CYBER-VIOLENCE: DIGITAL ABUSE IN THE CONTEXT OF DOMESTIC VIOLENCE

HADEEL AL-ALOSI*

I INTRODUCTION

While considerable attention has been given to various cybercrimes, such as hacking, identity theft, and online fraud, less focus has been given to the issue of technology-facilitated abuse between current and former intimate partners ('cyber-violence'). The term cyber-violence refers to repeated abuse committed by one person (the abuser) against a current or former intimate partner through the use of digital technology.[1] It includes a range of controlling and coercive behaviours, such as threatening phone calls, cyber-stalking, location tracking via smartphones, harassment on social media sites,[2] and the dissemination of intimate images of partners without consent ('revenge porn').[3]

The literature on non-physical forms of domestic violence[4] committed through the use of technology has slowly been emerging and there are now a few studies investigating such abuse. These studies, while limited and largely anecdotal, provide insight on the experiences of victims[5] and domestic violence practitioners dealing with cyber-violence. What is missing in the literature, however, is an examination of the case law involving technology-facilitated

* Lecturer and lawyer. LLB/Social Science (Criminology) (Hons) (UNSW), PhD (UNSW). Correspondence to Dr Hadeel Al-Alosi: H.Al-Alosi@westernsydney.edu.au. I would like to thank the anonymous reviewers who have provided invaluable feedback.

1 In this article, the term 'cyber-violence' is used interchangeably with the term 'technology-facilitated domestic abuse'.

2 Aily Shimizu, 'Recent Developments: Domestic Violence in the Digital Age: Towards the Creation of a Comprehensive Cyberstalking Statute' (2013) 28 *Berkeley Journal of Gender, Law & Justice* 116, 117.

3 The term 'revenge porn' has been criticised for failing to reflect that the images may have been distributed for a variety of reasons other than revenge and because it is inappropriate to label the images as 'pornography'. Although not without reluctance, the term 'revenge porn' is used in this article to refer to the non-consensual sharing of intimate images, as it is the most widely used and understood term in the literature. See Legal and Constitutional Affairs References Committee, Parliament of Australia, *Phenomenon Colloquially Referred to as 'Revenge Porn'* (2016).

4 Although the term 'domestic violence' encompasses a wide range of relationships (such as relationships between blood relatives and in-laws), the focus of this article is on domestic violence between current and former intimate partners.

5 Some prefer to use the term 'victim' to describe individuals who have, or are, experiencing domestic violence; others prefer to use the term 'survivor'. While acknowledging that each person's experience is unique, this article uses the term 'victim' for consistency.

domestic violence. This article contributes to the literature by reviewing cases heard in Australian courts of law involving allegations of cyber-violence to shed light on the limitations of the existing legislation in addressing such abuse. Although in a few of the cases identified the alleged cyber-violence perpetrator was female,[6] the vast majority of perpetrators were male. It is acknowledged that men do in fact experience technology-facilitated abuse committed by women and this article concludes that all individuals deserve protection from such abuse. Nevertheless, as it is well established that females are far more likely to be victims of domestic violence than males, the focus of this article is on cyber-violence committed against females by their current or former intimate male partner.

Part II of this article provides a general overview of domestic violence, which is followed by a discussion specifically on technology-facilitated domestic violence. It then synthesises the literature, empirical research, and case law involving cyber-violence. The article proceeds by discussing the adequacy of the existing legal remedies available to victims and concludes with suggestions for ways forward in combating cyber-violence. While the focus is on Australia, the article draws upon the international literature exploring digital forms of abuse.

II OVERVIEW AND PREVALENCE OF DOMESTIC VIOLENCE

There is no universal definition of 'domestic violence'. A useful definition that is used in this article is that provided in the *Australian National Plan to Reduce Violence against Women and Their Children* report, which defines such behaviour as 'acts of violence that occur between people who have, or have had, an intimate relationship'.[7] Domestic violence relationships are characterised by control, threats, and intimidation of one partner by another.[8] The abuse may take various forms, including physical, sexual, emotional, psychological, and financial abuse.[9]

Traditionally, 'the criminal justice system has continuously refused to recognise harms perpetrated against women in the private sphere as crimes'.[10] In the 1970s, domestic violence activists began advocating for violence committed in the home to be 'understood as criminal assault not just a private or civil matter'.[11] Domestic violence remains an inherently gendered crime, with males

6 See, eg, *Somerville and Somerville [No 3]* [2015] FCCA 2223; *Fiordan and Reesa* [2015] FamCA 1021; *Sully and Sully* [2015] FamCA 1111; *Day and Dawson* [2016] FCCA 888.

7 Council of Australian Governments, 'National Plan to Reduce Violence against Women and Their Children: Including the First Three-Year Action Plan' (Intergovernmental Agreement, 2011) 2.

8 Ibid.

9 Ibid.

10 Heather Douglas, 'The Criminal Law's Response to Domestic Violence: What's Going On?' (2008) 30 *Sydney Law Review* 439, 441.

11 Ibid 443.

comprising the vast majority of offenders and women the majority of victims.[12] Although men most commonly perpetuate the abuse against their female partner, domestic violence within same-sex relationships is not uncommon.[13] The impacts of domestic violence on the physical and psychological wellbeing of victims are immediate and long-term.[14] Immediate health impacts include physical injuries, miscarriage, sexually transmitted diseases, and death.[15] Impacts that develop over a longer term include anxiety, depression, post-traumatic stress disorder, alcohol and substance abuse, and homelessness.[16] In an Australian study, it has been found that male intimate partner abuse was the leading preventable contributor to death, disability, and illness for females in Victoria aged 15 to 44.[17]

Domestic violence does not only impact intimate partner victims, but also significantly affects the victim's children, regardless of whether the abuse is directed at them.[18] A notable example is the death of 11-year-old Luke Batty, who was killed by his father at a cricket ground in Victoria during 2014 after years of domestic violence directed towards Luke's mother, Rosie Batty.[19] Additionally, domestic violence creates significant social and economic expenses, costing Australia alone approximately $21.7 billion dollars per year.[20]

Although it is difficult to determine precisely how many women experience domestic violence, official statistics indicate that it is prevalent and affects women in Australia and worldwide.[21] According to the Australian Bureau of Statistics' 2012 *Personal Safety Survey*, 17 per cent of all women 18 years of age and over (1 479 900) had experienced violence by a partner since the age of 15.[22]

---

12 Christopher Angus, 'Domestic and Family Violence' (Briefing Paper No 5, Parliamentary Library, Parliament of Australia, 2015) 6; Amanda Gombru, Georgia Brignell and Hugh Donnelly, 'Sentencing for Domestic Violence' (Sentencing Trends & Issues No 45, Judicial Commission of NSW, June 2016) 5.

13 Liesl Mitchell, 'Domestic Violence in Australia – An Overview of the Issues' (Background Note, Parliamentary Library, Parliament of Australia, 2011) 2.

14 See, eg, World Health Organization, *Global and Regional Estimates of Violence against Women: Prevalence and Health Effects of Intimate Partner Violence and Non-Partner Sexual Violence* (Switzerland, 2013); Nata Duvvury et al, 'Intimate Partner Violence: Economic Costs and Implications for Growth and Development' (Women's Voice, Agency, & Participation Research Series No 3, World Bank, 1 November 2013); Janet Phillips and Penny Vandenbroek, 'Domestic, Family and Sexual Violence in Australia: An Overview of the Issues' (Research Paper, Parliamentary Library, Parliament of Australia, 2014).

15 World Health Organization, above n 14, 21–30; Duvvury et al, above n 14, 7.

16 World Health Organization, above n 14, 21–30; Duvvury et al, above n 14, 7; Phillips and Vandenbroek, above n 14, 18–19.

17 See VicHealth, 'The Health Costs of Violence: Measuring the Burden of Disease Caused by Intimate Partner Violence – A Summary of Findings' (Report, Victorian Government Department of Human Services, 2010).

18 Angus, above n 12, 14.

19 See, eg, Monique Ross, 'Father Who Killed Son, Luke Batty, at Cricket Ground Had History of Mental Illness, Says Boy's Anguished Mother', *ABC News* (online), 14 February 2014 <http://www.abc.net.au/news/2014-02-13/mother-in-shock-after-son-killed-by-father-at-cricket-oval/5258252>.

20 PwC Australia, Our Watch and VicHealth, 'A High Price to Pay: The Economic Case for Preventing Violence against Women' (Report, PwC Australia, November 2015) 4.

21 Angus, above n 12, 5; World Health Organization, above n 14, 2.

22 In comparison, only 5.3 per cent of Australian males aged 18 years and over (448 000) had experienced violence by a partner since the age of 15: Australian Bureau of Statistics ('ABS'), *4906.0 – Personal Safety, Australia, 2012* (11 December 2013) <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/4906.0Chapter7002012>.

In New South Wales ('NSW'), there were 29 001 domestic violence related assaults recorded during 2015, an increase of 1.9 per cent over the five-year period between January 2011 to December 2015.[23] In contrast, non-domestic violence related assaults decreased by 4.8 per cent during the same five-year period.[24] In Victoria, from 2009 to 2014, approximately 3 794 women aged 15 years and above were hospitalised due to injuries caused by an intimate partner, an average of 759 women per year.[25]

It has also been estimated in Australia that one woman is killed by her current or former intimate partner per week on average.[26] One reason for the significantly higher likelihood of males perpetrating serious acts of violence against their female partners is that men are often fuelled by a sense of entitlement and desire to control their partners.[27] Research also indicates that perpetrators tend to shift blame onto the victims in domestic violence matters by, for example, claiming the victim provoked them.[28]

In the 1980s, Australian legislatures began introducing legislation designed to give domestic violence victims the ability to apply for protection through civil proceedings, resulting in protection orders.[29] Generally, protection orders are designed to restrain a person from engaging in acts of domestic violence against another person with whom they are in a family or domestic relationship, including former and current intimate partners.[30] Although protection orders are applied through the civil system, breach of an order is a criminal offence in each Australian jurisdiction.[31] The usefulness of protection orders in preventing cyber-violence is discussed later in this article.

---

23 Derek Goh and Stephanie Ramsey, 'New South Wales Recorded Crime Statistics 2015' (Report, NSW Bureau of Crime Statistics and Research, April 2016) 16.

24 Ibid 14.

25 Erin Cassell and Angela Clapperton, 'Hospital-Treated Assault Injury among Victorian Women Aged 15 Years and over Due to Intimate Partner Violence (IPV), Victoria 2009/10 to 2013/14' (2015) 79 *Hazard* 1, 1 <https://www.monash.edu/__data/assets/pdf_file/0017/372302/haz79.pdf>.

26 Special Taskforce on Domestic and Family Violence in Queensland, 'Not Now, Not Ever: Putting an End to Domestic and Family Violence in Queensland' (Report, Queensland Government, 28 February 2015) 6. See also NSW Domestic Violence Death Review Team, 'Annual Report: 2013–2015' (NSW Government, 2015).

27 Centre for Innovative Justice, 'Opportunities for Early Intervention: Bringing Perpetrators of Family Violence into View' (RMIT University, March 2015) 16.

28 Douglas, 'Response to Domestic Violence', above n 10, 459–60. Brown et al note that in 2006 the NSW Ombudsman found that service providers have continued to express concern about the under-enforcement of protection orders by police: David Brown et al, *Criminal Laws: Materials and Commentary on Criminal Law and Process of New South Wales* (The Federation Press, 6th ed, 2015) 647.

29 Heather Douglas and Lee Godden, 'Intimate Partner Violence: Transforming Harm into a Crime' (2003) 10(2) *Murdoch University Electronic Journal of Law* 1, 2 <http://search.informit.com.au.wwwproxy1.library.unsw.edu.au/fullText;dn=20033753;res=AGISPT>.

30 In some Australian jurisdictions, there are also orders protecting people in non-domestic relationships. For example, in NSW these are known as 'apprehended personal violence orders': *Crimes (Domestic and Personal Violence) Act 2007* (NSW) pt 5.

31 Jane Wangmann, 'Incidents v Context: How Does the NSW Protection Order System Understand Intimate Partner Violence' (2012) 34 *Sydney Law Review* 695, 696–7.

More recently, the federal Australian government has made progress in combating domestic violence by investing in preventative measures.[32] In 2015, the Council of Australian Governments ('COAG') announced that it has agreed to jointly contribute $30 million for a national campaign designed to reduce domestic violence against women and their children.[33] Notably, the COAG stated that it 'will consider strategies to tackle the increased use of technology to facilitate abuse against women, and to ensure women have adequate legal protections against this form of abuse'.[34]

State governments have also taken initiative in tackling domestic violence. In February 2015, the Victorian Government established the Royal Commission into Family Violence as a result of a series of family violence related deaths, most notably the death of Luke Batty mentioned above.[35] The task of the Commission was to, among other things, make recommendations on how to better tackle family violence, support victims (especially women and their children), and make perpetrators accountable.[36] Although the Commission recognised that in 'recent times, technology-facilitated abuse – for example, surveillance and monitoring using phone apps and other software – has emerged as a new way of stalking victims even after the relationship has ended',[37] insufficient attention was paid to developing strategies aimed at tackling such abuse. Another initiative is the New South Wales Government's Domestic Violence Justice Strategy, which aims to improve the criminal justice system's response to domestic violence.[38] However, the strategy does not mention technology-facilitated abuse. As will be discussed in the following Part, this fails to acknowledge that domestic violence is increasingly being committed by electronic means.[39]

---

32 For an overview of some of the key policy initiatives introduced by Australian governments see Australia's National Research Organisation for Women's Safety, 'Meta-evaluation of Existing Interagency Partnerships, Collaboration, Coordination and/or Integrated Interventions and Service Responses to Violence against Women' (Landscapes: State of Knowledge Paper No 11, UNSW Australia, September 2015) 29.

33 Council of Australian Government, 'COAG Communiqué' (17 April 2015) 1 <http://www.coag.gov.au/sites/default/files/communique/COAG%20Communique%2017%20April%202015.pdf>.

34 Ibid.

35 Victorian Government, Royal Commission into Family Violence, *Summary and Recommendations* (2016) 1.

36 Ibid.

37 Ibid 17.

38 NSW Government, 'The NSW Domestic Violence Justice Strategy: 2013–17' (2017) <http://www.crimeprevention.nsw.gov.au/domesticviolence/Documents/domestic-violence/DVJS.pdf>.

39 Law Reform Commission of Western Australia, *Enhancing Family and Domestic Violence Laws: Final Report*, Final Report Project No 104 (2014) 132. See also Laurie L Baughman, 'Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators' (2010) 19 *Widener Law Journal* 933.

III THE RISE OF CYBER-VIOLENCE

Technology-facilitated abuse is a form of domestic violence that provides abusers new and more extensive ways to control, coerce, stalk, and harass their victims.[40] Technology, such as computers, smartphones, and tracking devices, allows abusers to overcome geographic and spatial boundaries that would have otherwise prevented them from contacting their victims. It also allows abusers to create 'a sense of omnipresence and eroding [the victim's] feelings of safety after separation'.[41] Consequently, while some individuals have physically left their abusive partner, technology has prevented them from completely severing ties.[42]

There is a growing body of Australian and international research on digital abuse experienced by individuals, in particular young females, such as cyber-bullying, cyber-stalking, and non-consensual sexting, by both people they know and strangers.[43] Although some research suggests that males and females are equally likely to be victims of online abuse, most studies indicate that females are overrepresented as victims for some types of severe harassment, especially online sexual harassment.[44] In the 2015 report *Digital Harassment and Abuse of Adult Australians*, which surveyed 3000 adults aged 18 to 54, it was found that 'perpetrators of digital harassment were twice more likely to be male

40 Tammy Hand, Donna Chung and Margaret Peters, 'The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation' (Stakeholder Paper No 6, Australian Domestic & Family Violence Clearinghouse, January 2009) 2. See also Susan Hopkins and Jenny Ostini, 'Addressing Technology Enabled Violence against Women and Girls in the Digital Age' (2016) 25(1) *Redress* 2.

41 Delanie Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' (2017) 23 *Violence Against Women* 584, 598.

42 Jill P Dimond, Casey Fiesler and Amy S Bruckman, 'Domestic Violence and Information Communication Technologies' (2011) 23 *Interacting with Computers* 413, 416.

43 Cyber Civil Rights Initiative, '2013 Nonconsensual Pornography Study Results' (Report, 2013) <https://www.cybercivilrights.org/ncpstats/>; Maeve Duggan et al, *Online Harassment* (Pew Research Center, 22 October 2014) <http://www.pewinternet.org/2014/10/22/online-harassment/>; Kathryn Branch et al, 'Revenge Porn Victimization of College Students in the United States: An Exploratory Analysis' (2017) 11 *International Journal of Cyber Criminology* 128; Amanda Lenhart, Michele Ybarra and Myeshia Price-Feeney, 'Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn"' (Data Memo No 12, Data & Society Research Institute, 13 December 2016); Bradford W Reyns, Billy Henson and Bonnie S Fisher, 'Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among College Students' (2012) 33 *Deviant Behavior* 1; Symantec, 'Norton Study Shows Online Harassment Nears Epidemic Proportions for Young Australian Women' (Press Release, 8 March 2016) <https://www.symantec.com/en/au/about/newsroom/press-releases/2016/symantec_0309_01>; Broadband Commission for Digital Development, 'Cyber Violence against Women and Girls: A Worldwide Wake-Up Call' (Discussion Paper, United Nations, October 2015); Renée Römkens, Tim de Jong and Hanna Harthoorn, *Violence against Women: European Union Survey Results in the Dutch Context* (Atria, 2016) 30–1; Plan International Australia and Our Watch, '"Don't Send Me That Pic"' (Survey, March 2016); Anastasia Powell and Nicola Henry, 'Digital Harassment and Abuse of Adult Australians: A Summary Report' (RMIT University, 2015).

44 For example, in the United States Pew Research Centre's study involving 2849 web users, it was found that although men were somewhat more likely than women to experience less severe forms of harassment, such as name-calling, women were significantly more likely to experience severe types of harassment, such as cyber-stalking and sexual online harassment: Duggan et al, above n 43, 3–4. See also Nicola Henry and Anastasia Powell, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2016) *Trauma, Violence, & Abuse* 1.

than female'.[45] Similarly, in the *Online Harassment: The Australian Woman's Experience* study, which surveyed 1053 Australian women, it was reported that 76 per cent of women under 30 years of age have experienced some form of online harassment,[46] indicating that cyber-violence against females has reached 'epidemic proportions'.[47] On an international level, the United Nations estimates that 73 per cent of females worldwide have endured online abuse.[48] Additionally, in a large-scale study in Europe, one in six women reported to have experienced some form of digital harassment since the age of 15, such as cyber-bullying, cyber-stalking, and circulation of sexually explicit pictures of themselves without consent.[49] This figure increased to one in three when looking at women only in the age group 18 to 29.

However, a major limitation of these studies is the lack of clarity as to what constitutes digital abuse and because the studies tend to capture one-off instances of online harassment, which may not fall within the scope of existing laws that usually require at least 'two or more incidents' that cause fear to the victim.[50] Additionally, most of the existing studies were not specifically concerned with online harassment committed by a current or former intimate partner; rather, the participants were asked generally whether they had been harassed online by anyone, including friends, acquaintances, and strangers.[51] Therefore some of the findings would not fit within the definition of technology-facilitated domestic violence.

Indeed, there is sparse empirical research specifically on technology-facilitated domestic violence.[52] One of those few studies is that conducted by a British domestic violence charity, Women's Aid, which involved surveying 307 female domestic violence victims in 2013.[53] In that study, 48 per cent reported experiencing online abuse by their former partner *after* they had ended the relationship and 45 per cent reported that their intimate partner had abused

---

45 Powell and Henry, 'Digital Harassment', above n 43.

46 Symantec, above n 43. Online harassment in the Norton study was broadly defined as including cyberbullying, unwanted contact, trolling, revenge porn, and threats of physical violence.

47 Ibid; Claire Reilly, '"Not Just Words": Online Harassment of Women an "Epidemic"' *CNet* (online), 8 March 2016 <https://www.cnet.com/au/news/not-just-words-online-harassment-of-women-epidemic-norton-research/>.

48 Broadband Commission for Digital Development, above n 43, 2.

49 Römkens, de Jong and Harthoorn, above n 43, 30–1.

50 National Centre for Cyberstalking Research, 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' (University of Bedfordshire, 2011) 2; see also Henry and Powell, 'Technology-Facilitated Sexual Violence', above n 44, 7.

51 For example, in the Pew Research Center's study, 38 per cent of the participants said that a stranger was responsible for their most recent experience of online harassment. A further 26 per cent said they did not know the identity of their online abuser: Duggan et al, above n 43, 5.

52 Delanie Woodlock, 'Technology-Facilitated Stalking: Findings and Recommendations from the SmartSafe Project' (Domestic Violence Resource Centre Victoria, 2013); Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, 'ReCharge: Women's Technology Safety, Legal Resources, Research & Training' (National Study Findings Report, 2015); McAfee, 'Do You Share Passwords with Your Partner?' (4 February 2013) <https://securingtomorrow.mcafee.com/consumer/family-safety/love-relationships-technology-survey/>; Clare Laxton, 'Virtual World, Real Fear: Woman's Aid Report into Online Abuse, Harassment and Stalking' (Women's Aid, 2014).

53 Laxton, above n 52, 8.

them online *during* their relationship.[54] Although not concerned specifically with cyber-violence, in its review of domestic violence homicides occurring between 2000 to 2012, the NSW Domestic Violence Death Review Team observed that technology was commonly being used by abusers to stalk, monitor, and control their intimate partners while the relationship was on foot, challenging 'misconceptions that stalking behaviours usually only manifest after the relationship has ended'.[55]

In Australia, the Domestic Violence Resource Centre is said to have conducted the first study specifically examining the use of technology by abusers in the context of domestic violence in 2013, known as the *SmartSafe Project*.[56] It involved surveying 152 domestic violence practitioners and 46 female victims. The technology and online platforms identified as being most commonly used by abusers to commit cyber-violence were smartphone (82 per cent); mobile phone (82 per cent); Facebook (82 per cent); email (52 per cent); and Global Positioning Systems ('GPS') tracking (29 per cent).[57] As will be seen in Part IV of this article, review of the Australian case law also showed that Facebook was a popular platform used by perpetrators to commit cyber-violence and was often used in combination with other digital devices.

Building on the *SmartSafe Project*, the Domestic Violence Resource Centre in collaboration with Women's Legal Service NSW and WESNET, conducted an online survey for domestic violence practitioners in Australia that was available between November 2014 and February 2015.[58] Ninety-eight per cent of the 546 practitioner participants said they had clients who had experienced cyber-violence.[59] This is consistent with observations made by Victoria Police, who have submitted:

> The widespread use of mobile phones has made it easier for perpetrators to harass, stalk and intimidate their victims. Over the past five years, intimate partner violence related harassment offences have increased more significantly than any other offence category. Although these offences predominantly relate to phone calls, text messages and emails, there were also several instances of tracking devices being used … As technology becomes more affordable and readily used, family violence incidents involving these technologies will increase.[60]

Accordingly, it is evident that cyber-violence is prevalent and an issue of growing concern that requires further examination.

---

54 Ibid.

55 NSW Domestic Violence Death Review Team, above n 26, 62.

56 Woodlock, 'Technology-Facilitated Stalking', above n 52.

57 Ibid 15.

58 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 3.

59 Ibid 5.

60 Victoria, Royal Commission into Family Violence, *Report and Recommendations* (2016) vol 1, 29, quoting Victoria Police, Submission to the Royal Commission into Family Violence, 37.

IV REVIEW OF THE CASE LAW INVOLVING CYBER-VIOLENCE

As mentioned above, this article seeks to contribute to the knowledge about the challenges posed by cyber-violence by examining relevant Australian case law. This analysis is valuable in gaining insight into how the courts are dealing with allegations of cyber-violence, identifying the various types of digital abuse faced by complainants, and evaluating the adequacy of the existing laws in dealing with such behaviour. The methodology entailed systematically searching Australian legal databases and court websites using appropriate search terms. The searches were not limited to criminal cases and it was found that a majority of allegations of cyber-violence had arisen in family law proceedings relating to parenting arrangements. Family law courts are generally not concerned with determining the guilt or innocence of an individual for a crime. Thus, a limitation of the findings is that many of the cyber-violence complaints discussed below are only allegations that have not been substantiated to the criminal standard of proof of beyond reasonable doubt.

There were far less reported criminal proceedings dealing with cyber-violence even though, as will be argued in this article, such conduct warrants criminal condemnation. However, it should be noted that, because the vast majority of criminal offences are dealt with summarily in the local courts, including breaches of civil protection orders, they are often not reported.[61] This is also an unavoidable limitation of this study that made quantifying the number of cases dealing with cyber-violence inappropriate.

Given the ubiquity of digital communication devices, it is unsurprising that some individuals are misusing technology to abuse and harass their current or former intimate partners. In the case law reviewed, it was common in both family law and criminal law proceedings for victims to allege that the abuser had sent them offensive text messages and/or emails, and made continuous threatening phone calls.[62] This behaviour was usually accompanied by other forms of cyber-violence, such as spying on victims, abusing victims on social media sites, and sharing intimate photos of the victim without their consent. Below is a discussion of these behaviours and, where relevant, the case law is used to illustrate the different manifestations of cyber-violence and how the courts are dealing with such abuse.

A Cyber-Stalking, Tracking Devices, and Key-Logging

Evidently, there is a strong association between domestic violence and stalking.[63] When stalking occurs in the online environment, it is referred to as

61 Douglas, 'Response to Domestic Violence', above n 10, 446.

62 For example, *Woolley and Dickinson* [2014] FCCA 1819; *Whitehouse and Whitehouse* [2015] FCCA 362; *Sakkers v Thornton* [2009] WASC 175; *Conomy v Maden* [2016] WASCA 30; *Weston v Cartmell* [2015] WASC 87.

63 See ABS, above n 22; NSW Domestic Violence Death Review Team, above n 26, 62; Katrina Baum et al, 'National Crime Victimization Survey: Stalking Victimization in the United States' (Special Report, Bureau of Justice Statistics, January 2009); TK Logan, 'Research on Partner Stalking: Putting the Pieces

'cyber-stalking', which is 'analogous to traditional forms of stalking in that it incorporates persistent behaviours that instil apprehension and fear'.[64] Stalking by intimate partners has been identified as a risk factor for physical violence, including sexual abuse and murder, often occurring when a female separates, or attempts to separate, from a violent partner.[65] For example, in the United Kingdom Women's Aid study, 38 per cent of surveyed domestic violence victims reported online stalking after they had separated from their partner.[66]

One method used by abusers to stalk and track the whereabouts of their victim is through GPS.[67] These systems are satellite-based navigation technology that determine worldwide positioning and pinpoint locations. There is considerable anecdotal evidence reporting that domestic violence abusers often stalk their ex-partners via a device with GPS capability.[68] In the *SmartSafe Project*, approximately 29 per cent of practitioners claimed that abusers relied on GPS to stalk their clients.[69] In the 2015 national survey, 34 per cent of domestic violence practitioners said they had clients who had been GPS tracked 'often' or 'all the time'.[70] In their submission to the enquiry on *Remedies for the Serious Invasions of Privacy,* the NSW Women's Legal Services also noted:

> We have clients who are separated under one roof, where they are still living with a perpetrator but in separate locked away bedrooms, and they find surveillance devices in their private rooms … Also with surveillance devices you have a lot of spyware and GPS tracking and often the things that are most insidious are the things that we commonly use, Find my Phone in your iPhone or things that are linked up through Cloud computing and children being given devices that already have things on them … Many of these things can be remotely removed from the phone and are not detectable.[71]

Together' (Report, National Institute of Justice, October 2010) <https://www.nij.gov/topics/crime/intimate-partner-violence/stalking/documents/research-on-partner-stalking.pdf>; Kevin S Douglas and Donald G Dutton, 'Assessing the Link between Stalking and Domestic Violence' (2001) 6 *Aggression and Violent Behavior* 519.

64 Emma Ogilvie, 'Cyberstalking' (Paper No 166, Australian Institute of Criminology, September 2000) 1.

65 See Hand, Chung and Peters, above n 40.

66 Laxton, above n 52.

67 See Colleen Woods, 'Finding Safe Distance: Tracing the Connections between Domestic Violence and Information Communication Technologies' (Research Paper, University of Technology Sydney, 2014).

68 See, eg, Dimond, Fiesler and Bruckman, above n 42; Woodlock, 'Technology-Facilitated Stalking', above n 52, 24; Kevin Orland, 'Stalker Victims Should Check for GPS', *CBS News* (online), 6 February 2003 <http://www.cbsnews.com/news/stalker-victims-should-check-for-gps/>; Matt Wordsworth '"Stalker Apps" and GPS Allow Domestic Violence Abusers to Discover Hidden Refuges', *ABC News* (online), 28 June 2015 <http://www.abc.net.au/news/2015-06-28/stalker-apps-and-gps-endanger-domestic-violence-victims/6570882>; Aarti Shahani, 'Smartphones Are Used To Stalk, Control Domestic Abuse Victims', *All Tech Considered* (online), 15 September 2014 <http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.

69 Woodlock, 'Technology-Facilitated Stalking', above n 52.

70 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 6.

71 Standing Committee on Law and Justice, 'Remedies for the Serious Invasion of Privacy in New South Wales' (Report, Legislative Council, 3 March 2016) 22, quoting Ms Alexandra Davis (solicitor at Women's Legal Services NSW).

The passage above further highlights that spyware is being used to facilitate domestic violence.[72] There are different types of spyware software, some of which can be freely downloaded online.[73] Spyware software was originally developed to assist parents to monitor their children's online activities, but is now also being used by abusers to monitor their current or former partner's internet usage.[74] For example, spyware was used by Simon Gittany who murdered his then fiancé, Lisa Harnum, by pushing her from a 15th floor balcony in their Sydney home upon realising she was going to leave him.[75] At trial for the murder, the Court described Gittany as a 'jealous and possessive partner',[76] who had kept 'track of [Lisa Harnum's] movements with surveillance cameras installed in their unit and secretly monitor[ed] her mobile telephone with spying software he had installed without her knowledge'.[77] Gittany was eventually sentenced to a term of imprisonment with a non-parole period of 18 years.[78]

Some spyware software facilitates key-logging, which records every keystroke entered into a computer. It allows the installer to collect personal information such as passwords, email addresses, and access to their victim's internet banking.[79] To install keystroke loggers, the abuser needs to have access to the victim's computer.[80] However, remote keystroke technology does not require physical access to a person's technological device, as it can be installed remotely by, for example, sending an email with the software attached.[81] Once the person downloads the attachment the abuser will automatically be able to monitor the victim's online activities.[82] Attempts to delete the browser history are also recorded.[83] This means that, while online resources may provide useful information on how victims can escape, abusers can use keystroke technology to monitor the victim's online activities, revealing the victim's exit strategy.[84]

---

72 Ibid. See also Woods, above n 67; Shahani, above n 68; Rachel Olding, 'Spyware's Role in Domestic Violence', *The Sydney Morning Herald* (online), 22 March 2014 <http://www.smh.com.au/technology/technology-news/spywares-role-in-domestic-violence-20140321-358sj.html>.

73 Woods, above n 67, 21; Women's Aid, *Spyware* (2017) <https://www.womensaid.ie/help/digitalabuse/spyware.html>; Zoe Kleinman, 'Spyware Use in Domestic Violence "Escalating"', *BBC News* (online), 22 December 2014 <http://www.bbc.com/news/technology-30579307>.

74 Hand, Chung and Peters, above n 40, 6–7; Cynthia Southworth et al, 'Intimate Partner Violence, Technology, and Stalking' (2007) 13 *Violence Against Women* 842, 848.

75 *R v Gittany [No 5]* [2014] NSWSC 49.

76 Ibid [6] (McCallum J).

77 Ibid [7] (McCallum J).

78 See *Gittany v The Queen* [2016] NSWCCA 182.

79 Hand, Chung and Peters, above n 40, 6–7; Australian Institute of Criminology, 'More Malware – Adware, Spyware, Spam and Spim' (High Tech Crime Brief No 11, Australian Government, 2006) 1.

80 Hand, Chung and Peters, above n 40, 7; Dalia Colon, 'Tech Terror: Cyber-Stalking and Domestic Violence', *Miami Herald* (online), 9 October 2010 <http://www.miamiherald.com/latest-news/article1936972.html>.

81 Southworth et al, above n 74, 848.

82 WESNET, 'Who's Spying on Your Computer? Spyware, Surveillance and Safety for Survivors' (National Network to End Domestic Violence, 2016) 2–3 <https://techsafety.org.au/wp-content/uploads/2016/12/WESNET_SpywareandSafety.pdf>.

83 Southworth et al, above n 74, 848.

84 Hand, Chung and Peters, above n 40, 6; Justine A Dunlap, 'Intimate Terrorism and Technology: There's an App for that' (2012) 7 *University of Massachusetts Law Review* 10, 18.

Several Australian cases reviewed involved an abusive partner using a tracking device to monitor their victim.[85] In *Mardine and Uysal*, a family law case concerning the custody of children, it was alleged that the father continuously invaded the mother's privacy during their relationship by installing keystroke software and a GPS monitoring system in her phone without her knowledge.[86] The mother stated that, as a result of the father's surveillance, she continuously felt restrained and insecure when using the internet and that this affected 'her ability to communicate with family and friends' residing overseas.[87]

In *Casano and Antipov* it was alleged 'the father downloaded an application onto his phone which enabled him to track the mother's location and monitor her telephone calls'.[88] The mother also claimed that he had accessed her Facebook account to monitor her and police records showed that 'the mother received over one hundred abusive text messages which made her feel upset, depressed and scared for her safety'.[89] Although the Family Court was not concerned with the criminal liability of the father, the Court did consider the evidence of cyber-violence when determining who should have parental responsibility for the child involved. Given the history of domestic violence, including cyber-violence, committed by the father, it was held that it was in the best interest of the child for the mother to have sole parental responsibility.[90]

A criminal law case involving cyber-stalking is *Roncevic v Boxx,* where the offender and the victim had been in a relationship from 2002 to 2014.[91] During this period, the victim tried to leave the offender on five separate occasions. When the victim ended the relationship in 2014, the offender began to stalk her and continuously interrogate her about her new relationship, later admitting that he had 'put a GPS tracker in her car. That's how I know where she's been going'.[92] The police were able to locate and seize the GPS tracker from the victim's vehicle, and forensic analysis of the offender's phone revealed that he would receive a text message every time he sought out information about the victim's whereabouts. During 11 to 16 April 2014 alone there were over 100 text messages found on the offender's mobile phone identifying the victim's location. The offender was originally sentenced to 27 months' imprisonment for stalking with intent to harass and using a carriage service to harass, but on appeal to the Australian Capital Territory Supreme Court, the penalty was reduced to 21 months. In contrast, in a Western Australian case, *Musgrove v Millard*, the offender was sentenced to only eight months' imprisonment under section 7 of the *Surveillance Devices Act 1998* (WA) for unlawfully installing a

85 *Wigfield and Dempsey* [2014] FCCA 195; *DPP (Vic) v Krepp* [2016] VCC 529; *Hedditch and Fowler* [2014] FCCA 1416; *Delucca and Decarlo* [2016] FamCA 497; *Mardine and Uysal* [2014] FCCA 146; *Casano and Antipov [No 3]* [2016] FamCA 653; *Bamber and Banton* [2016] FCCA 1860; *Musgrove and Millard* [2012] WASC 60.

86 *Mardine and Uysal* [2014] FCCA 146.

87 Ibid [58] (Small J).

88 *Casano and Antipov [No 3]* [2016] FamCA 653, [12] (Hannam J).

89 Ibid [135] (Hannam J).

90 Ibid [329] (Hannam J).

91 *Roncevic v Boxx* [2015] ACTSC 53.

92 Ibid [9] (Penfold J).

tracking device in his former partner's motor vehicle.[93] The significant disparity in sentences in the two cases may partly be explained by the fact that the maximum term of imprisonment under section 7 is 12 months' imprisonment, while the stalking offence in the Australian Capital Territory carries a maximum term of five years' imprisonment.[94] This highlights the need for uniform laws throughout Australia to promote consistency.

B Cyber-Violence on Social Media Sites

Domestic violence is characterised by systematic controlling, tormenting, and isolating behaviour perpetrated by one intimate partner against another.[95] Technology has given abusers the opportunity to maintain this abuse both during the relationship and after separation.[96] Social media sites, in particular Facebook, have been identified as being a medium through which individuals can monitor, control, and isolate their intimate partners.[97] Australian family courts seem to have accepted that the 'uploading of material on to Facebook pages constitutes family violence within its broad definition'.[98] In *Lackey and Mae* Neville FM commented:

> An unfortunate and increasing feature of modern litigation, particularly but not exclusively in family law, is the use of 'social media'. While it can be used for good, often it is used as a weapon, either by one or both of the parties, and or by their respective supporters … [I]t seems often to be the case that people will put on such media (particularly but not only *Facebook*) comments that I suspect they would not say directly to the person against or about whom such remarks are directed. In this regard, such remarks are, in my view, a form of cyber-bullying. Often, they are very cowardly, because those who 'post' such derogatory, cruel and nasty comments (regularly peppered with disgusting language and equally vile photographs) appear to feel a degree of immunity; they think they are beyond the purview or accountability of the law, and that they need not take any responsibility for their remarks.[99]

In several cases reviewed, victims alleged that abusers had hacked into their Facebook account to isolate them from their social networks and make it difficult for them to maintain friendships.[100] In other cases, the abuser allegedly forced their partner to give them their email and social media account passwords during

---

93 *Musgrove v Millard* [2012] WASC 60.

94 *Crimes Act 1900* (ACT) s 35.

95 See, eg, Marion Oke, 'Using Narrative Methods in Cross-Cultural Research with Mongolian and Australian Women Survivors of Domestic Violence' (2008) 8 *Qualitative Research Journal* 2, 10; Steve Mulligan, 'Redefining Domestic Violence: Using the Power and Control Paradigm for Domestic Violence Legislation' (2009) 29 *Children's Legal Rights Journal* 33, 35.

96 See, eg, NSW Domestic Violence Death Review Team, above n 26, 62; Southworth et al, above n 74, 842.

97 See, eg, Dimond, Fiesler and Bruckman, above n 42; Woodlock, 'Technology-Facilitated Stalking', above n 52; Millie J Darvell, Shari P Walsh and Katherine M White, 'Facebook Tells Me So: Applying the Theory of Planned Behavior to Understand Partner-Monitoring Behavior on Facebook' (2011) 14 *Cyberpsychology, Behavior, and Social Networking* 717.

98 *Moyne and Ashby* [2014] FCCA 2309, [131] (Judge McGuire).

99 *Lackey and Mae* [2013] FMCAfam 284, [9]–[10].

100 *Longer and Longer* [2013] FMCAfam 257, [71] (Terry FM); *CR v CM* [2015] QDC 146, [10] (Smith DCJA). See also *Peters and March* [2010] FamCA 151, [79] (Ryan J); *Casano and Antipov [No 3]* [2016] FamCA 653, [12] (Hannam J).

the relationship.[101] While such controlling behaviour should be a warning sign to victims, as observed by the NSW Domestic Violence Death Review Team, they 'may not recognise the seriousness of the abuser's behaviour, and may not make the connection between behaviours such as monitoring mobile phone use, constant messaging or the abuser constantly "checking up" on the victim, and domestic violence'.[102]

The family law case of *Holinski and Holinski* illustrates some of the tactics facilitated by technology that may be used to control intimate partners.[103] In this case, which concerned parenting arrangements, the mother alleged that the father 'conducted daily checks on her internet account, read all her emails, checked the history of her Skype account and all telephones to and from the house and told her that he arranged for all of her emails to be forwarded to his private account'.[104] The father admitted 'he accessed the mother's emails but said it was a joint account. He also agreed that he checked the internet usage each week but denied he supervised the mother's Skype calls'.[105]

Abusers have also used social media sites and digital communication devices to contact and harass victims.[106] In some cases, this was despite the existence of a protection order restraining the defendant from contacting the protected person. For example, in the family law case of *Harrell and Hancock-Harrell*, the mother claimed that 'the father continued to "send [her] abusive, offensive, denigrating, harassing and bullying emails in complete disregard to [her], the protection order, his bail conditions and everyone and anyone that has asked him to stop contacting [her]"'.[107] Another example is the family law case of *Milner and Milner*, where it was alleged that the father continued to engage in online harassment and abuse against the mother despite the existence of a protection order prohibiting contact.[108] The Court noted that the father 'posted several disturbing comments on Facebook, referring to [the mother] as a whore and stating: "When I read shit in the paper about dudes doing their spouses in … I don't accept it nor condone it but I can see why they have gone off the fkn rails now"'.[109]

In some cases, it seems that the offender knew they were breaching a protection order by harassing the victim via technology. For example, in the criminal law case of *Conomy v Maden,* there was evidence that the offender

101 *Longer and Longer* [2013] FMCAfam 257; *Mardine and Uysal* [2014] FCCA 146; *Holinski and Holinski* [2016] FamCA 45.

102 NSW Domestic Violence Death Review Team, above n 26, 62.

103 *Holinski and Holinski* [2016] FamCA 45.

104 Ibid [102] (Hannam J).

105 Ibid.

106 For example see *Harrell and Hancock-Harrell* [2016] FamCA 831; *Bamber and Banton* [2016] FCCA 1860; *Conomy v Maden* [2016] WASCA 30; *Phillips v Police* (2016) 125 SASR 427; *Delucca and Decarlo* [2016] FamCA 497; *Massey and Montgomery* [2016] FCCA 1890; *Whitehouse and Whitehouse* [2015] FCCA 3621; *Pattison and Parry* [2015] FCCA 3185; *Caldera and Mateo* [2014] FCCA 1686; *Milner and Milner* [2016] FCCA 2254; *Perceval and Perry* [2014] FCCA 911; *Sampson and North* [2014] FCWA 75; *Woolley and Dickinson* [2014] FCCA 1819; *Landin and Eades* [2013] FCCA 1276.

107 *Harrell and Hancock-Harrell* [2016] FamCA 831, [59] (Tree J).

108 *Milner and Milner* [2016] FCCA 2254.

109 Ibid [21] (Judge Hartnett).

intentionally breached a protection order that explicitly stated that he was not to '[c]ommunicate or attempt to communicate with [the victim] by any means whatsoever including SMS or text messages or other electronic means'.[110] This indicates the need for more effective measures to deter cyber-violence abusers, an issue discussed later in this article.

In other cases, it is not clear whether the defendants knew that posting derogatory remarks about the victim on social media or contacting the victim via technology constituted a breach of a protection order. This highlights the need for the courts and legal practitioners to ensure that defendants understand that non-contact provisions extend to digital harassment. One way of making this clear can be demonstrated by *Sloan and Stephenson*, where the Court specifically ordered the parties not to communicate 'with the other, or any member of the other's household or extended family via Facebook or any other social networking site'.[111] Another example is *Felton and Penman*, where the Court restrained the father from 'publishing or posting any derogatory or critical comments [about] the mother on any medium, in any public place or on social media'.[112]

The Family Court has some power to prevent partners from publishing insults directed at the victim during the proceedings by the use of section 121 of the *Family Law Act 1975* (Cth). This section makes it an offence punishable by a maximum imprisonment term of one year for a person to publish 'in a newspaper or periodical publication, by radio broadcast or television or by *other electronic means* … any account of any proceedings, or of any part of any proceedings'[113] that identifies any party to family law proceedings.[114] Section 121 has been commonly used to penalise journalists and other media representatives who publish material about the parties in traditional forms of media (such as television, newspaper and radio).[115] Given the advancements in technology, the Family Court has interpreted section 121 broadly, stating that it captures publications posted by the parties involved in the proceedings on 'Facebook, My Space, Twitter and any other social networking site'.[116] For example, in *Lackey and Mae*, the mother claimed that she had been subject to domestic violence throughout their relationship and, upon her ending their relationship, the father was using technology to continue the abuse.[117] The ex-husband had published on his Facebook profile insults directed at parties involved in the family law

110 *Conomy v Maden* [2016] WASCA 30, [48] (The Court). See also *Weston v Cartmell* [2015] WASC 87.

111 *Sloan and Stephenson* [2011] FMCAfam 771, [7] (Harman FM). See also *Caldera and Mateo* [2014] FCCA 1686*; Bangi and Belov* [2015] FamCA 206; *Vincent and Reeves* [2015] FCCA 616; *Morton and Cooke* [2016] FCCA 1022; *Venture and Venture [No 2]* [2014] FCCA 3073; *Janssen and Janssen [No 2]* [2016] FamCA 796; *Yeomann and Cole* [2014] FCCA 3027; *Ahmed and Jeret* [2016] FamCA 442.

112 *Felton and Penman* [2016] FCCA 1816.

113 *Family Law Act 1975* (Cth) s 121(1) (emphasis added).

114 This includes any witness and any other person concerned with the family law proceedings.

115 Evelyn Young and Louise Fairbairn, 'Netiquette in Aladdin's Cave' (2014) 88(3) *Law Institute Journal* 42, 44.

116 *Sloan and Stephenson* [2011] FMCAfam 771, [52] (Harman FM).

117 *Lackey and Mae* [2013] FMCAfam 284.

proceedings, which was held to be a breach of section 121. Accordingly, the Court ordered the father to immediately remove the posts and that:

> [F]or the next 2 years from the date of these orders, the Marshal of the Court periodically monitor social media (*Facebook* in particular) for any 'postings' by the Father or members of the paternal family, that might refer to any person (including the children) or any matter that has been the subject of the current proceedings.[118]

Although the sharing of information on social media sites gives rise to all sorts of privacy concerns for all users, it may be particularly problematic for domestic violence victims.[119] Facebook gives users the option to 'check in' when they are visiting a certain location, which may inform abusers about their victim's location, putting the victim's physical safety at risk.[120] Privacy settings allow users to limit the availability of their information on social media sites to certain family and friends, but apparently these settings can be relatively easy to evade.[121] Domestic violence victims have expressed challenges in maintaining their safety while using social media sites, especially when friends 'tagged' them in photos or when their location appeared in a post.[122] In the *SmartSafe Project,* a domestic violence practitioner stated she 'had two clients who have relocated and changed their names but [who] have still been found by [the perpetrator] stalking the clients' friends on Facebook'.[123] Similarly, in a study on women experiencing domestic violence in regional and rural Victoria, several participants reported to being harassed, publicly shamed, and monitored by their ex-partner on Facebook.[124]

In the cases reviewed, there were frequent allegations of Facebook stalking.[125] In some cases, the abusers created false Facebook accounts to communicate with victims and monitor their online activity.[126] This is possible because social media sites usually do not require creators to verify their identity, meaning that abusers can create a fake profile to befriend and gain access to their victim.[127] Social media stalking may have adverse implications not only on victims, but also on the victim's family members, as demonstrated in *MAA v SAG*, where the offender had created a fake Facebook page, posing as a 15 year-old boy to communicate

118 See order 16 of the *Lackey and Mae* decision: ibid (emphasis in original). See also *Snell and Snell [No 5]* [2015] FamCA 420; *Longford and Byrne* [2015] FCCA 2504.

119 Baughman, above n 39, 935; Dimond, Fiesler and Bruckman, above n 42, 418.

120 Ibid. See also Woodlock, 'The Abuse of Technology', above n 41, 594.

121 Baughman, above n 39, 944.

122 See Dimond, Fiesler and Bruckman, above n 42.

123 Woodlock, 'Technology-Facilitated Stalking', above n 52, 17.

124 Amanda George and Bridget Harris, 'Landscapes of Violence: Women Surviving Family Violence in Regional and Rural Victoria' (Research Report, Deakin University Centre for Rural and Regional Law and Justice, 2014) 151 ff.

125 *Dabrowski v Greeuw* [2014] WADC 175; *Ahmed and Jeret* [2016] FamCA 442; *Woolley and Dickinson* [2014] FCCA 1819. For a New Zealand case involving cyber-stalking and Facebook in a domestic violence relationship see *Chase v Fini* [2016] NZFC 2547.

126 *Woolley and Dickinson* [2014] FCCA 1819; *Roy and Biermann* [2014] FamCA 636; *Ahmed and Jeret* [2016] FamCA 442; *Setter and Howe* [2016] FCCA 2208.

127 Baughman, above n 39, 944.

with the victim's daughter and obtain information about the victim.[128] Upon finding out that the boy she had been communicating with was really the abuser masquerading as a teenager, the daughter 'became severely depressed'.[129] The Queensland District Court dismissed the abuser's appeal, stating that the Magistrate did not err in granting the victim a protection order restraining him from contacting the victim and her children.[130]

In *Starcevic and Watson*, the Court noted that the abuser continued breaching a protection order that was in force while he was in prison.[131] Unable to communicate with the victim during his incarceration, the abuser 'commenced a campaign of using others to threaten the mother and her associates',[132] which included his relatives posting belligerent and defamatory posts on Facebook about the victim.[133] Similar allegations were made in *Perceval and Perry,* which involved a father who had previously been imprisoned for sexually assaulting the mother of his children.[134] While in prison, his relatives wrote Facebook posts 'alleging the [victim] was a mentally unstable liar who made the allegations of rape against the father for money'.[135] In other cases, it was the abuser's new partner who was engaging in harassing and intimidating conduct by making posts about the ex-partner on social media sites.[136]

C Revenge Porn

One of the challenges created by the explosion of social media sites is the non-consensual sharing of intimate images, known as 'revenge porn' or 'non-consensual sexting'.[137] In an Australian study, one in ten adults reported that someone had posted online, or sent to someone else, a nude or semi-nude image of them without their permission.[138] According to the Senate Standing Committee on Legal and Constitutional Affairs:

> Non-consensual sharing of intimate images is a serious and growing problem in Australia, facilitated in part by technological advances and increasing use of social media. Non-consensual sharing of intimate images can have a significant impact

128 *MAA v SAG* [2013] QDC 31. See also *George and Nichols* [2016] FamCA 519; Dimond, Fiesler and Bruckman, above n 42.
129 *MAA v SAG* [2013] QDC 31, [22] (McGiuness DCJ).
130 Ibid [44]–[45] (McGuiness DCJ).
131 *Starcevic and Watson* [2016] FamCA 391.
132 Ibid [30] (Tree J).
133 Ibid [31] (Tree J). See also *Edwards and Granger* [2013] FamCA 918.
134 *Perceval and Perry* [2014] FCCA 911.
135 Ibid [28] (Judge Halligan).
136 See, eg, *Rogers and Mooney* [2016] FCCA 1951; *Kester and Schultz* [2014] FCCA 174; *Howlett and Morris* [2016] FamCA 710.
137 Lyombe Eko, *The Regulation of Sex-Themed Visual Imagery: From Clay Tablets to Tablet Computers* (Palgrave Macmillan, 2016) 280. It should be noted that the image need not be sexually explicit, but may depict a person in a state of undress or semi-undress. This may include the distribution of an image of a woman without her religious headscarf, which may be considered an intimate image: Women's Legal Services NSW, Submission No 32 to NSW Standing Committee on Law and Justice, *Inquiry into Remedies for the Serious Invasion of Privacy in New South Wales*, 29 September 2015, 5.
138 Powell and Henry, 'Digital Harassment', above n 43, 2.

> on [the] victim, psychologically and physically, as well as being damaging to the victim's reputation and standing.[139]

While the research on revenge porn is still developing, such behaviour is said to commonly occur in the context of domestic violence,[140] with the typical scenario being an abuser disseminating, or threatening to disseminate, intimate images of their ex-partner after separation.[141] In the *SmartSafe Project,* nearly half of the of the practitioners surveyed said that they had clients report that their abusers threatened to disseminate private photos or images of them.[142] Of the victim participants, 42 per cent stated that their former partner '"sometimes" followed through their threats and distributed intimate photos or videos'.[143] Several practitioners also provided examples of clients who had their intimate images disseminated by their ex-partner.[144] Similarly, legal practitioners in California have observed a significant rise in revenge porn allegations in domestic violence restraining order cases.[145]

There have been several publicised examples of celebrities who have been victims of revenge porn.[146] An Australian example is the 2010 incident involving Lara Bingle whose nude images were shared without her consent by her former partner, Brendan Fevola.[147] Although there were reports that Bingle would be suing 'Fevola for "breach of privacy, defamation and misuse of her image"', such litigation 'never eventuated'.[148]

In Australia, there are a few reported civil proceedings brought by females against former partners who shared their victim's intimate images without

---

139 Legal and Constitutional Affairs References Committee, above n 3, 49 [5.1].

140 Standing Committee on Law and Justice, above n 71, 21; Adam Dodge, *Threats of Revenge Porn - A New Way to Silence Survivors of Domestic Violence* (27 July 2015) Laura's House <https://www.lauras house.org/news/threats_of_revenge_porn_a_new_way_to_silence_survivors_of_domestic_violence>.

141 Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49 *Wake Forest Law Review* 345, 353. For anecdotal evidence from victims who have had, or been threatened to have, their intimate images disseminated by ex-partners, see Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, Submission No 120 to Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, May 2014, 3–4; Office of the eSafety Commissioner, *Women's Stories* (2017) eSafety Women <https://www.esafety.gov.au/women/take-control/case-studies>.

142 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 10.

143 Ibid.

144 Ibid.

145 Haley Goldberg, *Revenge Porn: When Domestic Violence Goes Viral* (21 March 2017) Self <http://www.self.com/story/revenge-porn-domestic-violence>.

146 See, eg, Joi-Marie McKenzie, 'Mischa Barton Feels "Conned" as Victim of Apparent Revenge Porn Scheme', *ABC News* (online), 3 April 2017 <http://abcnews.go.com/Entertainment/mischa-barton-feels-conned-victim-apparent-revenge-porn/story?id=46550231>; Janelle Griffith, 'Revenge Porn: Well-Known Celebrity Victims', *New Jersey Newspaper* (online), 9 January 2015 <http://www.nj.com/entertainment/index.ssf/2015/01/celebrity_revenge_porn_victims.html>.

147 Thomas Hunter, 'Bingle Lawsuit against Fevola over Nude Photo Strikes a Blow for Women's Rights, Says Agent', *Sydney Morning Herald* (online), 2 March 2010 <http://www.smh.com.au/lifestyle/celebrity/bingle-lawsuit-against-fevola-over-nude-photo-strikes-a-blow-for-womens-rights-says-agent-20100301-pdv5.html>; Samantha Maiden, 'Push to Criminalise Revenge Porn to Stop Naked Photos Appearing Online without Consent', *The Daily Telegraph* (online), 13 September 2015 <http://www.dailytelegraph.com.au/news/nsw/push-to-criminalise-revenge-porn-to-stop-naked-photos-appearing-online-without-consent/news-story/cbebe6be1fb4ee578be702f831b162f6>.

148 Standing Committee on Law and Justice, above n 71, 19.

consent.[149] In *Wilson v Ferguson*, the male partner posted on his Facebook profile images depicting his former female partner naked after they had separated.[150] Accompanying the images, he included a comment stating, 'Happy to help all ya boys at home … enjoy!!', and later added a comment that read, 'Let this be a fkn lesson … I will shit on anyone that tries to fk me ova. That is all!'.[151] The plaintiff was awarded $35 000 in damages for the significant distress and embarrassment caused by the defendant's spiteful actions. Additionally, she was awarded $13 404 for economic loss for the time she was unable to return to work after the incident.[152] Similarly, in the case of *Giller v Procopets*, the female plaintiff sued her former male partner for recording and subsequently distributing videos of them engaging in sexual intercourse.[153] The Court held that a claim founded on a breach of confidence had been established and awarded the female plaintiff $40 000 for the breach.[154]

To date, there have been only a few reported Australian cases where abusers have faced criminal charges for disseminating revenge porn.[155] One of those few cases is *Police v Usmanov* where, in order to 'get back' at his former intimate partner, the offender posted on Facebook six naked images of the victim.[156] He then sent an email to the victim informing her '[s]ome of your photos are now on Facebook'.[157] Upon refusing the victim's request to remove the images from the website, the victim reported the incident to the police. The offender was subsequently charged under section 578C of the *Crimes Act 1900* (NSW), which makes it an offence to publish an indecent article, with a maximum penalty of $11 000 and/or 12 months' imprisonment. He was sentenced to six months home detention, but on appeal the New South Wales District Court suspended the sentence after taking into account that the offender was a 'twenty year old with no prior criminal history and an otherwise respectable and responsible background'.[158]

A publicised example of a male victimised by revenge porn that resulted in criminal charges being laid against the alleged female offender is the case of National Rugby League player, Bryce Cartwright. It has been reported that his ex-girlfriend, Brittany Hura, posted sexually explicit photos of Cartwright on social media and threatened to kill him. She was subsequently charged with using a carriage service to menace, harass or cause offence and stalk/intimidation with the intent to cause fear of physical harm.[159]

---

149 See, eg, *Giller v Procopets* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.

150 *Wilson v Ferguson* [2015] WASC 15.

151 Ibid [27] (Mitchell J).

152 Ibid [85] (Mitchell J).

153 *Giller v Procopets* [2004] VSC 113.

154 See also *Giller v Procopets* (2008) 24 VR 1; *Giller v Procopets [No 2]* (2009) 24 VR 1.

155 See, eg, *Usmanov v The Queen* [2012] NSWDC 290; *R v McDonald* (2013) 233 A Crim R 185; *DPP (Vic) v Henderson* [2015] VCC 1333.

156 *Police v Usmanov* [2011] NSWLC 40, [3] (Deputy Chief Magistrate Mottley). See also *Usmanov v The Queen* [2012] NSWDC 290.

157 *Police v Usmanov* [2011] NSWLC 40 [5] (Deputy Chief Magistrate Mottley).

158 *Usmanov v The Queen* [2012] NSWDC 290, [2] (Blanch CJ District Court).

159 Adrian Proszenko and Nick Ralston, 'Former Girlfriend of Bryce Cartwright Charged after String of Social Media Posts', *The Sydney Morning Herald* (online), 13 December 2016 <http://www.smh.com.au/

Having provided an overview of the main types of cyber-violence identified in the case law reviewed and synthesised this with the findings of the existing research, the next section considers the sufficiency of the current legal framework in dealing with cyber-violence.

V THE ADEQUACY OF THE EXISTING LAWS IN TACKLING CYBER-VIOLENCE

As mentioned previously, in the 1980s Australian legislatures began introducing legislation designed to give domestic violence victims the ability to apply for protection through civil proceedings.[160] Originally, protection orders were limited to restraining physical acts of violence, but have since been extended to include non-physical abuse, such as emotional and economic abuse and, more recently, digital intimidation and harassment.[161] When granted, protection orders impose restrictions on the behaviour of the defendant, such as the condition that they do not contact the protected person. Although protection orders are civil orders, breaching an order is a summary criminal offence.[162] Today, domestic violence protection orders are the most commonly sought legal remedy by victims and those acting on their behalf to prevent the continuation of domestic violence.[163]

Protection orders have the potential to protect victims from technology-facilitated abuse. An advantage of such orders is that those seeking protection can ask the court to specifically include a condition that meets their needs. For example, a person can seek a condition that restrains the defendant from harassing, stalking, or intimidating them *by any means*, including through the use of technological devices. However, there has been a concern that protection order applications are often dealt with perfunctorily and with insufficient attention paid to the circumstances of the case.[164] In one Victorian study, it was found that Victorian magistrates spent an average of three minutes on each protection order application.[165] Additionally, analysis of the case law indicated that abusers were often not deterred by protection orders from committing cyber-violence. This may have been because the defendants lacked awareness that the protection order extended to online communications, or it may have been an intentional breach. Intentional breaches are not uncommon, especially given the tendency of

---

rugby-league/league-news/former-girlfriend-of-bryce-cartwright-charged-after-string-of-social-media-posts-20161213-gta6bk.html>; Jack Houghton, 'Bryce Cartwright: Ex-girlfriend Brittany Hura Charged after Threatening to Kill Him', *The Daily Telegraph* (online), 14 December 2016 <http://www.dailytelegraph.com.au/news/nsw/bryce-cartwright-exgirlfriend-brittany-hura-charged-after-threatening-to-kill-him/news-story/0c5f3ca16ffb29d5644cca8bb6d1d6b5->.

160 Douglas and Godden, above n 29, 2.

161 Wangmann, above n 31, 698–9.

162 Heather Douglas and Robin Fitzgerald, 'Legal Processes and Gendered Violence: Cross-Applications for Domestic Violence Protection Orders' (2013) 36 *University of New South Wales Law Journal* 56, 60.

163 Ibid 56.

164 Centre for Innovative Justice, above n 27, 20.

165 Ibid.

defendants to see protection orders as 'merely a piece of paper' and in circumstances where police regularly fail to enforce the orders.[166]

The effectiveness of protection orders is further undermined in situations where police only charge defendants for breaching an order when the defendant's conduct also constitutes a serious criminal offence, such as assault or stalking.[167] In Douglas' study of 350 breaches of protection orders in Queensland, it was found that stalking constituted a breach of an order in 61 cases, but in none of those cases was a stalking charge laid.[168] In *Casano and Antipov*, the Family Court observed:

> The transcript of the hearing in which the father was found guilty of the charge arising from the phone call from the hospital in late January 2013, indicates that the prosecution particularised the offence as using a telephone service to 'offend' rather than the alternative particular of using the telephone service to 'menace' or 'harass'. The prosecution also elected to rely upon this single telephone call in seeking [a protection order] for the mother's protection although the mother had complained about a course of threatening and harassing telephone calls and text messages sent by the father over an extended period of time.[169]

Charging offenders only for a breach of a protection order and not for the accompanying offence(s) as well fails to recognise the extent of the harm inflicted on the victim and imposes on the offender lower penalties than what may be warranted.[170] For example, in Victoria a breach of any condition in a protection order carries a maximum penalty of two years' imprisonment and/or a fine up to 240 penalty units (which currently equates to $38 056.80),[171] while the offence of stalking carries a maximum penalty of 10 years' imprisonment.[172] It should be noted, however, that the failure to prosecute might be due to several factors. These include problems in proving the alleged offences, the victim's reluctance to engage with the criminal prosecution, and because not all acts of domestic violence meet the definition of existing criminal offences.[173]

As demonstrated by *Giller v Procopets* and *Wilson v Ferguson,* cyber-violence victims can bring civil action against their abusers.[174] For instance, victims of revenge porn may have remedies under defamation law, copyright law, or based on the equitable doctrine of breach of confidence. However, proving these civil causes of action can be difficult in the context of domestic violence and there is currently no statutory cause of action for an invasion of privacy in Australia, which means that 'victims of revenge pornography have to rely on the courts to develop remedies for the invasion of privacy they have

166 Douglas and Fitzgerald, above n 162, 60, quoting Sesha Kethineni and Dawn Beichner, 'A Comparison of Civil and Criminal Orders of Protection as Remedies for Domestic Violence Victims in a Midwestern County' (2009) 24 *Journal of Family Violence* 311, 311–12.

167 Douglas, 'Response to Domestic Violence', above n 10, 448–9; Brown et al, above n 28, 648.

168 Douglas, 'Response to Domestic Violence', above n 10, 450.

169 *Casano and Antipov [No 3]* [2016] FamCA 653, [137] (Hannam J).

170 Douglas, 'Response to Domestic Violence', above n 10, 447–53.

171 *Family Violence Protection Act 2008* (Vic) s 123(2). See also s 123A.

172 *Crimes Act 1958* (Vic) s 21A(1).

173 See Heather Douglas, 'Do We Need a Specific Domestic Violence Offence?' (2015) 39 *Melbourne University Law Review* 434.

174 *Giller v Procopets* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.

suffered'.[175] In relation to revenge porn, the NSW Standing Committee on Law and Justice noted:

> The bulk of evidence was that the available civil remedies, in particular the equitable action for breach of confidence, was [sic] inaccessible, offered a 'poor fit', and failed to offer [an] appropriate remedy to people who suffered a serious invasion of privacy.[176]

It should be noted, however, that at the time of writing, the Australian federal government released a discussion paper and is calling for submissions on a proposed civil penalty regime to deal with revenge porn.[177]

Nevertheless, not all victims have the resources to pursue civil claims against perpetrators.[178] Civil litigation is costly and time-consuming, which may cause victims further distress or deter them from seeking justice altogether.[179] Litigation may be futile in situations where the abuser has 'few assets' to compensate the victim,[180] meaning that '[i]n the real world, civil lawsuits are no remedy at all'.[181] Civil remedies also do not carry the public condemnation and sanctions warranted to address various types of cyber-violence. This has been acknowledged by Australian law reform committees that have been conducting inquiries into the adequacy of civil remedies in dealing with revenge porn and the submissions received show overwhelming support for specific criminal offences to deal with such behaviour.[182]

Recently, the New South Wales Government has been considering possible legislative responses to revenge porn, recognising the impact such behaviour may have on domestic violence victims, including 'extreme fear and mental harm'.[183] In June this year, Parliament passed legislation making it a criminal offence to intentionally distribute an 'intimate image' of a person without their consent or threatening such distribution.[184] If breached, the offender would be liable to a maximum of three years' imprisonment and/or a fine up to 100 penalty units

---

175 Tom Gostsis, 'Revenge Pornography, Privacy and the Law' (E-Brief Issue 7, Parliamentary Library, NSW Parliament, 2015) 10.

176 Standing Committee on Law and Justice, above n 71, 9.

177 Department of Communications and the Arts, 'Civil Penalties Regime for Non-consensual Sharing of Intimate Images' (Discussion Paper, Australian Government, May 2017).

178 See Citron and Franks, above n 141, 349; Nicola Henry and Anastasia Powell, 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law' (2016) 25 *Social & Legal Studies* 397, 404.

179 Alyse Dickson, '"Revenge Porn": A Victim Focused Response' (2016) 2 *UniSA Student Law Review* 42, 54.

180 Citron and Franks, above n 141, 349.

181 Mitchell J Matorin, 'In the Real World, Revenge Porn Is Far Worse than Making It Illegal', *Talking Points Memo* (online), 18 October 2013 <http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn>.

182 See especially Legal and Constitutional Affairs References Committee, above n 3; Standing Committee on Law and Justice, above n 71.

183 NSW Department of Justice, 'The Sharing of Intimate Images without Consent – "Revenge Porn"' (Discussion Paper, NSW Government, September 2016) 4.

184 *Crimes Amendment (Intimate Images) Act 2017* (NSW). An 'intimate image' is defined as under s 91FN as (a) an image of a person's private parts, or of a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, or (b) an image that has been altered to appear to show a person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy.

(which currently equates to $11 000). Notably, the legislation also amends the *Crimes (Domestic and Personal Violence) Act 2007* (NSW) to specifically state that the new offences constitute 'personal violence' for the purposes of protection orders.

The new offences would potentially overcome the perceived inadequacies of the existing laws used to prosecute revenge porn in New South Wales. In *Police v Usmanov*, the police relied upon section 578C of the *Crimes Act 1900* (NSW) to charge the offender for posting naked images of his former intimate partner.[185] This section states that it is an offence for a person to publish an 'indecent article'.[186] However, the term 'indecent' is not defined in the legislation. The courts usually apply the community standards test to determine if the material is indecent; that is, whether the material would offend the 'reasonable, ordinary, decent-minded, but not unduly sensitive, person'.[187] An intimate image will not always meet the definition of indecency and, as noted by the Court in *Police v Usmanov*, there are still uncertainties about the use of section 578C in dealing with revenge porn:

> Despite an extensive search, no NSW reported decisions could be located that assist with the approach to be taken in a matter such as this where the material has been published on Facebook or the Internet. Nor are there any NSW reported decisions where the material published is indecent but does not constitute child pornography.[188]

The federal government has been considering introducing specific legislation that will make revenge porn a criminal offence, as in other jurisdictions, including Canada, Japan, the United States, and the United Kingdom.[189] Likewise, the Northern Territory and Western Australian governments have expressed an intention to introduce legislation targeting revenge porn.[190] To date, however, no specific legislation has been enacted in any Australian jurisdiction, except Victoria and South Australia, which currently have in force statutory criminal offences specifically dealing with revenge porn.[191]

While there does not appear to be any sufficient data evaluating the impact of Victorian and South Australian legislation, data from other countries indicate that there has been a significant rise in incidences being reported to the police since introducing specific legislation criminalising revenge porn. For example, in the United Kingdom, which criminalised such behaviour in 2015, there were 1160

185 *Police v Usmanov* [2011] NSWLC 40, [1] (Deputy Chief Magistrate Mottley).

186 Under section 578C(1), an 'article' is defined as including 'any thing that contains or embodies matter to be read or looked at, or that is to be looked at, or that is a record'. A 'record' includes a film or 'any other thing of the same or of a different kind or nature, on which is recorded a sound or picture and from which, with the aid of a suitable apparatus, the sound or picture can be produced …': s 578(1). This would capture videos and images.

187 *Phillips v Police* (1994) 75 A Crim R 480, 486 (Debelle J). See also *Crowe v Graham* (1968) 121 CLR 375; *Connolly v Willis* [1984] 1 NSWLR 373; *Police v Butler* [2003] NSWLC 2; *Beck v New South Wales* [2012] NSWSC 1483.

188 *Police v Usmanov* [2011] NSWLC 40, [10] (Deputy Chief Magistrate Mottley).

189 See Criminal Code Amendment (Private Sexual Material) Bill 2015 (Cth).

190 NSW Department of Justice, above n 183, 6.

191 See *Summary Offences Act 1966* (Vic) ss 41DA–41DB; *Summary Offences Act 1953* (SA) ss 26A–26E.

reported incidents of revenge pornography from April to December 2015.[192] Yet, it was found that 61 per cent of reported incidences 'resulted in no action being taken against the alleged perpetrator', mainly due to the police believing there was insufficient evidence or because victims withdrew their complaints.[193] Similarly, it has been found that there were 1143 reported revenge porn incidents reported to the police in Japan, but only 276 prosecutions.[194] The experiences in these countries highlight that the effectiveness of the law relies heavily on its enforcement.

Nevertheless, there are criminal laws throughout Australia that may address some types of cyber-violence. At the Commonwealth level, section 474.17(1) of the *Criminal Code Act 1995* (Cth) sch 2 ('*Criminal Code*') makes it an offence to use telecommunication services to menace, harass or cause offence, which may be used to prosecute revenge porn incidents. In New South Wales, section 13(1) of the *Crimes (Domestic and Personal Violence) Act 2007* makes it an offence to stalk or intimidate with intent to cause fear of physical or mental harm. Section 359B(c)(ii) of the Queensland *Criminal Code Act 1899* explicitly addresses electronic means of stalking, stating that that stalking includes 'contacting a person in any way, including, for example, by telephone, mail, fax, email or through the use of any technology'.

Yet, because stalking offences usually require proof of continuous acts directed at the victim, some types of cyber-violence may not be captured by the existing offences, such as one-off revenge porn incidents or a single threatening post on social media about an ex-partner.[195] An isolated incident by itself may seem insignificant, but may be quite serious and damaging to the victim where there has been a history of domestic violence committed by the abuser. It is also uncertain if the existing offences cover situations where the abuser makes derogatory comments on their personal social media profile page that later comes to the attention of the victim, or where the abuser monitors the victim via a tracking device, or hacks into the victim's social media account.[196] In some Australian jurisdictions, surveillance legislation makes it an offence to knowingly install a tracking device to monitor a person without their permission.[197] However, there are substantial inconsistencies with the existing surveillance

192 See *Criminal Justice and Courts Act 2015* (UK) c 1, s 33.

193 Peter Sherlock, 'Revenge Pornography Victims as Young as 11, Investigation Finds', *BBC News* (online), 27 April 2016 <http://www.bbc.com/news/uk-england-36054273?ns_mchannel=social&ns_campaign=bbc_daily_politics_and_sunday_politics&ns_source=facebook&ns_linkname=news_central>.

194 Freedom House, *Freedom on the Net 2016: Japan: Country Profile* (2017) <https://freedomhouse.org/report/freedom-net/2016/japan>. See also 'The Repercussions of Revenge Porn', *The Mainichi* (online), 23 January 2017 <https://mainichi.jp/english/articles/20170123/p2a/00m/0na/012000c>; 'Revenge Porn: Misery Merchants', *The Economist* (online), 5 July 2014 <http://www.economist.com/news/international/21606307-how-should-online-publication-explicit-images-without-their-subjects-consent-be>.

195 Dickson, above n 179, 50–1; Nicola Henry and Anastasia Powell, 'Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment against Adult Women' (2015) 48 *Australian & New Zealand Journal of Criminology* 104, 110.

196 Law Reform Commission of Western Australia, above n 39, 133.

197 See, eg, *Surveillance Devices Act 2007* (NSW) s 9; *Surveillance Devices Act 2007* (NT) s 13; *Surveillance Devices Act 2016* (SA) s 7; *Surveillance Devices Act 1999* (Vic) s 8; *Surveillance Devices Act 1998* (WA) s 7.

laws, meaning that the legal rights of victims are highly contingent upon the jurisdiction in which they reside.

Accordingly, there have been calls for a national approach to cyber-violence and better-targeted offences to deal with technology-facilitated domestic abuse:

> The limited scope of current legislative frameworks, the lack of case law, the uncertainty around whether Commonwealth or state/territory law should apply, as well as the lack of specific legislation to tackle technology-facilitated sexual violence and harassment, means that Australian law at present 'does not sufficiently accommodate the intent, magnitude, and range of harms' that are committed through offensive behaviours involving technology.[198]

The Australian Association of Social Workers has urged 'all States and Territories [to] review their family violence legislation to ensure it provides protection from digital/cyber abuse and harassment by technology'.[199] Given the borderless nature of the internet and the ability to traverse geographical barriers by the use of technology, there is a need for consistent and uniform laws. This is particularly necessary because it is common for partners to move interstate following separation, which may pose problems in holding abusers liable under the current legal framework that is characterised by a patchwork of different laws throughout Australia.[200] A failure to implement a national approach to tackle acts of cyber-violence 'can result in victims falling through gaps in the law depending on where they live or where the perpetrator is located'.[201]

Some have argued that the existing legislation can adequately deal with various types of cyber-violence, but have expressed concern about the lack of enforcement of the law.[202] Anecdotal evidence both within and outside Australia suggests there is a lack of community confidence in police pursuing complaints.[203] According to solicitors at the Women's Legal Services NSW:

> [W]e have had clients where the police refused to do that because of the costs and because running computer forensics is done by certain crime units. Those sorts of matters are usually reserved for indictable offences and things that are considered

198 Henry and Powell, 'Beyond the "Sext"', above n 195, 110, quoting Law Reform Committee, Parliament of Victoria, *Inquiry into Sexting: Report of the Law Reform Committee Inquiry into Sexting* (2013) 140.

199 Australian Association of Social Workers, Submission to the Australian Law Reform Commission, *Family Violence: Improving Legal Frameworks*, 2 July 2010, 4.

200 See Legal and Constitutional Affairs References Committee, above n 3, [3.5].

201 Dickson, above n 179, 50. It should be noted that the Australian federal government has made some progress this year by introducing principles that aim to promote nationally consistent laws throughout to tackle revenge porn. See Law, Crime and Community Safety Council, 'National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images' <https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National-statement-of-principles-criminalisation-non-consensual-sharing-intimate-images.PDF>.

202 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 19. See also Charissa Sun, 'Technology-Facilitated Stalking and Abuse: Putting Our Legal Framework to the Test' [2015] (June) *Law Society Journal* <http://www.wlsnsw.org.au/wp-content/uploads/LSJ-Article-Charissa-Sun-June-2015-LSJ.pdf>.

203 See Woodlock, 'Technology-Facilitated Stalking', above n 52; Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52; Douglas, 'Response to Domestic Violence', above n 10; Laxton, above n 52; Citron and Franks, above n 141; Jessica West, 'Cyber-Violence against Women' (Battered Women's Support Services, May 2014) 23.

> more serious than, for example, a breach of an Apprehended Violence Order [AVO] or a stalking or intimidation offence.[204]

In the *SmartSafe Project*, 62 per cent of participants believed that police only 'sometimes' took 'technology-facilitated abuse seriously' and believed that police overlooked the severity of non-physical violence.[205] The participants also expressed concerns that the police frequently showed reluctance in pursuing complaints.[206] For example, one practitioner reported that the '[p]olice often say they can't be sure the perpetrator actually sent the messages, even though they can prove they were sent from his phone'.[207] Similarly, in the United Kingdom Women's Aid study, 75 per cent of domestic violence victims indicated a concern that the police did not know how to effectively respond to online abuse.[208] This included 12 per cent of victims who reported the abuse to the police, but claimed that they 'had not been helped'.[209]

Judge Harland's comment in *Bancroft v Lindsay* may partly explain why cyber-violence is being overlooked:

> The documents that are now before the Court and the father's conduct, to me has all the hallmarks of someone continuing to engage in controlling and coercive violence. Violence does not need to be physical and in fact, this kind of controlling, aggressive, stalking behaviour can be much more damaging. It is easier for people to understand physical violence. Bruises are visible. But for the person who is subjected to controlling and coercive violence, it can be very hard to make other people understand what they have been going through …[210]

While cyber-violence may not leave visible scars on victims, such abuse can be just 'as terrifying as physical violence' and therefore should be taken seriously.[211] Failure to take action against perpetrators may have the effect of deterring victims from reporting the abuse, believing that their complaints will not be pursued.[212]

There is also evidence of victim-blaming attitudes, both within the police force and the wider community. In the *SmartSafe Project*, one domestic violence practitioner stated, '[o]ften police put the responsibility back onto the woman and say she should stop visiting Facebook or using devices'.[213] Cyber-violence

---

204 Standing Committee on Law and Justice, above n 71, 22, quoting Ms Alexandra Davis.

205 Seventeen per cent said they believed that the police 'rarely' handled their complaints seriously and only 13 per cent said they 'always' did: Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 15.

206 Ibid 16. See also Law Reform Commission of Western Australia, above n 39, 62.

207 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 16.

208 Laxton, above n 52, 8.

209 Ibid.

210 *Bancroft and Lindsay* [2016] FCCA 1236, [16] (Judge Harland).

211 See Broadband Commission for Digital Development, above n 43. The NSW Law Reform Commission has also argued that 'intimidation and stalking can be as terrifying as physical violence, and should remain as a substantive criminal offence': Law Reform Commission, *Apprehended Violence Orders*, Report No 103 (2003) 244 [12.14].

212 Danielle Keats Citron, 'Law's Expressive Value in Combating Cyber Gender Harassment' (2009) 108 *Michigan Law Review* 373, 402.

213 Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, above n 52, 16.

victims have been told to 'just get off social media',[214] '"it's online, it's not real", "just ignore it" and "don't feed the trolls"'[215] and 'to get off the computer if [they] could not "handle a little heat" in [their] inbox'.[216] Female victims of revenge porn are 'frequently criticized for having taken nude pictures of themselves at all'.[217] It has been suggested that victims of technology-facilitated abuse take extra precaution by:

> Shut[ing] off GPS and wi-fi, stay away from social media – Twitter, Facebook, Instagram; whatever – and remember that the perpetrator will be monitoring the sites of your family and friends to see you wherever you are, because you might pop up; they might take photos of you. So please make sure that children do the same.[218]

It is questionable why victims (and their children) are being told to forsake their digital devices and online identity when the focus should be on holding perpetrators accountable for their actions. The suggestion that victims refrain from using technology also fails to acknowledge that technology can enhance victims' relationships with friends and family,[219] and can provide victims with valuable online resources and access to support services, such as e-counselling.[220] The following section outlines the ways in which cyber-violence can be better addressed by supporting victims.

VI WAYS FORWARD IN THE FIGHT AGAINST CYBER-VIOLENCE

As noted above, Australian governments have made positive steps in combating physical acts of domestic violence. However, given the rise of cyber-violence, initiatives aimed at preventing domestic violence are undermined without specifically addressing the issue of technology-facilitated abuse. Therefore, governments need to explore both civil and criminal penalties to strengthen the remedies available to victims, prevent cyber-violence, and to promote offender accountability.

Protection orders can play a role in preventing some types of cyber-violence, but the effectiveness of protection orders relies on it clearly outlining that digital abuse constitutes a breach. The NSW Women's Legal Service has recommended that protection orders should specifically include conditions prohibiting defendants from keeping a protected person under surveillance and distributing,

---

214 Ibid.

215 West, above n 203, 23.

216 Citron, above n 212, 397, quoting Markos Moulitsas, 'Death Threats and Blogging' on Markos Moulitsas, *Daily Kos* (12 April 2007) <https://www.dailykos.com/story/2007/4/11/322169/->.

217 West, above n 203, 25.

218 Commonwealth, *Parliamentary Debates*, Federation Chamber, 8 February 2016, 930 (Nola Marino).

219 Woodlock, 'The Abuse of Technology', above n 41, 588.

220 Hand, Chung and Peters above n 40, 10. See also Jerry Finn and Teresa Atkinson, 'Promoting the Safe and Strategic Use of Technology for Victims of Intimate Partner Violence: Evaluation of the Technology Safety Project' (2009) 24 *Journal of Family Violence* 53.

or threatening to distribute, intimate images of the protected person.[221] To improve compliance, the police, courts, and legal practitioners should play an active role in ensuring that defendants understand the scope of the protection order made against them and that it extends to technology-facilitated abuse. In addition, it is important that police pursue complaints and, where the breach of an order also amounts to a criminal offence, the offender should also be charged for the substantive offence.[222]

The case law reviewed further highlights that the Australian family courts can assist in protecting victims from cyber-violence in family law proceedings through the use of section 121 of the *Family Law Act 1975* (Cth).[223] Legal practitioners should also inform their clients about the implications of breaching section 121. However, despite the potential of section 121 in preventing ex-partners from posting derogatory remarks online about their former partner, it is limited in that it only protects the privacy of victims and potential victims while the family law proceedings are on foot; it does not prevent cyber-violence before or after the proceedings. Additionally, the maximum penalty of imprisonment up to one year for breaching section 121 may be inadequate in some circumstances.

While the civil law does provide cyber-violence victims with limited remedies, such conduct requires a criminal response. Civil proceedings are a private matter between individuals that primarily aim to compensate complainants for any loss or harm caused and are therefore a weak response to conduct worthy of public condemnation. Criminal law remedies are primarily aimed at punishing the offender and play an important censuring function; '[i]t is the censure conveyed by criminal liability which marks out its special social significance'.[224]

Whether existing criminal laws can effectively deal with cyber-violence is arguable, particularly given the lack of research investigating the adequacies of existing laws in dealing with the various types of technology-facilitated abuse. However, there are several advantages in introducing legislation that specifically addresses cyber-violence. One benefit is that the criminal law can communicate to the public the boundaries of legally permissible behaviour and send the message that digital abuse will not be tolerated.[225] Specific offences would signal that cyber-violence is a serious offence in its own right, which would encourage police to pursue cyber-violence complaints, thereby increasing community confidence in the enforcement of the law. The penalties attached to the offences, if not trivial, may encourage victims to report the abuse because 'targeted individuals would be more likely to come forward since reporting such incidents would not seem fruitless'.[226]

---

221 Standing Committee on Law and Justice, above n 71, 37–8 [3.44].

222 See Douglas, 'Specific Domestic Violence Offence', above n 173, 438.

223 As discussed above, section 121 makes it an offence to publish any material identifying the parties to the proceedings, including posts on social media.

224 Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law* (Oxford University Press, 7th ed, 2013) 1.

225 See Citron, above n 212.

226 Ibid 412.

To facilitate law enforcement, the law needs to address evidentiary issues faced by police and victims when the abuse is facilitated by technology.[227] One suggestion put forward in the literature is for there to be agreements between website hosts and law enforcement agencies when investigating revenge porn complaints.[228] Yet, it is questionable whether implementing this suggestion is feasible given the global reach of the internet and the potential barrier in creating agreements with faceless offshore website hosts.

There have been discussions about giving internet service providers and website hosts greater power to remove suspected revenge porn images without the consent of the person who uploaded the material.[229] Suggestions have also been made to introduce legislation that would make it an offence for internet service providers and website hosts that fail to report such material to authorities, similar to the obligations imposed on providers and hosts under the Commonwealth *Criminal Code* regarding child abuse material.[230] This may be appropriate in light of anecdotal evidence that some website hosts have refused to remove images despite victims' requests.[231] However, the implications of imposing criminal liability on online intermediaries need to carefully be considered. In particular, if internet service providers were obligated to remove suspected revenge porn and other abusive content, it would be necessary to consider what penalty, if any, should be imposed for breaching their obligations.

It is also vital that any proposed legislation addresses indirect harassment and third-party abuse. This includes the situation where, for example, the abuser makes derogatory and threatening remarks publicly about the victim on their personal Facebook page.[232] Another scenario that should be addressed is where the abuser's family, friends, or new partner harasses the victim online.[233]

Nevertheless, the effectiveness of the law in tackling cyber-violence is significantly undercut if it is not accompanied by non-legal initiatives. Given that police are often a victim's first contact with the criminal justice system and bearing in mind the fundamental role they play in enforcing the law, 'there needs to be continuous training with police about the nature and dynamics of violence … [because] it seems as though technology-facilitated violence is treated as a lesser form of violence and we would challenge that'.[234] It would also be

---

227 See Legal and Constitutional Affairs References Committee, above n 3, [2.30]–[2.32] (discussing evidentiary issues for police in responding to revenge porn complaints).

228 See, eg, Henry and Powell, 'Sexual Violence in the Digital Age', above n 178, 411.

229 See especially Department of Communications and the Arts, above n 177.

230 *Criminal Code* s 474.25.

231 See Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, above n 141.

232 See, eg, *Janssen and Janssen [No 2]* [2016] FamCA 796; *Howlett and Morris* [2016] FamCA 710; *Bancroft and Lindsay* [2016] FCCA 1236; *Landin and Eades* [2013] FCCA 1276.

233 This was a common scenario that occurred in a number of cases reviewed, such as *Starcevic and Watson* [2016] FamCA 391; *Perceval and Perry* [2014] FCCA 911; *Sampson and North* [2014] FCWA 75; *Edwards Granger* [2013] FamCA 918. See also Dimond, Fiesler and Bruckman, above n 42.

234 Standing Committee on Law and Justice, above n 71, 22. See also Women's Legal Services NSW, 'Inquiry into Remedies for the Serious Invasion of Privacy in New South Wales' (Report of Proceedings before Standing Committee on Law and Justice, 30 October 2015) 46 (Ms Snell).

beneficial to offer this training to members of other professions who work closely with domestic violence victims.[235]

Additionally, there should be education campaigns directed at the general public that focus on perpetrator accountability and challenge victim-blaming attitudes. Such initiatives should make clear that victims are not expected to forsake their use of the internet and digital communication devices simply to avoid cyber-violence. At the same time, educational campaigns should offer information on how to minimise the chances of experiencing cyber-violence. To date, there have been some initiatives that have been of value to cyber-violence victims. For example, in the United States, an evaluation of the Technology Safety Project of the Washington Coalition Against Domestic Violence, which aimed to reduce the risk posed by abusers by educating victims about technology safety, found that the Project improved victims' confidence and knowledge about how to protect themselves from abusers online.[236]

More recently, Facebook, in collaboration with the National Network to End Domestic Violence, has shown initiative by launching in 2013 its *Privacy and Safety on Facebook: A Guide for Survivors of Abuse*.[237] The Guide, which is aimed at domestic violence victims, explains the advanced privacy controls and safety features available on Facebook, with the aim of assisting victims 'to stay connected through social media while continuing to maintain their safety'.[238] It also provides safety tips and outlines the options available if someone is using the site to harass, stalk, intimidate, or threaten users. This is an important step forward in light of the findings discussed above indicating that Facebook has become a popular platform used by abusers to harass their ex-partners.

During 2016, Telstra, an Australian telecommunications company, donated 20 000 smartphones to women experiencing domestic violence as a way to allow victims stay in touch with family and friends, as well as access online support services.[239] Part of the initiative involved educating victims on how to protect themselves from cyber-violence. Another notable initiative in Australia is the Office of the Children's eSafety Commissioner's launch of its eSafety Women website in 2016. The website aims to 'empower Australian women to take control of their online experiences'[240] by providing resources designed to help women minimise the risks of being a victim of technology-facilitated abuse.

235 Southworth et al, above n 74, 851–2.

236 Finn and Atkinson, above n 220.

237 National Network to End Domestic Violence, 'Privacy and Safety on Facebook: A Guide for Survivors of Abuse' (Guide, 2015) <https://www.facebook.com/notes/facebook-safety/ safety-and-privacy-on-facebook-a-guide-for-survivors-of- abuse/601205259900260>.

238 WESNET, *Facebook Privacy Guide* (1 September 2013) <http://wesnet.org.au/2013/09/facebook-privacy-guide/>.

239 WESNET, *Telstra Safe Connections Project* (2016) <http://wesnet.org.au/telstra/>.

240 Office of the eSafety Commissioner, *eSafetyWomen* (2017) <https://www.esafety.gov.au/Women>.

VII CONCLUSION

Domestic violence has been recognised around the world as a preventable issue demanding intervention. While governments have taken initiative in protecting victims from physical abuse, there needs to be greater focus on how to protect individuals physically, psychologically, and emotionally, both online and offline. The fact that the abuse occurs online should not diminish the seriousness of its impact on victims, nor should victims have to wait until the violence has travelled offline before there is intervention. Like other forms of cybercrime, a uniform response is required to address cyber-violence, rather than a patchwork of legislation throughout Australia.

The civil law, including civil protection orders, can (and should) provide cyber-violence victims with legal remedies against their abusers. However, there are considerable limitations of the civil system in dealing with cyber-violence and a criminal law response is needed. The value of the criminal law lays in its potential to convey the proper level of social condemnation cyber-violence deserves.

On a final note, the law should not be seen as the sole response to technology-facilitated abuse. Non-legal remedies tackling this issue should be introduced, including training of police and practitioners working with domestic violence about the impacts of technology-facilitated abuse, awareness campaigns directed at the general public, and support services for cyber-violence victims. Education is the key to changing societal attitudes and filling in the gaps in our understanding about the interrelationship between intimate partner abuse and technology. To improve victim support and implement effective preventative measures, further qualitative and quantitative research examining the phenomenon of cyber-violence is vital.