are designed for archetypal cyber-dependent activity such as hacking and data breaches and would be appropriate for prosecuting use of ransomware. Under s 477.1, for instance, it is an offence to cause unauthorised access to data held in a computer with intent to commit a serious Commonwealth, State or Territory offence. A serious offence is one punishable by imprisonment for five or more years.[43] This provision, used in conjunction with a state or territory offence of extortion or blackmail, would allow for the prosecution of someone using ransomware by Commonwealth prosecuting authorities. For example, s 249K of the *Crimes Act 1900* (NSW) criminalises blackmail, requiring an accused person to have made "any unwarranted demand with menaces"[44] and with the intention of "obtaining a gain or of causing a loss".[45] Section 415 of the *Criminal Code Act 1899* (Qld) provides that a person commits the crime of extortion if he or she makes a demand without reasonable cause, with the intent "to gain a benefit for any person" or "cause a detriment to any person" with a threat to cause a detriment.[46] The use of ransomware to extort payment in exchange for release

40 *Criminal Code Act 1995* (Cth), Sch 1 ss 477.1–477.2.

41 *Criminal Code Act 1995* (Cth), Sch 1 s 477.3.

42 *Criminal Code Act 1995* (Cth), Sch 1 ss 478.3–478.4.

43 *Criminal Code Act 1995* (Cth), Sch 1 s 477.1(9).

44 "Menaces" is defined as "an express or implied threat of any action detrimental or unpleasant to another person": *Crimes Act 1900* (NSW), s 249M.

45 Maximum penalty is 10 years: *Crimes Act 1900* (NSW), s 249K.

46 Maximum penalty is 14 years: *Criminal Code Act 1899* (Qld), s 415; the *Criminal Code Act 1899* (Qld) also provides that the maximum penalty may be increased to life imprisonment if the extortion threat is likely to cause serious personal injury to someone, or likely to cause

of data or to regain control of a computer system, would invariably satisfy the elements of such serious offences.

Each Australian state and territory also has its own suite of codified computer offences that largely mirror those in the *Commonwealth Criminal Code*. This means that there are also laws at the state and territory level which criminalise such cyber-dependent activities as unauthorised access to, modification of, or impairment to computer function or data.[47] In some jurisdictions, such activities are penalised if they are committed with the intent to commit a serious (non-cyber) offence.

There are also state or territory-specific computer offences without direct equivalents in the other Australian jurisdictions. For instance, the *Queensland Criminal Code* provides a variable penalty regime for "computer hacking and misuse" depending on the value of damage caused or benefit gained. A person who accesses a computer or network without consent, and who "causes or intends to cause detriment or damage, or gains or intends to gain a benefit" is liable to imprisonment for five years. The penalty increases to 10 years imprisonment if the unauthorised access or use of the computer system causes damage or provides a benefit to the accused to the value of more than $5,000.[48] Such a provision would be directly applicable to use of ransomware. The *Criminal Law Consolidation Act 1935* (SA) criminalises the possession, production, supply or obtaining of computer viruses where there is intent "of committing or facilitating the commission (either by that person or someone else) of, a serious computer offence".[49] This provision would apply to persons creating and selling ransomware-as-service as well as anyone purchasing or possessing the ransomware virus with the intent to use it.

The above snapshot of the Australian legal framework demonstrates that it contains a range of offences designed broadly for cyber-dependent crime, some of which may be used in conjunction with "serious offences" of the non-cyber-variety, such as blackmail or extortion. A person accused of committing a cyber-dependent crime would likely face multiple different charges under the relevant Australian legal regime given the complexity of cyber offending. Under the *Crimes Act 1900* (NSW), for instance, someone accused of deploying ransomware could conceivably face, *inter alia*, the following charges:

"substantial economic loss in an industrial or commercial activity". It is conceivable that such high sentences could be imposed in relation to a conviction for using ransomware.

47 See, for example, *Crimes Act 1900* (NSW), s 308C; *Criminal Code Act 1983* (NT), ss 276B–276C; *Criminal Law Consolidation Act 1935* (SA), s 86E; *Crimes Act 1958* (Vic), s 247B.

48 *Criminal Code Act 1899* (Qld), s 408E(2)–(3).

49 *Criminal Law Consolidation Act 1935* (SA), s 86I.

- unauthorised access, modification or impairment with intent to commit a serious indictable offence;[50]
- unauthorised modification of data with intent to cause impairment;[51]
- unauthorised impairment of electronic communication;[52]
- possession of data[53] with intent to commit a serious computer offence;[54]
- producing, supplying or obtaining data with intent to commit a serious computer offence;[55] and
- blackmail.[56]

The Australian legal framework applicable to cyber-dependent crimes therefore appears to be relatively comprehensive and fit-for-purpose. Why, then, is cyber-dependent crime so notoriously difficult to prosecute? The next section addresses some of the challenges to criminal prosecution of cyber-dependent crime in Australia and elsewhere.

Challenges to prosecuting cyber-dependent crime

[5.70] A recent assessment by the Australian Labor Party concluded that "[r]ansomware is largely a crime of impunity in Australia today".[57] Despite the existence of appropriate criminal offences to cover a range of cyber-dependent criminal activities, cybercriminals are able to target Australian individuals, businesses and other entities with few consequences.

One of the concerns in relation to cyber-dependent crime, and the rise of ransomware, is that it is now so widespread as to present an almost insurmountable challenge for traditional law enforcement. Individuals and entities targeted by ransomware are frequently now paying the ransom as the most expedient and cost-effective way to regain access to their data or systems.[58] This is not helped by the burgeoning cyber insurance market

50 *Crimes Act 1900* (NSW), s 308C.

51 *Crimes Act 1900* (NSW), s 308D.

52 *Crimes Act 1900* (NSW), s 308E.

53 "Data" is defined in s 308 as "information in any form" or "any program (or part of a program)" which would likely include a ransomware program: *Crimes Act 1900* (NSW), s 308.

54 *Crimes Act 1900* (NSW), s 308F.

55 *Crimes Act 1900* (NSW), s 308G.

56 *Crimes Act 1900* (NSW), s 249K.

57 Keneally and Watts, n 13, 8.

58 Purtill, n 21.

which encourages businesses targeted by ransomware to pay the ransom.[59] Cyber security experts and policy makers warn against paying any ransom to cybercriminals on the grounds that there are no guarantees that those behind the threat will not destroy data or permanently impair systems once paid.[60] Furthermore, payment of ransoms has only emboldened cybercriminals to increase the frequency of attacks, raise the amount of ransom and pursue big game targets.[61] The success of ransomware attacks has also contributed to the proliferation of ransomware as a "weapon of choice" for other cybercriminals.

In addition to the considerable volume of cybercrime, there is the added law enforcement challenge of being able to identify perpetrators who go to great lengths to hide their identities and cover their tracks online. It takes specialist technical skills and computer forensics resources to determine who is behind cybercriminal activity. Such resources are usually well beyond the budget and capabilities of local police and prosecuting authorities.[62] Furthermore, it can be hard to convince local law enforcement that it is an important enough issue to investigate and prosecute, and those tasked with carrying out investigations and prosecutions are often ill-equipped to handle the technical complexity.[63]

Even when a cybercriminal can be identified and located, the principal challenge to law enforcement of cyber-dependent crime is jurisdiction. Enforcement of criminal law, including prosecution and punishment, is the territorial prerogative of sovereign states.[64] Where the perpetrators of cybercrime are located overseas, it is almost impossible to investigate and prosecute such crimes without international coordination and cooperation. The prospects for law enforcement in relation to cyber-dependent crimes is

59 J Lemnitzer, "Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help", *The Conversation* (17 February 2021) <theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254>.

60 Australian Cyber Security Centre, n 12.

61 Keneally and Watts, n 13, 14–15.

62 A Peters and A Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime" (2019–2020) 10(3) *Journal of National Security Law and Policy* 487, 514.

63 Peters and Jordan, n 62; A Leppänen and T Kankaanranta, "Cybercrime Investigation in Finland" (2017) 18(2) *Journal of Scandinavian Studies in Criminology and Crime Prevention* 157, 170–172; Commonwealth of Australia, Comment to Intergovernmental Expert Group on Cybercrime, *Seventh Session of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime* (22 March 2021) <unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Comments/7th_IEG_Cyber_-_MS_comments.pdf>.

64 See Chapter 3 on "Jurisdiction".

therefore going to be contingent on increased international cooperation among domestic investigating and prosecuting agencies alongside the establishment of well-resourced multinational cybercrime task forces.[65]

An example of such a task force is the European Union's Joint Cybercrime Action Taskforce (J-CAT) which was established in 2014. J-CAT's purpose is "to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by its partners".[66] One of J-CAT's recent successes against ransomware was a coordinated campaign to take down a virtual private network (VPN) service, thereby disrupting "a safe haven" used by ransomware groups to hide their identities and locations.[67]

Yet actual criminal prosecutions for cybercrime remain rare, even where there is well-resourced cross-border cooperation and no jurisdictional issues. Gathering admissible digital evidence that sufficiently links an identified perpetrator to the criminal act is a complex task and does not guarantee a successful prosecution.[68] Another contributing factor to impunity for cyber-dependent criminals is underreporting by individuals and businesses. Reasons for not reporting cybercrime can include embarrassment of becoming a victim; uncertainty about how and where to report cyber incidents, a belief that police cannot do anything; and businesses making the decision to simply deal with the fall out of a cyberattack internally to minimise loss of time and money.[69] At present, however, the main impediments to successful legal responses to cyber-dependent crime are jurisdictional hurdles and the sheer volume of incidents that make it impossible for police to mount time-consuming and resource-intensive cross-border investigations.

65 F Hanson, "Time to Admit We're Failing on Cybercrime", *ASPI Strategist* (16 February 2018) <aspistrategist.org.au/time-admit-failing-cybercrime>; see also Commonwealth of Australia, n 63.

66 Europol, "Joint Cybercrime Action Taskforce" <europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>.

67 Europol, "Coordinated Action Cuts Off Access to VPN Service Used by Ransomware Groups" (Press Release, 30 June 2021) <europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups>.

68 Peters and Jordan, n 62, 515.

69 Federal Bureau of Investigation, "Ransomware Victims Urged to Report Infections to Federal Law Enforcement" (Public Service Announcement, I-091516-PSA, 15 September 2016) <ic3.gov/Media/Y2016/PSA160915>.

The rest of this chapter turns to consider how law deals with cyber-*enabled* offending, before offering some concluding remarks in [5.160] on current and future policy responses to cybercrime.

Cyber-Enabled Crimes

[5.80] It should come as no surprise that the internet is used as a tool by offenders who are not typically considered "cybercriminals" in the same way as those perpetrating cyber-dependent crimes. In such cases, the crimes are *enabled* by digital technologies, but are not unique to them. Crimes related to interpersonal violence – including sexual harassment and family violence – are useful examples of this sort of dynamic: perpetrators can use phones, home computers and even smart devices as part of their violence. In trying to understand these kinds of cybercrime, we should recognise the "increasingly embedded and intertwined nature of the physical, digital, and biological", particularly when it involves family violence.[70] In these cases, it is important to treat the use of technology and the internet as fitting within the broader pattern of violence or abuse.

There is no question that the use of the internet to perpetuate interpersonal violence poses some unique challenges: Todhunter notes that online violence deviates from prototypical forms of violence as it is not necessarily a "discrete act of violence against an identifiable target".[71] It can occur across jurisdictions, impact a wide range of victims, involve a range of complex harms and be carried out by people "who would not otherwise be disposed to violence, and who may not even consider their conduct as violence".[72] Despite these differences between online and offline violence, we should treat the conduct as part of a broader pattern of interpersonal and family violence.[73]

There is often resistance to new laws prohibiting online abusive behaviour for both reasons of freedom of speech, and also because there is a failure to appreciate the harm caused by this behaviour; harm which is "often trivialised and minimised in the policies and practices of police, media, the legal profession and other responders to the problem".[74] Assessing the conduct through a wider

70 N Henry, A Flynn and A Powell, "Technology-Facilitated Domestic and Sexual Violence: A Review" (2020) 26(15–16) *Violence Against Women* 1828, 1830.

71 O Todhunter, "Logged In and Fed Up: Responding to Gendered Violence in Online Spaces" (2018) 22(4) *Media and Arts Law Review* 420, 422.

72 Todhunter, n 71.

73 Harris and Woodlock, n 3, 532–533.

74 Powell and Henry, n 4, 218.

lens suggests that this failure to appreciate the harm caused by online violence reflects how "offline" forms of harassment are also "trivialised, regarded as part of normal, flirtatious exchanges between men and women in public and private life".[75] Both the online conduct and the broader "offline" pattern it fits within need to be addressed for any legal response to be effective.

This section first considers how abusers use technology to perpetrate family violence[76] online. It provides an overview of the prevalence of such offending before underscoring the fact that the harm caused by online violence is real. Focusing on the technological means of offending risks underestimating the significant impact that it has on the lives of its victims. This section then uses the examples of image-based sexual abuse and online harassment to assess legal responses to cyber-enabled family violence in Australia.

Cyber-enabled family violence

[5.90] How is family violence enabled by digital technology? Perpetrators of family violence use digital technology to achieve the same ends they also seek through other forms of abuse: to control and coerce their intimate partner. This can occur through a variety of methods. The Australian Domestic Violence Bench Book explains that all sorts of technologies – computers, smart phones, GPS navigators, digital cameras and digital recording equipment – are used to stalk and surveil the target victim.[77] These tools are "recognised as easy, accessible and instantaneous methods by which a perpetrator can control, monitor, humiliate and shame the victim, and make it more difficult for the victim to leave the abuse relationship or seek help".[78] The sad reality is that technology has provided abusers with

75 Powell and Henry, n 4.

76 "Family violence" is a broad term used to describe a range of abusive behaviours that "may occur within intimate, immediate and extended family and other communal or extended kinship relationships of mutual obligation and support". Violence includes "physical, sexual, emotional and psychological abuse or injury, as well as conduct designed to exert power by restricting access to financial, familial and cultural resources and limiting social autonomy, sometimes referred to as coercive control": "Terminology" in Australian Institute of Judicial Administration, *National Domestic and Family Violence Bench Book* (6 October 2021) ¶3 <dfvbenchbook.aija.org.au/contents> (*National Domestic and Family Violence Bench Book*).

77 "Following, harassing and monitoring" in *National Domestic and Family Violence Bench Book*, n 76, ¶3.1.6.

78 *National Domestic and Family Violence Bench Book*, n 76.

"new and more extensive ways to control, coerce, stalk, and harass their victims".[79]

These technological developments have "compounded the severity and complexity of domestic abuse".[80] Similar to cybercriminals who use ransomware to extort companies, perpetrators of family violence do not need to have a great deal of technical expertise to carry out their offending. It often only requires a few keystrokes for perpetrators to be able "harass both their current and former intimate partners without leaving the comfort of their home, instigating fear in an attempt to maintain control".[81]

While some forms of technology-facilitated violence are lo-fi and based on persistent texts, emails or phone calls, others are more sophisticated. To give one of the most troubling examples, spyware and "internet-of-things" devices are increasingly being used by perpetrators.[82] If they can get access to the victim's computers and phones, spyware can be easily purchased and installed without their knowledge.[83] It can allow perpetrators to track the physical location of devices, see every incoming and outgoing message, every web search, listen to live phone calls and turn devices into remote listening devices.[84] The information that is gathered from this activity can be used to "remind victims of their dominion and strength; to remind them that despite their physical absence, their abuser remains in control".[85]

The prevalence of cyber-enabled family violence

[5.100] It is hard to say how often internet tools are used to perpetuate family violence. Research into cyberstalking and other kinds of technology-facilitated family violence is scarce; Essert suggests this might be because it is easier to avoid detection online, and that this sort of conduct is underreported.[86] Much of the research is based on surveys, and the majority of the quantitative

79 H Al-Alosi, "Cyber-Violence: Digital Abuse in the Context of Domestic Violence" (2017) 40(4) *University of New South Wales Law Journal* 1573, 1578.

80 C Essert, "Addressing Imperfect Solutions to Technology-Facilitated Domestic Violence" (2019) 41(3–4) *Women's Rights Law Reporter* 117, 124.

81 Essert, n 80.

82 Essert, n 80, 132–134.

83 Essert, n 80, 133.

84 Essert, n 80.

85 Essert, n 80, 133.

86 Essert, n 80, 125.

research in the field has been on "sexting" among children and adolescents.[87] There has been far less research into non-consensual behaviours related to the use of images between adults, despite the fact there is some research indicating that it is more prevalent.[88]

However, a few things are quite clear. Technology-facilitated abuse repeats the patterns of other forms of family violence. Men are the vast majority of perpetrators.[89] In fact (and unsurprisingly), digital technologies are a very common part of the toolkit of perpetrators of family violence: a 2020 Australian survey with frontline domestic violence workers found that almost all survey respondents (99.3%) had clients who had experienced technology-facilitated stalking and abuse.[90] The most commonly used tool was text messaging, with 60.7% of practitioners seeing it "all the time"; smartphones (36.1%) and Facebook (35.1%) were the next two most commonly used technologies.[91] The use of cameras to covertly or overtly monitor women and children had increased by 182% since the last survey (35% of respondents said they saw them used to perpetrate abuse "all the time"), and GPS tracking was also a common part (16%). This is not a new feature of family violence. Research has consistently demonstrated that technology-facilitating family violence is relatively prevalent. A 2013 study found that 97% family violence practitioners supported clients whose partners or ex-partners were using mobile technology to track them.[92] The same study found that 78% of victims had been abused or harassed through technology, and 44% said they had been threatened over text, email or social media.[93]

This has also been found in other jurisdictions. A 2016 US survey of people over 15 years of age found that 12% of respondents who had been in a romantic relationship had experienced digital abuse by their current or former

87 N Henry, A Flynn and A Powell, "Image-Based Sexual Abuse: Victims and Perpetrators" (Trends & Issues in Crime and Criminal Justice No 572, Australian Institute of Criminology, March 2019) 3, 19.

88 Henry, Flynn and Powell, n 87.

89 Al-Alosi, n 79, 1574.

90 D Woodlock et al, *Second National Survey on Technology Abuse and Domestic Violence* (Report, November 2020) 2.

91 Woodlock et al, n 90.

92 D Woodlock, *Technology-Facilitated Stalking: Findings and Recommendations from the SmartSafe Project* (Domestic Violence Resource Centre Victoria, 2013) 15.

93 Woodlock, n 92, 24.

intimate partner.[94] The forms of abuse the survey asked about included "being monitored online or by phone, being purposefully embarrassed online, being called offensive names, and being stalked".[95] It was more prevalent among young people and LGBTQI+ people.[96] Interestingly, the survey reported that men and women experienced intimate partner digital abuse at equal rates.[97] The most common forms of digital abuse were digital monitoring and purposeful embarrassment online.[98] A more recent Australian study found a strikingly high rate of victimisation by image-based sexual abuse: 23% of respondents reported being a victim of at least one form of image-based sexual abuse, including the creation, distribution or threatened distribution of intimate images.[99] Overall, women and men reported similar levels of victimisation by image-based sexual abuse.[100]

The impact of cyber-enabled family violence

[5.110] Online violence can have a very tangible impact. It can affect a person's career and financial livelihood, cause serious psychological harm and fear.[101] It also has the effect of excluding users from online spaces, limiting their autonomy and access.[102] As Powell and Henry explain:

> … technology facilitated sexual violence is an extension of "everyday" forms of sexual violence and a further manifestation of gender inequality. [It] is a form of inequality that further prevents individuals and groups from participating *freely* in public and private life, resulting in a denial of "digital citizenship".[103]

As noted above, online harassment has often failed to be taken seriously, with investigators and prosecutors treating offline, physical violence as being much more problematic and the "real" kind violence conduct deserving of a

94 M Ybarra et al, *Intimate Partner Digital Abuse* (Report No 01.18.17, Data & Society Research Institute, January 2017) 3, 26 <https://datasociety.net/library/intimate-partner-digital-abuse/>.

95 Ybarra et al, n 94.

96 Ybarra et al, n 94.

97 Ybarra et al, n 94, 4.

98 Ybarra et al, n 94, 11.

99 Henry, Flynn and Powell, n 87, 9–10.

100 Henry, Flynn and Powell, n 87, 11.

101 Todhunter, n 71, 425–428.

102 Todhunter, n 71, 428.

103 Powell and Henry, n 4, 201.

response.[104] Testimony from victims of family violence suggests that they are forced to deal with perceptions that cyber-enabled violence is less serious and distinct from other forms of abuse and stalking.[105] This reflects how the dominant idea that the only kind of "real" violence is physical obscures the impact forms of non-physical violence.[106] This is view of "real" violence is erroneous. There is substantial evidence that cyber-enabled family violence causes real harm to its victims: by overcoming geographic and spatial boundaries, perpetrators are able to continue to contact victims, eroding their perception of safety by "creating a sense of omnipresence".[107] It makes it much more difficult to completely sever ties.[108] A 2020 Australian survey of domestic violence practitioners confirmed this view: the term "fear" was the most commonly used word to describe how technology-facilitated abuse impacted on victims.[109] The Survey Report explained that respondents reported it caused "exhaustion, despair and hopelessness" and that it "increased isolation, and a fear of using technology to keep in contact with friends, family and services".[110]

The difficulty of conceptualising and framing this kind of offending can be seen in the debate about what name to give this kind of offending. Henry, Flynn and Powell and use the phrase "technologically enabled abuse";[111] Douglas, Harris and Dragiewicz use "technology-facilitated domestic and family violence".[112] Harris and Woodlock argue that we should use the phrase "digital coercive control" as it describes the method, the intent and the impact of the conduct, and because the phrase "coercive control" "situates harm within a wider setting of sex-based inequality".[113] This way of describing abusive conduct against intimate partners conducted online is preferable to terms like "cyberbullying" or "cyberstalking". Focusing only on the technology used can miss how the offending fits into this wider pattern.

104 See Woodlock et al, n 90, 4.

105 Harris and Woodlock, n 3, 533–534.

106 Powell and Henry, n 4, 50.

107 D Woodluck, "The Abuse of Technology in Domestic Violence and Stalking" (2017) 23(5) *Violence Against Women* 584.

108 Al-Alosi, n 79, 1578.

109 Woodlock et al, n 90, 4.

110 Woodlock et al, n 90.

111 Henry et al, n 70.

112 H Douglas, B A Harris and M Dragiewicz, "Technology-Facilitated Domestic and Family Violence: Women's Experiences" (2019) 59(3) *British Journal of Criminology* 551.

113 Harris and Woodlock, n 3, 533.

This has been an issue with much extant literature on family violence conducted online. It focuses on the medium of abuse – the technology – rather than the actors carrying out the abuse and their relationship to one another, and the arena in which it occurs.[114] While it is possible that some people only experience abuse facilitated by the technology, other studies have "noted the co-occurrence of other forms of abuse and/or traditional stalking".[115] The focus on the medium has curtailed the kinds of conduct that have been studied. There has been much more written on online misogyny and violence associated with online dating than intimate partner and relational violence.[116] This has been observed by other scholars: Powell and Henry note that "studies of virtual or cybercriminality have paid surprisingly little attention to the dynamics of gender, power and inequality".[117] Similarly, Al-Alosi argues that while cybercrimes like "hacking, identity theft, and online fraud" have received considerable attention, "less focus has been given to the issue of technology-facilitated abuse between current and former intimate partners".[118] Instead, by paying proper attention to the nature of the harm rather than just the technology we can help resist the idea of the technologically enabled abuse is less serious than other forms of violence.

The next section discusses legal responses to cyber-enabled interpersonal violence in the Australian context.

Assessing legal responses to cyber-enabled family violence

[5.120] There are several ways the law can intervene in family violence enabled by the internet. Criminal prosecution is one possible legal response, and there several potentially relevant criminal offences. Some crimes relate specifically to things that happen via digital means, whereas others can apply to both online and offline conduct. Intervention orders are another legal avenue that may be pursued to protect victims of online family violence. This section provides a brief overview of the type of computer misuse offences found in Australian law that could be applicable to cyber-enabled family violence before turning to assess legal responses to two types of family violence committed online: image-based sexual abuse and online sexual harassment.

114 Harris and Woodlock, n 3, 532.

115 Harris and Woodlock, n 3.

116 Harris and Woodlock, n 3, 532.

117 Powell and Henry, n 4, 50.

118 Al-Alosi, n 79, 1573.

Crimes relating to the improper use of computers

[5.130] As discussed in [5.60], there are nine criminal jurisdictions in Australia: one for each state and territory, and a Commonwealth criminal jurisdiction. The criminal legal framework in each jurisdiction provides for offences that specifically refer to the misuse of computers, with considerable overlap among them. While computer crimes are perhaps more obviously suited to cyber-dependent crimes such as ransomware, there are a number of computer offences that could equally apply to cyber-enabled interpersonal violence. For example, s 408E of the *Commonwealth Criminal Code* makes it an offence to "use a restricted computer (password protected) without the consent of the person who controls the computer".[119] While the maximum penalty for this offence is two years imprisonment, this increases to 10 years if the "person causes or intends to cause detriment or damage, or intends to gain a benefit".[120] Such a provision may be applicable to both cyber-dependent and cyber-enabled offending.

There are several Commonwealth offences relating to the improper use of technology that would be suitable for online family violence. For example, s 372.1 of the *Commonwealth Criminal Code* criminalises identity fraud, making it an offence to "make, supply or use" the identification information of another person to pretend to be, or pass oneself off, as another person. This could be relevant where a perpetrator pretends to be an ex-partner and harass the victim through that impersonation. Other offences refer to the use of a carriage service (which includes telephone and internet services) to make a threat to kill,[121] a threat to cause serious harm,[122] or to menace, harass or cause offence.[123]

Legal responses to image-based sexual abuse

[5.140] One of the most well-known forms of cyber-enabled abuse is the sharing of intimate images without the permission of the subject of the image. This conduct – known as image-based sexual abuse – has been the focus of substantial legislative reform around the world.[124] It is a complex phenomenon, and perpetrators can include family members, friends, acquaintances and unknown people, along with intimate partners.[125] Unlike

119 *Criminal Code Act 1995* (Cth), Sch 1 s 408E.

120 *Criminal Code Act 1995* (Cth), Sch 1 s 408E.

121 *Criminal Code Act 1995* (Cth), Sch 1 s 417.15.

122 *Criminal Code Act 1995* (Cth), Sch 1 s 474.15.

123 *Criminal Code Act 1995* (Cth), Sch 1 s 474.17.

124 Powell and Henry, n 4, 203.

125 Henry, Flynn and Powell, n 87, 2.

the forms of cyber-enabled abuse discussed below, while some internet-based sexual abuse "mirrors the dynamic of male-to-female partner abuse, this is far from a gendered issue, with vulnerable and disadvantaged groups most likely to be victimised, and common dynamics of peer-to-peer sexual harassment and abuse also being found to exist".[126]

There is some debate about whether there is a need for specific legislation for image-based sexual abuse (given it is often covered by broad criminal offences or civil wrongs),[127] but Australian jurisdictions have opted to specifically criminalise it. In Queensland, for example, the *Criminal Code Act 1899* (Qld) includes several crimes that are particularly relevant in online contexts. Some offences refer to the creation and distribution of material in breach of a person's privacy. Section 227A makes it an offence to "observe or visually record" another person without their consent and in "circumstances where a reasonable adult would expect to be afforded privacy".[128] In addition, s 227A(2) criminalises the conduct colloquially known as "upskirting", by making it an offence to "observe or visually record another person[s] genital or anal region without [their] consent" where a "reasonable adult would expect to be afforded privacy in relation to that region".[129] It is a further offence to distribute these "prohibited visual recordings" without the consent of the person.[130] The maximum penalty for these offences is imprisonment for two years.

In Victoria, image-based sexual abuse is criminalised by ss 40–41DB of the *Summary Offences Act 1966* (Vic). Similar to Queensland, some of the offences specifically deal with "observing"[131] or "visually capturing"[132] another person's genital or anal region "in circumstances where it would be reasonable for that other person to expect that his or her genital or anal region" could not be observed/visually captured.[133] It is a further offence to distribute images of another person's genital or anal regions (regardless of whether the act of visually capturing the image was in breach of the act).[134] There are also more general offences dealing with the distribution[135] or the threat to

126 Henry, Flynn and Powell, n 87, 14.

127 Powell and Henry, n 4, 203.

128 *Criminal Code Act 1899* (Qld), s 227A.

129 *Criminal Code Act 1899* (Qld), s 227A(2).

130 *Criminal Code Act 1899* (Qld), s 227B.

131 *Summary Offences Act 1966* (Vic), s 41A.

132 *Summary Offences Act 1966* (Vic), s 41B.

133 *Summary Offences Act 1966* (Vic), ss 41A, 41B.

134 *Summary Offences Act 1966* (Vic), s 41C.

135 *Summary Offences Act 1966* (Vic), s 41DA.

distribute[136] intimate images: the Act provides it is an offence to intentionally distribute an intimate image of another person where the "distribution of the image is contrary to community standards of acceptable conduct".[137] It defines "community standards of acceptable conduct" as including the "nature and content of the image", the circumstances in which the image was captured and distributed, the age and intellectual capacity of the person depicted image, and the extent to which the distribution affects their privacy.[138]

While the criminal legislation appears suitable for prosecuting image-based sexual abuse, challenges to combating this type of offending remain. Many victims might be reluctant to report to police because they worry about being blamed for having originally consented to the image, or fear that the images will be accessed by police or others.[139] This is another area where we see the difficulties caused by naming and perceptions of the conduct: the narrow conceptualisation of the conduct as "revenge pornography" carried out as an act of retribution assumes a particular intention on the part of the perpetrator, and it has shaped the legislative response and continues to shape the criminal justice response.[140]

In addition, different people might have different understandings of what amounts to an intimate image. Powell and Henry observe in relation to the Victorian legislation that different people in the community might have different ideas of what amounts to an intimate or sexual image, and that this should be taken into account when interpreting the legislation:

> For instance, would existing laws criminalise the non-consensual distribution of an image of a Muslim woman in her underwear without her hijab on? Would an "intimate" image include women's cleavage or nipples underneath clothing? We contend that interpretations of the meaning of such language should take into account the nature and the content of the image, the degree to which the distribution affects the privacy of the person, as well as the degree to which distribution of images violates that person's community's standards of acceptable conduct.[141]

There are other challenges. Requiring a specific intention to cause emotional harm and distress, or proof of harm or distress, may make prosecution

136 *Summary Offences Act 1966* (Vic), s 41DB.

137 *Summary Offences Act 1966* (Vic), s 41DA.

138 *Summary Offences Act 1966* (Vic), s 41.

139 Powell and Henry, n 4, 203.

140 Powell and Henry, n 4, 203.

141 Powell and Henry, n 4, 208.

difficult.[142] In addition, whether the distribution by third parties of images that they know to be private should be criminalised is contested.[143]

In the background is the challenge of assessing the harm of the distribution. In some cases the subject of the images may suffer limited or no consequences, whereas in others there might be more significant physical, psychological, social and financial consequences, including "risks to personal safety due to stalking, domestic violence, deep shame and humiliation, altered relationships with others, reputational damage, loss of employment prospects, low self-esteem, suicide ideation and withdrawal from social life".[144] The impact might not be felt immediately: one of the ways that the use of digital technologies exacerbates the offending is that online images can remain indefinitely online once they have been distributed.[145]

Investigating cyber-enabled family violence poses real challenges for police and prosecutors. The victim might feel disempowered or may be the only one who can gather relevant evidence of the behaviour.[146] Furthermore – and like other forms of cyber-enabled violence – police and judicial officers might have the perception that the digitally based behaviour is less serious than physical violence, and there may be "a tendency to trivialise the victim's experience and minimise the harm suffered, leading to inadequate legal responses".[147]

Legal responses to stalking and other forms of online sexual harassment

[5.150] The primary way that courts deal with online harassment occurring in the context of family violence is through protection orders (also known as intervention orders). These orders apply to a range of conduct, but regularly cover technologically facilitated abuse like that discussed above: conduct such as persistent messaging or use of recording and tracking device. The operation of family violence protection orders are quite similar across Australia.[148] Some jurisdictions adopt a model where the order can be made either by the court or

142 Powell and Henry, n 4, 208–209.

143 Powell and Henry, n 4, 209.

144 Powell and Henry, n 4.

145 Powell and Henry, n 4.

146 "Following, harassing and monitoring" in *National Domestic and Family Violence Bench Book*, n 76, ¶3.1.5.

147 "Following, harassing and monitoring" in *National Domestic and Family Violence Bench Book*, n 76, ¶3.1.5.

148 "Purpose" in *National Domestic and Family Violence Bench Book*, n 76, ¶7.1.

the police. For example, in Queensland, a person who is experiencing family violence can apply to the Magistrates Court for a Domestic Violence Protection Order (DVO)[149] or a protection notice can be made by police.[150] A DVO can contain conditions relating to the use of technology, prohibiting the respondent to the order from engaging in domestic violence, contacting the accused or attempting to locate them.[151] If a person breaches a DVO, it can result in a criminal charge.[152] In Tasmania, police are able to make the order without the need to go to court.[153] Other jurisdictions require a court to bring the protection order into effect. For example, in Victoria, police can make a family violence safety notice for temporary protection,[154] but longer-term protection orders can only be made by a Court.[155]

After assessing a series of cases of cyber-enabled family violence, Al-Alosi notes that protection orders have some advantages: they allow for those seeking protection to ask the court to include the conditions that addresses their specific situation and needs.[156] However, getting the conditions right is important. In order to be effective, they need to explicitly include the things that are happening, such as prohibitions on "keeping a protected person under surveillance and distributing, or threatening to distribute, intimate images of the protected person".[157] The legal system – police, courts and lawyers – must also actively ensure that the defendant understands what the order provides and the consequences of breaching it.[158]

Some offences are more specifically targeted to a kind of conduct that can be enabled through digital means. For example, digital technology facilitates stalking behaviour. Some jurisdictions have introduced offences related to stalking,[159] or modified existing offences to apply to these new uses. In Queensland, four elements make up the crime of unlawful stalking. It has to be

149 *Domestic and Family Violence Protection Act 2012* (Qld), s 32.

150 *Domestic and Family Violence Protection Act 2012* (Qld), s 101.

151 *Domestic and Family Violence Protection Act 2012* (Qld), s 28.

152 *Domestic and Family Violence Protection Act 2012* (Qld), s 177.

153 *Family Violence Act 2004* (Tas), s 14.

154 *Family Violence Protection Act 2008* (Vic), Pt 3.

155 *Family Violence Protection Act 2008* (Vic), Pt 4.

156 Al-Alosi, n 79, 1592.

157 Al-Alosi, n 79, 1599–1600.

158 Al-Alosi, n 79, 1600.

159 For example, *Crimes (Domestic and Personal Violence) Act 2007* (NSW), s 13; *Criminal Code Act 1899* (Qld), s 359E; *Crimes Act 1958* (Vic), s 21A.

(1) intentionally directed at a person; (2) engage in on more than one occasion, or "if the conduct lasts for a long time, it is engaged in on any one occasion"; (3) it consists of "stalking" behaviour (which is defined); and (4) it causes the aggrieved person "detriment reasonably arising in the circumstances".[160] Stalking behaviours include conduct that can be facilitated or enabled by technology, including "following" or "watching" a person, contacting them "in any way", posting (or emailing) offensive material, or making threats.[161] While following, harassing and monitoring victims is a feature of intimate partner violence that does not necessarily rely on the digital technologies, the technology does make it enable it.[162]

There is no consensus on whether there should be cyber-specific offences for online harassment, or if instead we should rely on general offences. There are merits to either approach. For example, specific offences can more precisely communicate that the "new" conduct is considered criminal, or special investigatory powers can attach to assist with prosecutions. It can assist in the administration of justice by allowing for the easier allocation of cyber-enabled offending to specialist investigators, prosecutors and (where appropriate) courts. However, there is a risk that the creation of a subset of offences has the effect of disconnecting the conduct from broader patterns of violence and abuse. Al-Alosi is agnostic about whether further legislation should be introduced, noting that there is a lack of research about the adequacy of existing law to deal with the various types of technology-facilitated abuse.[163] She does note that criminal law can help communicate to the public the boundaries of acceptable behaviour, as well as encouraging police to pursue complaints and victims to report.[164]

Concluding Remarks

[5.160] Legislatures are limited in what they can do to respond to new and emerging cyber-dependent and cyber-enabled crimes. With respect to use of ransomware, for example, there is a patchwork of computer offences and ordinary crimes that could be used to prosecute, but there is no single Australian offence that captures all aspects of this complex incursion. In relation to cyber-enabled family violence, there is no consensus about whether specific or more

160 *Criminal Code Act 1899* (Qld), ss 359A–359E.

161 *Criminal Code Act 1899* (Qld).

162 "Following, harassing and monitoring" in *National Domestic and Family Violence Bench Book*, n 76, ¶3.1.5.

163 Al-Alosi, n 79, 1600.

164 Al-Alosi, n 79.

general crimes is preferable for image-based sexual abuse and online sexual harassment.[165] The difficulties of designing the legislation are compounded by challenges in detecting and punishing perpetrators, particularly when they are located in other jurisdictions or have obscured their identity by hiding their IP address.[166]

There are some significant similarities between the shortcomings of the legal responses to cyber-dependent ransomware and cyber-enabled family violence. There is a lack of public awareness about the legal regulation of cybercrime, meaning people do not know what mechanisms are available for them if they have been victims of ransomware or online violence.[167] In addition, it can be difficult to convince police of the seriousness of the conduct and the necessity to respond,[168] and this lack of understanding also exists in other legal institutions, with judges and magistrates not taking cybercrime seriously or not understanding digital evidence.[169] Obtaining relevant admissible evidence may also require agreement among national and international technology providers, website hosts and law enforcement agencies.[170]

Law should not, however, be the only mechanism for addressing cybercrime. Other measures to be explored include policy and structural changes, and a focus on designing computer systems in a way that allows for easier action and prevention strategies.[171] Police must be properly trained to recognise the serious harms caused by cybercrime and better resourced to investigate crimes committed by technological means. The general public should be educated with a particular focus on perpetrator accountability.[172]

Importantly, it should be made clear that "victims are not expected to forsake their use of the internet and digital communication devices simply to avoid cyber-violence".[173] Many policy responses to cybercrime expect individuals to change their online behaviour to better protect themselves. For example, the

165 Powell and Henry, n 4, 226.

166 Powell and Henry, n 4.

167 Todhunter, n 71, 431. See also C Cross et al, "Responding to Cybercrime: Results of a Comparison between Community Members and Police Personnel" (Trends & Issues in Crime and Criminal Justice No 635, Australian Institute of Criminology, August 2021).

168 Cross et al, n 167.

169 Todhunter, n 71, 432–433; Peters and Jordan, n 62, 514.

170 Al-Alosi, n 79, 1601.

171 Powell and Henry, n 4, 228; see also J Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity" (2019) 15(1) *St Anthony's International Review* 83.

172 Al-Alosi, n 79, 1602.

173 Al-Alosi, n 79.

Australian Government "ReportCyber" website encourages victims to change their security settings to avoid cybercrime.[174] Similarly, state and federal police websites set out ways individuals can be a "tougher target for cybercriminals", including keeping their computer updated, choosing strong passwords and refraining from giving out personal information online.[175] Police advise that businesses can prevent cyberattacks by requiring cumbersome multi-factor authentication and regular staff training to identify potential malware.[176] Police suggest a range of strategies to avoid online harassment, all of which stifle the individual's freedom to use social media in the way that other people do, including things like reducing the amount of personal information online, thinking "carefully" about what they post, closing social media accounts or changing email addresses.[177]

While individuals and businesses can and should implement strategies to minimise their risk of falling victim to cybercrime, attempts to combat cybercrime must be carried out in a way that enables and protects people's capacity to use the internet and digital tools without placing undue burdens and restrictions on users. To that end, the onus to prevent cybercrime should extend to the designers of digital products, databases and electronic communications. The Australian Computer Society has highlighted the fact that "cybercrime almost exclusively leverages the lack of security-focused design in everything from your smartphone and web browser to your credit card and even the electronic systems in your car".[178] We should therefore be encouraging – perhaps mandating – technology and software programmers to design their systems in a way that reduces the risk of the technology being misused. A holistic response that involves users, government, law enforcement, cybersecurity specialists and the technology industry itself, is likely to be the only effective way to respond to cybercrime going forward.

174 "Threats", *Australian Cyber Security Centre* <cyber.gov.au/acsc/individuals-and-families/threats>.

175 See, for example, "Online Safety", *ACT Policing* <police.act.gov.au/safety-and-security/online-safety>; "Online Safety", *NSW Police* <police.nsw.gov.au/safety_and_prevention/crime_prevention/online_safety>; "Reporting Cybercrime", *Queensland Police Service* <police.qld.gov.au/reporting/reporting-cybercrime>.

176 "Prevent a Cyber Incident", *Victorian Government* <vic.gov.au/prevent-cyber-incidents>.

177 "Do Things Securely", *Australian Cyber Security Centre* <cyber.gov.au/acsc/individuals-and-families/do-things-securely>; "Cyber Bullying", *Queensland Police Service* <police.qld.gov.au/safety-and-preventing-crime/r-u-in-control/cyber-bullying>.

178 Australian Computer Society, *Cybersecurity: Threats, Challenges, Opportunities* (Report, 14 November 2016) 14 <acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf>.