WOMEN'S LEGAL SERVICES NSW

Incorporating
Domestic Violence Legal Service
Indigenous Women's Legal Program

23 December 2015

Committee Secretary
Senate Legal and Constitutional Affairs Committee
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Dear Committee Secretary,

Inquiry into the phenomenon colloquially referred to as 'revenge porn' (non-consensual sharing of intimate images)

1. Women's Legal Services NSW (WLS NSW) thanks the Legal and Constitutional Affairs References Committee for the opportunity to comment on the phenomenon colloquially referred to as 'revenge porn', which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm inquiry.

2. WLS NSW is a community legal centre that aims to achieve access to justice and a just legal system for women in NSW. We seek to promote women's human rights, redress inequalities experienced by women and to foster legal and social change through strategic legal services, community development, community legal education and law and policy reform work. We prioritise women who are disadvantaged by their cultural, social and economic circumstances. We provide specialist legal services relating to domestic and family violence, sexual assault, family law, discrimination, victims support, care and protection, human rights and access to justice.

3. WLS NSW, along with many other organisations, has been overwhelmed during 2015 with calls for submissions to many Inquiries. While the community and institutional focus on domestic and family violence this year has been very welcome, it has also put additional pressures on already stretched community organisations such as ours. We say this only to indicate that although our submission to this Inquiry is brief this does not reflect the seriousness with which we take this issue.

4. Throughout 2015 WLS NSW has been engaged in the Recharge Project in partnership with the Women's Services Network (WESNET), Domestic Violence Resource Centre Victoria and the Australian Communications Consumer Action Network. It has involved a national survey on technology-facilitated stalking and abuse as well as the development of legal guides for each State and Territory and training materials for women escaping such abuse and those assisting them. The national survey found 98%

of the 546 domestic violence workers surveyed reported they had clients who had experienced technology-facilitated stalking and abuse.[1] This project extends the SmartSafe project (www.smartsafe.org.au) Australia-wide.

5. Over the past few years we have seen a significant increase in technology-facilitated stalking and abuse, that is, the use of technology, such as the internet, social media, mobile phones, computers, and surveillance devices, to stalk and perpetrate abuse on a person. In particular, we are seeing a concerning trend of technology being regularly used against women by perpetrators as a tactic within a wider context of domestic violence, including the non-consensual sharing of intimate sexual images.

6. We challenge the use of the terminology 'revenge porn' as it a misnomer, which focuses unduly on the actions of the victim, categorising their actions as pornography and encouraging victim blaming, rather than focusing squarely on real harm, which is caused by the perpetrator. As such, we prefer the term non-consensual sharing of intimate sexual images.

7. Laws must be developed to adequately respond to the misuse and abuse of new and emerging forms of technology.

8. Adequate and ongoing training must be provided for Police so the laws are enforced, and to social workers and caseworkers to assist women with responding to these situations, including technology safety planning.

9. We refer to the attached submissions we have made on this issue this year: Submission in response to the Exposure Draft of Criminal Code Amendment (Private Sexual Material) Bill 2015, dated 2 October 2015; and Submission in response to the Inquiry into remedies for the serious invasion of privacy in NSW, dated 29 September 2015.

10. In these submissions we provide extensive comments on the need to strengthen existing NSW and federal laws.

11. We also advocate for regular training for all Police about the law and the nature and dynamics of domestic violence including training in the gathering of evidence with respect to technology-facilitated stalking and abuse which includes the non-consensual sharing of intimate sexual images.

If you would like to discuss any aspect of this submission, please contact Liz Snell, Law Reform and Policy Coordinator on 02 8745 6900.

Yours faithfully,
Women's Legal Services NSW

Janet Loughman
Principal Solicitor

Encl: Submission in response to the Inquiry into remedies for the serious invasion of privacy in NSW (29 September 2015)
Submission in response to the Exposure Draft of Criminal Code Amendment (Private Sexual Material) Bill 2015 (2 October 2015)

[1] DVRCV/Delanie, *SmartSafe Survey for Australian Support Workers*, 2015.

WOMEN'S LEGAL SERVICES NSW

Incorporating
Domestic Violence Legal Service
Indigenous Women's Legal Program

1 October 2015

Mr Tim Watts MP
Federal Member for Gellibrand
Australian Labor Party

By email: Tim.Watts.MP@aph.gov.au

Dear Mr Tim Watts and Ms Terri Butler,

Exposure Draft of Criminal Code Amendment (Private Sexual Material) Bill 2015

Introduction

1. Women's Legal Services NSW (WLS NSW) thanks the Australian Labor Party for the opportunity to comment on the Exposure Draft of the *Criminal Code Amendment (Private Sexual Material) Bill 2015.*

2. WLS NSW is a community legal centre that aims to achieve access to justice and a just legal system for women in NSW. We seek to promote women's human rights, redress inequalities experienced by women and to foster legal and social change through strategic legal services, community development, community legal education and law and policy reform work. We prioritise women who are disadvantaged by their cultural, social and economic circumstances. We provide specialist legal services relating to domestic and family violence, sexual assault, family law, discrimination, victims support, care and protection, human rights and access to justice.

3. WLS NSW is currently engaged in the Recharge Project in partnership with the Women's Services Network (WESNET), Domestic Violence Resource Centre Victoria and the Australian Communications Consumer Action Network. It has involved a national survey on technology-facilitated stalking and abuse as well as the development of legal guides for each State and Territory and training materials for women escaping such abuse and those assisting them. The national survey found 98% of the 546 domestic violence workers surveyed reported they had clients who had experienced technology-facilitated stalking and abuse.[1] This project will extend the SmartSafe project (www.smartsafe.org.au) Australia-wide.

[1]DVRCV/Delanie, *SmartSafe Survey for Australian Support Workers*, 2015.

4. Over the past few years we have seen a significant increase in technology-facilitated sexual violence. We agree with the Discussion Paper that current civil and criminal laws dealing with this use of technology are unclear and inadequate.

5. Laws must be developed to adequately respond to the misuse and abuse of new and emerging forms of technology. Adequate and ongoing training must be provided for Police so the laws are enforced, and to social workers and caseworkers to assist women with responding to these situations.

6. We note that some people who experience violence prefer the term 'victim' and others prefer the term 'survivor'. In this submission we use the term 'victim' which is intended to be inclusive of both victims and survivors.

Overview

7. In summary we recommend:

7.1 The creation of a specific criminal offence where intimate sexual images are actually or threatened to be shared without consent.

7.2 It should be irrelevant for any offence where threats are made to share private sexual material, whether the material actually exists. This should be explicitly stated in any legislation.

7.3 Consistent and uniform legislation should be enacted in each Australian State and Territory to mirror any enacted Commonwealth offence, so as to capture when these behaviours occur without the use of a carriage service.

7.4 It should be an offence to threaten to share private sexual images of a third party without consent.

7.5 There should be greater consideration of the impact of non-sexual material being shared or threatened to be shared when it occurs within a context of domestic violence.

7.6 Sections 474.24D(2) and 474.24D(3) should be amended so they begin: *'The material must depict, or be stated or implied to depict:…'*

7.7 The exceptions in section 474.24D(4) should be considered further and amended.

7.8 The definition in section 474.24D(3)(c) ought to be extended to state 'for a female or a transgender or intersex person who identifies as a female—the breasts' to acknowledge gender and sex diversity.

7.9 The offence be based on harm and distress caused (or at risk of being caused) rather than the defendant's intention.

7.10 Section 474.24E(1)(e) be clarified so that subsections (i) and (ii) both be available whether the private sexual material was actually or threatened to be shared.

7.11 'Risk of harm' should be an objective test based on whether a reasonable

person would consider there to be a risk, with a subjective element so it is considered within the circumstances of the case.

7.12 Any offence explicitly states that the court may order a take down, deliver up order or similar order.

7.13 Further consideration be made to the necessity of a media defence as outlined in section 474.24H.

7.14 It be explicitly stated that for the purpose of consent, upon ending a relationship, any prior consent relating to private sexual material is impliedly withdrawn.

7.15 Consideration be given to the potential impact of this offence on minors.

Threats to share private sexual material

Do you support the creation of a specific criminal offence in relation to "revenge porn" threats?

8. WLS NSW supports the creation of a specific criminal offence where private sexual images are actually shared without consent or threatened to be shared without consent.

9. It should be irrelevant for any offence where threats are made to share private sexual material, whether the material actually exists. For example, we have had clients where the other party has threatened to share intimate still or moving images that were allegedly filmed without knowledge or consent. Therefore, the client has not known whether the intimate still or moving images actually exist, however, their fear of distress and harm is real. It should be immaterial if the material does not actually exist or if the threats were empty. We recommend this should be explicitly stated in the Bill.

10. We also suggest consistent and uniform legislation be enacted in each Australian State and Territory to mirror any enacted Commonwealth offence, so as to capture when this behaviour occurs without the use of a carriage service. The behaviour should be criminalised irrespective of whether it is technology-facilitated or in-person behaviour.

Should the offence apply to a situation where a person (Person A) makes threats to a person (Person B) that they will share a private sexual image or recording of another person (Person C)?

11. WLS NSW supports the offence extending to situations where threats are made to share intimate images of a third party.

The meaning of "private sexual material"

What should be the meaning of "private sexual material"?

12. We note that the definition of 'private sexual material' in section 474.24D of the Bill is limited. It does not capture intimate material of a non-sexual nature used to shame, humiliate or control a woman within the context of domestic violence. For

example an image of a woman without her religious headscarf can cause harm to a victim if such an image is shared or threatened to be shared without consent.

13. We recommend greater consideration of the impact of non-sexual material being shared or threatened to be shared when it occurs within a context of domestic violence, and in particular, the potential impact on culturally diverse women. We recommend there should be some recognition of the serious impact sharing or threatening to share such images could have on the victim.

14. The meaning of 'private sexual material' is also limited by the need for the material to depict at least one of the factors listed in section 474.24D(3). Our concern is a practical consideration that commonly arises in scenarios where a person is threatening to share private sexual material. For many of our clients who have received such threats, it may be that the threatened image does not in fact exist or they have not seen the image to know what it in fact depicts. For example, where a person threatens to share private sexual material of the victim they say they covertly recorded without the victim's consent, the harm caused is just as real, even where that person is lying about the existence of this private sexual material. In such cases, if you only capture scenarios where you can prove the material *actually* depicts something listed in section 474.24D(4), you would significantly impede the application of this offence. We therefore recommend amending sections 474.24D(2) and 474.24D(3) so they begin:

'The material must depict, or be stated or implied to depict:…'

15. By extending the definition to situations where the material is stated or implied to depict private sexual material, this will assist police to overcome resource intensive and onerous evidentiary limitations. If threats are made over a carriage service that private sexual material will be non-consensually shared, the police should be able to lay charges without needing to obtain a copy of that material. To have the section otherwise worded would suggest that to prosecute, the police would need to show what was depicted, and therefore, may need to obtain warrants to seize electronic devices of the offender and utilise computer forensics to find the alleged material. This is likely to be too resource intensive to be practical and a deterrent to investigating and prosecuting matters.

16. We note the limitations on material being 'private sexual material' in section 474.24D(4) where the material has been altered or combines material in certain circumstances. It appears the intention of this exemption envisages situations where, for example, a woman's head is doctored onto a photo of another woman's naked body. We question why it is necessary to have such a limitation.

17. We now live in a digital age where electronic devices have built in editing functionality as well as the wide availability of Apps, software and programs for images to be altered and edited with incredible ease. A layperson now has at their fingertips the capabilities to edit an image and make it look convincing and real as if professionally done. If a victim's head is convincingly photo-shopped onto an image of a naked woman in a sexual act so a reasonable person would think the person depicted is the victim, and this were distributed using a carriage service, how is the harm caused less real? We therefore recommend reconsidering the exceptions in section 474.24D(4), in particular

474.24D(4)(b)(iii).

How can we ensure that the offence is inclusive of all persons regardless of gender or gender identity?

18. We believe that any legislation should be inclusive of sex and gender diversity.

19. To avoid any doubt that the section 474.24D(3)(c) definition of 'private sexual material' to include 'the breasts of a female person' includes transgender and intersex people who identify as a female, we recommend adopting wording similar to the approach in section 61B(5) of the *Crimes Act 1900* (ACT). This provision prohibits using a device to observe or capture visual data in certain circumstances including:

> *For a female or a transgender or intersex person who identifies as a female—the breasts.*

Intention of perpetrators

How can we ensure that the offence applies to the range of intentions, motivations or reasons for sharing private sexual images and recordings without consent?

20. Section 474.24E does not depend upon the defendant's intention, but rather, focuses on the actual or potential harm or distress caused to the victim. The benefit of this approach is that it is not necessary to prove why a defendant shared or threatened to share private sexual material, which can be for varied reasons such as to cause harm, to humiliate, to gain social status, for sexual gratification or to receive monetary reward.[2] We generally agree with this approach of focusing on harm or distress to constitute an offence.

21. However, It is not entirely clear how section 474.24E(1)(e) will operate where it states:

Either:

(i) the conduct mentioned in paragraph (a) causes distress or harm to a subject of the material; or

(ii) there is a risk that the conduct mentioned in paragraph (a) will cause distress or harm to a subject of the material;

22. It is not clear if these subsections are an either/or approach in any situation or if subsection (i) is intended to only apply where the private sexual material is actually shared and subsection (ii) is intended for threatened publication.

23. We recommend that subsections (i) and (ii) above should be available in any situation whether the private sexual material was actually shared or threatened to be shared. For example, where a woman is in a domestic violence relationship and due to fear, coercion or control, states distress or harm was not caused, the

[2] See Nicola Henry and Anastasia Powell, 'Sexual Violence and Harassment in the Digital Age', Presentation to Women's Legal Services NSW, 24 April 2015 www.wlsnsw.org.au/wp-content/uploads/NSW-Womens-Legal-Services-Presentation-24_April_2015.pdf

prosecution could instead rely upon the risk that the conduct would cause distress or harm which is a lower threshold test.

24. We recommend 'risk of harm' should be an objective test based on whether a reasonable person would consider there to be a risk, but also with a subjective element so it is considered within the circumstances of the case.

25. Further, it is difficult to imagine how the prosecution will be able to successfully prove that there was a *risk* the conduct would cause distress or harm when section 474.24E(4)(b) states '*a person's conduct does not cause distress merely because that is a natural and probable consequence of the conduct.'* This may need further consideration.

How can we ensure that the offence is responsive to the range of effects of this behaviour on victims?

26. We recommend that any offence explicitly state that the court may order a take down, deliver up order or similar order be made. This would be similar to section 26E(3) of the *Summary Offences Act 1953 (SA),* which allows for the court to order the forfeiture of records of still or moving images in filming offences. This would provide a practical form of redress for victims where, for example, the image remains online and it is within the defendant's control to remove the content.

Protections for the media

How can we strike the right balance between ensuring protections for the media whilst also protecting victims?

27. We question the need for a defence to excuse the media posting private sexual material of a victim without consent, and cannot envisage circumstances where this would be justified. We recommend further consideration be made to the necessity of the defence as outlined in section 474.24H(4) of the Bill.

The meaning of "consent"

How should consent be defined in the context of the sharing of private sexual material?

28. We support the inclusion of 'reckless as to the subject's lack of consent' as outlined in s474.24E(1)(d). Further to the explanation of consent in section 474.24E(3) of the Bill we recommend it be explicitly stated that for the purpose of determining consent, upon ending a relationship, any prior consent relating to private sexual material is impliedly withdrawn.

29. Disability, age, domestic violence context, duress and deception are other relevant factors to consider when looking at consent.

Other relevant consideration

Minors

30. Technology-facilitated sexual violence is a growing issue for young women under 18 years of age. This raises a number of issues where either the victim or the perpetrator are minors.

31. We recommend greater consideration should be given to the potential impact of this offence on minors.

If you would like to discuss any aspect of this submission, please contact Alex Davis, Solicitor or Liz Snell, Law Reform and Policy Coordinator

Yours faithfully,
Women's Legal Services NSW

Janet Loughman
Principal Solicitor

WOMEN'S LEGAL SERVICES NSW

Incorporating
Domestic Violence Legal Service
Indigenous Women's Legal Program

29 September 2015

The Director
Standing Committee on Law and Justice
Parliament House
Macquarie St
Sydney NSW 2000

By email: lawandjustice@parliament.nsw.gov.au

Dear Director,

Inquiry into remedies for the serious invasion of privacy in New South Wales

Introduction

1. Women's Legal Services NSW (WLS NSW) thanks the Standing Committee on Law and Justice for the opportunity to comment on the Inquiry into remedies for the serious invasion of privacy in New South Wales.

2. WLS NSW is a community legal centre that aims to achieve access to justice and a just legal system for women in NSW. We seek to promote women's human rights, redress inequalities experienced by women and to foster legal and social change through strategic legal services, community development, community legal education and law and policy reform work. We prioritise women who are disadvantaged by their cultural, social and economic circumstances. We provide specialist legal services relating to domestic and family violence, sexual assault, family law, discrimination, victims support, care and protection, human rights and access to justice.

3. WLS NSW is currently engaged in the Recharge Project in partnership with the Women's Services Network (WESNET), Domestic Violence Resource Centre Victoria and the Australian Communications Consumer Action Network. It has involved a national survey on technology-facilitated stalking and abuse as well as the development of legal guides for each State and Territory and training materials for women escaping such abuse and those assisting them. The national survey found 98% of the 546 domestic violence workers surveyed reported they had clients who had experienced technology-facilitated stalking and abuse.[1] This project will extend

[1] DVRCV/Delanie, *SmartSafe Survey for Australian Support Workers*, 2015.

the SmartSafe project (www.smartsafe.org.au) Australia-wide.

4. Over the past few years we have seen a significant increase in technology-facilitated stalking and abuse (also referred to as technology-facilitated domestic violence), that is, the use of technology to shame, humiliate, intimidate, harass and abuse women. Current civil and criminal laws dealing with this use of technology are unclear and inadequate.

5. Laws must be developed to adequately respond to the misuse and abuse of new and emerging forms of technology. Adequate and ongoing training must be provided for Police so the laws are enforced, and to social workers and caseworkers to assist women with responding to these situations, including technology safety planning.

Overview

6. The focus of our submission is on adequately addressing these issues, including through strengthening protection orders through amendments to the *Crimes (Domestic and Personal Violence) Act*; strengthening the criminal law response; as well as civil remedies.

7. We also note different jurisdictions around Australia have been discussing the importance of exclusion zones, for example, outside abortion clinics and health clinics providing reproductive health services, which are designed to balance the right of freedom of speech with the right to privacy. This issue is also briefly discussed.

8. In summary we recommend:

   8.1 Recognition of the many forms of technology-facilitated stalking and abuse discussed in this submission as forms of violence against women.

   8.2 That the principles guiding privacy reform include the right to equality and the right to security of person.

   8.3 The creation of exclusion zones around abortion clinics and health clinics providing reproductive services be considered in the context of this Inquiry.

   8.4 Updated consultation on the statutory review of the *Crimes (Domestic and Personal Violence) Act 2007 (NSW),* including an exposure draft bill that contemplates the realities of technology-facilitated stalking and abuse.

   8.5 Including an apprehended violence order (AVO) prohibiting the defendant from attempting to locate, asking someone else to locate, follow or keep the protected person under surveillance.

   8.6 Including an AVO prohibiting the actual or threatened publishing or sharing of images or videos of the protected person of an intimate nature.

   8.7 Including a provision allowing AVOs to be used for an injunctive order such as a take down order or deliver up order.

   8.8 A review by the Australian Communications and Media Authority ('ACMA') into the current charges of service providers under s 314 of the *Telecommunications*

Act 1997 (Cth).

8.9 Consideration be given to establishing an encrypted electronic device in all NSW Police stations that could be used to quickly and cheaply scan a person's device for spyware or malware; access social media accounts without firewalls; and extract relevant data in an admissible form.

8.10 Regular training for all Police about the law and the nature and dynamics of domestic violence include training in the gathering of evidence with respect to technology-facilitated stalking and abuse.

8.11 Creating new criminal sanctions in NSW to address the actual or threatened distribution without consent of moving or still images of an intimate sexual nature.

8.12 Any new criminal sanctions introduced should consider the potential impact of the laws on minors.

8.13 The establishment of a NSW and federal statutory cause of action for serious invasions of privacy.

8.14 A statutory tort for serious invasions of privacy allow for damages to be awarded for emotional harm.

8.15 If a statutory tort for serious invasions of privacy is not introduced, the courts should be empowered by legislation to award compensation for emotional distress in cases of breach of confidence.

8.16 If a statutory tort for serious invasions of privacy is created, having a schedule in accompanying regulations which sets out a clear and simple take down process.

8.17 If a new criminal offence is created to address the distribution or threatened distribution of intimate sexual images there needs to be a corresponding amendment so this new offence is considered a personal violence offence for the purposes of NSW Victims Support.

8.18 In determining reasonable expectations of privacy, include the Australian Law Reform Commission's *Serious Invasions of Privacy in the Digital Era Final Report* ('ALRC's Final Report') Recommendation 6-2 factors as well as an additional factor 'the nature of the relationship between the parties'.

8.19 A NSW serious invasion of privacy tort takes into account damage caused as a result of intentional emotional harm other than a psychiatric illness.

8.20 There be a 'serious' threshold for any proposed new NSW tort of invasion of privacy.

8.21 The seriousness threshold be met where a person shares intimate images of a non-sexual nature within the context of domestic violence, such as an image of a woman without her religious headscarf which may be highly distressing or harmful to that woman.

8.22 In any defence to a statutory cause of action for serious invasions of privacy that

the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property that there be a requirement the act or conduct was proportionate, or necessary and reasonable.

8.23 There be a public interest defence and balancing of rights defence for a statutory cause of action for serious invasions of privacy.

8.24 A NSW statutory cause of action for serious invasions of privacy should provide for compensatory damages, including for emotional distress and in some circumstances that damages also include aggravated and exemplary damages.

8.25 Local Courts should be given the power to grant stand-alone injunctive orders, such as take down orders and/or deliver up orders.

8.26 Other than monetary remedies and injunctions, we support the list of remedies recommended in the ALRC's *Final Report* as being appropriate for a NSW statutory cause of action. This includes an order requiring the defendant to apologise to the plaintiff;[2] a correction order;[3] an order for delivery up, destruction or removal of material;[4] a declaration.[5]

8.27 There be sanctions for failure to comply with an order without reasonable excuse.

8.28 Provision should be made to make legal processes accessible for example, technical assistance for impecunious claimants, availability of legal aid, limited cost provisions in lower courts or tribunals, court and tribunal fee waivers.

8.29 An independent body should be able to bring proceedings on behalf of an individual or individuals.

8.30 Referrals to mediation or conciliation are only made after an assessment that such a referral is appropriate, including that an option of lawyer-assisted alternative dispute resolution be available where there is an imbalance of power such as in cases of domestic violence and sexual assault; face to face and regional services for Aboriginal and Torres Strait Islander people, people from culturally and linguistically diverse backgrounds and people with disability.

Terminology

9. While technology-facilitated stalking and abuse is not currently explicitly defined in legislation in NSW, we understand it to include the following behaviours, which are not intended to be exhaustive: tracking a person's location through GPS and other devices without the person's consent; using covert recording devices including spyware and cameras to monitor or gather private information; accessing a person's

[2] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-11
[3] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-10.
[4] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-9
[5] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-12

computer, phone or other device without their knowledge or consent; monitoring or unauthorised access of a person's social media accounts, email accounts, internet dating accounts and other accounts; changing or demanding passwords; sending large volumes of electronic communications to threaten, intimidate or harass; impersonating the person online; sharing or threatening to share or publish intimate still or moving images or private information in a public forum, on online chat rooms, blogs, websites or with people whom the person knows, including for the purpose of humiliating or controlling the person.[6]

10. The expression 'intimate sexual images' is intended to capture images of a sexual nature and images where the person appears naked or partially naked which may have been taken with consent but are shared without consent.

11. The expression images of an 'intimate nature' is intended to capture the use of intimate sexual images as well as images of a non-sexual nature used to shame, humiliate or control a woman within the context of domestic violence. For example an image of a woman without her religious headscarf can cause harm to a victim if they are shared or threatened to be shared without consent. We urge the Standing Committee to give these forms of invasions of privacy serious consideration and to recognise the serious impact sharing images such as these could have on the victim.

12. We note that some people who experience violence prefer the term 'victim' and others prefer the term 'survivor'. In this submission we use the term 'victim' which is intended to be inclusive of both victims and survivors.

Human rights framework

Violence against women

13. Violence against women is one of the most widespread human rights abuses. In Australia:

14. Domestic violence puts more women aged 15-44 years at risk of ill health and premature death than any other risk factor;[7]

15. One in three Australian women will report being a victim of physical violence and almost one in five will report being a victim of sexual violence in their lifetime according to the Australian Bureau of Statistics.[8] We also know that family violence and sexual assault are under reported.

16. Whatever the form violence takes, it has serious and often devastating consequences for victims, their extended families and the community.

---

[6] This list, adapted from the list of actions Women's Legal Services Victoria and the Domestic Violence Resource Centre Victoria proposed, should be included in a statutory cause of action for serious invasions of privacy. See Women's Legal Services Victoria and the Domestic Violence Resource Centre Victoria, *Submission in response to the Australian Law Reform Commission's Inquiry into serious invasions of privacy in the digital era*, 2013.

[7] VicHealth and Department of Human Services, *The Health Costs of Violence. Measuring the Burden of Disease*
Caused by Intimate Partner Violence – A Summary of Findings, 2004 at 10.

[8] Australian Bureau of Statistics (2005) Personal Safety Survey, ABS Cat. No. 4906.0, Canberra: Commonwealth of Australia. (ABS 2005).

17. Violence against women also comes at an enormous economic cost. Research released by the Government shows that each year violence against women costs the nation $13.6 billion.[9] This figure is expected to rise to $15.6 billion by 2021.

18. CEDAW Committee *General Comment No 19* makes clear that gender-based violence is a form of discrimination within Article 1 of *CEDAW*[10] and Article 2 of *CEDAW* obliges state parties to legislate to prohibit all discrimination against women. Such violence is a violation of the rights to life, to equality, to liberty and security of person, to the highest standard attainable of physical and mental health, to just and favourable conditions of work and not to be subjected to torture and other cruel, inhuman, or degrading treatment or punishment.[11]

19. The use of technology to shame, humiliate, intimidate, harass and abuse women is a form of gendered violence that must be urgently addressed.

20. Under international human rights, States are required to act with due diligence to protect, promote and fulfill their human rights obligations.[12]

21. Significantly, States may be held responsible for private acts, such as domestic and family violence, if they fail to act with due diligence to prevent, investigate or punish acts of violence.[13]

22. Human rights are based on the inherent dignity of the person.

Balancing of human rights

23. While there is a right to freedom of opinion and expression, the *International Covenant on Civil and Political Rights* also acknowledges that with rights come responsibilities, including 'respect of the rights or reputations of others'.[14]

24. The *International Covenant on Civil and Political Rights* (ICCPR) states that restrictions on the right to freedom of opinion and expression can only be limited to the extent 'provided by law and are necessary'.[15] We submit that the sharing of intimate images with third parties without informed consent and the other forms of technology-facilitated stalking and abuse outlined at paragraph 9 above; constitute such circumstances.

---

[9] KPMG, The Cost of Violence against Women and their Children. Safety Taskforce , Department of Families,
Housing, Community Services and Indigenous Affairs, Australian Government, 2009.

[10] CEDAW Committee, *General Recommendation No. 19: Violence against Women*, UN Doc A/47/38 (1992), para 7.

[11] *CEDAW Committee General Comment No 19,* para 7. See also: *International Covenant on Civil and Political Rights (ICCPR)* ratified by Australia on 13 August 1980, Articles 2, 3, 7 and 26; *International Covenant on Economic, Social and Cultural Rights (ICESC*R), ratified by Australia on 10 December 1975, Articles 3 and 10.

[12] Human Rights Committee, *General Comment No. 31*, CCPR/C/74/CRP.4/Rev.6, para. 8; Committee on the
Rights of the Child, *General Comment No. 5*, CRC/GC/2003/5, 27 November 2003, para. 1; Committee on Economic, Social and Cultural Rights, General Comment No. 14, E/C.12/2000/4 (2000), para. 33.

[13] *CEDAW General Comment 19: Violence against Women*, as contained in UN Doc A/47/38 (1992) at paragraph 9.

[14] ICCPR, Article 19(3)(a)

[15] ICCPR Article 19(3)

25. Additional relevant human rights include the right to equality, which includes the right to be free from violence; the right to security; as well as the right to privacy.

26. Discrimination against women is both a cause and consequence of violence against women. The *Convention on the Elimination of All forms of Discrimination against Women* (CEDAW) calls for the incorporation of the principle of the equality of women and men 'through law and other appropriate means'.[16] This should occur through positive measures, such as the promotion of substantive equality, as well as through prohibitions on all forms of discrimination against women. Sanctions are also required in the event these rights are violated.

27. CEDAW General Recommendation No 12 recommends States' periodic reports to the Committee include information about 'the legislation in force to protect women against the incidence of *all* kinds of violence in everyday life' (emphasis added). This should include the perpetration of violence against women through the use of technology.

28. Article 9 of the *International Covenant on Civil and Political Rights* provides the right to liberty and security of person. We welcome General Comment No. 35 on Article 9 which replaces General Comment No 8. This General Comment states 'the right to security of person protects individuals against intentional infliction of bodily or mental injury, regardless of whether the victim is detained or non-detained'.[17] We submit protection from mental injury includes protection from psychological harm, such as through the use of technology to shame, humiliate, intimidate, harass and abuse women. Significantly, General Comment No 35 proposes a requirement for State parties to 'respond appropriately to patterns of violence against categories of victims … such as violence against women'.[18]

29. Article 17 of the *International Covenant on Civil and Political Rights* provides a right to privacy. General Comment No 16 on Article 17: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation states 'the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law'.[19]

30. Further, 'effective measures have to be taken by States to ensure that information concerning a person's private life … is never used for purposes incompatible with the Covenant'.[20]

31. We strongly argue that using technology as a form of violence against women is incompatible with the ICCPR.

32. In addition to Australia's human rights obligations, we see no public interest in permitting the sharing of intimate images without informed consent or in the other

[16] CEDAW, Article 2
[17] Human Rights Committee, *General Comment No. 35 on Article 9: Liberty and security of person,* CCPR/C/GC/35 16 December 2014 at para 9.
[18] Human Rights Committee, *General Comment No. 35 on Article 9: Liberty and security of person*, CCPR/C/GC/35 16 December 2014 at para 9.
[19] Human Rights Committee, *General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (Art. 17) 4 August 1988, para 10.
[20] Ibid.

activities outlined in paragraph 9.

Exclusion zones outside abortion clinics

33. Women seeking to access abortion clinics in NSW are being subjected to violence, intimidation and humiliation in breach of their privacy, from protestors seeking to express their right to freedom of expression. We submit that it is a relevant issue for this Inquiry to consider the balancing of the right to privacy with freedom of speech. An appropriate, balanced public policy approach, we submit is to legislate for exclusion zones ie prescribed areas outside abortion clinics and health clinics providing reproductive health services where public protest is prohibited. An exclusion zone does not prohibit freedom of speech but prevents intentional harm against individuals from occurring in a set space around a clinic and makes this space free from violence, intimidation and humiliation. This approach balances the right to privacy and freedom from violence, with freedom of speech.

34. We note the interest in creating an exclusion zone in Albury[21] and recommend the creation of exclusion zones be considered in the context of this inquiry.[22]

Term of Reference (a): Adequacy of existing remedies for serious invasions of privacy

35. Current NSW and federal criminal and civil laws dealing with technology-facilitated stalking and abuse are unclear, inadequate and inappropriate, often requiring old laws to be creatively interpreted to adapt to new technologies the legislation had not originally contemplated.

36. This section will examine the adequacy or otherwise of NSW protection order legislation and criminal law legislation.

Strengthening Apprehended Domestic Violence Orders (ADVO) legislation

37. The *Crimes (Domestic and Personal Violence) Act 2007* (NSW) (the *Crimes (DPV) Act*) is currently under review in NSW. The review commenced in 2011 and has not yet been finalised. Given the fast changing impact of technology on the means by which domestic violence is orchestrated, it is imperative that community consultation on any proposed changes to the *Crimes (DPV) Act* be re-invigorated prior to a Bill being put to Parliament. Further, the NSW Department of Justice and the government's Behavioural Insights Unit are currently reviewing the wording of NSW apprehended violence orders, which are based on s 35 of the *Crimes (DPV) Act.* These review processes need to be aligned, and the subject of further community consultation.

38. We therefore recommend an exposure draft of a bill to amend the *Crimes (DPV) Act* be prepared for comment which contemplates the realities of technology-facilitated stalking and abuse.

39. If the *Crimes (DPV) Act* were strengthened, this could provide a cost effective,

[21] 'Advocates push for greater medical privacy for women', PM, 14 January 2015 accessed on 20 September 2015 at: http://www.abc.net.au/pm/content/2015/s4162322.htm

[22] We also note the use of another term to describe exclusion zones in Albury, namely privacy zones.

accessible and efficient means of dealing with serious invasions of privacy involving technology-facilitated stalking and abuse.

40. At present, most behaviours related to technology-facilitated stalking and abuse must be interpreted as acts of 'intimidation' to fall within the provisions of the *Crimes (DPV) Act.* Section 7 of the *Crimes (DPV) Act* defines intimidation of a person to mean:

> (1) (*a) conduct amounting to harassment or molestation of the person, or*
>
> *(b) an approach made to the person by any means (including by telephone, telephone text messaging, e-mailing and other technologically assisted means) that causes the person to fear for his or her safety, or*
>
> *(c) any conduct that causes a reasonable apprehension of injury to a person or to a person with whom he or she has a domestic relationship, or of violence or damage to any person or property.*
>
> *(2) For the purpose of determining whether a person's conduct amounts to intimidation, a court may have regard to any pattern of violence (especially violence constituting a domestic violence offence) in the person's behaviour.*

41. While the legislation contemplates a suite of technologies within s 7(1)(b), this is limited to situations where they are used to cause 'fear for safety.'

42. Section 7(1)(c) refers to conduct that causes 'a reasonable apprehension of injury' to a person or person with whom he or she has a domestic relationship. While some would argue 'a reasonable apprehension of injury' includes psychological injury, such as humiliation, this has not been our experience.

43. Other aspects of harassment which are not currently being effectively captured within this provision include: the unauthorised use of surveillance devices; impersonating a person online; or sharing or threatening to share intimate images online.

44. Many of our clients experiencing technology-facilitated stalking and abuse face additional barriers through police attitudes towards their complaints. This can be that the harassment is somehow considered less harmful when online or that proving the offender is responsible is too burdensome once technology is involved. While training has a vital role to play, clearer legislation can help shape understanding and encourage people including police to appreciate that the impacts of technology-facilitated stalking and abuse can be as harmful, and sometimes more harmful than in-person behaviours.[23]

45. We submit that there needs to be a more clearly defined meaning of harassment. This could be assisted with a non-exhaustive list of examples.

46. We would consider 'unauthorised surveillance' to be invasive, coercive and controlling behaviour that exploits a power imbalance in a relationship and should be clearly prohibited in the legislation as a form of intimidation. This would be consistent

[23] Stonard, K.E., Bowen, E., Walker, K., & Price, S.A. "They'll always find a way to get to you": Technology use in adolescent romantic relationships & its role in dating violence and abuse. *Journal of Interpersonal Violence* (2015) 1-35.

with the objects of the Act set out in section 9. Further, unauthorised surveillance is acknowledged as a form of domestic violence in equivalent protection order legislation in South Australia[24] and Queensland.[25]

47. If unauthorised surveillance were to be added to the definition of intimidation, we recommend it be a defined term. A similar definition of 'unauthorised surveillance' in section 8(5) of the *Domestic and Family Violence Protection Act 2012* (Qld) could be adopted. This section reads:

> *unauthorised surveillance, of a person, means the unreasonable monitoring or tracking of the person's movements, activities or interpersonal associations without the person's consent, including, for example, by using technology. Examples of surveillance by using technology—*
>
> - *reading a person's SMS messages*
> - *monitoring a person's email account or internet browser history*
> - *monitoring a person's account with a social networking internet site*
> - *using a GPS device to track a person's movements*
> - *checking the recorded history in a person's GPS device*

48. Importantly, the above definition acknowledges the monitoring or tracking must be 'unreasonable'. We would suggest this definition contemplates circumstances where surveillance may be reasonable, such as protecting one's immediate safety or lawful interest. For example, where a victim of domestic violence downloads a phone app to record conversations to prove the other party is breaching an AVO or threatening or intimidating them, this should not be captured as 'unauthorised surveillance' because it is reasonable in the circumstances. If unauthorised surveillance were included in the Act, it is critical that consideration be given to this so a victim protecting themselves or their children from domestic violence does not end up as an ADVO defendant.

49. We believe it is important the legislation be amended to reflect the realities of technology-facilitated stalking and abuse so it is clearer that these behaviours are a form of intimidation. One option would be to broaden the definition of 'intimidation' so s 7(1)(a) were drawn out into three subsections to read:

> *(a) conduct amounting to harassment (including by telephone, telephone text messaging, e-mailing and other technologically assisted means), or*
>
> *(aa) conduct amounting to unauthorised surveillance, or*
>
> *(aaa) conduct amounting to molestation of the person …*

50. Section 8 of the *Crimes (DPV) Act* defines stalking to include:

> *(1) the following of a person about or the watching or frequenting of the vicinity of, or an approach to, a person's place of residence, business or work or any place that a person frequents for the purposes of any social or leisure activity.*
>
> *(2) For the purposes of determining whether a person's conduct amounts to*

[24] *Intervention Orders (Prevention of Abuse) Act 2009* (SA), s 8(4)(k).
[25] *Domestic and Family Violence Protection Act 2012* (Qld), s 8(5).

stalking, a court may have regard to any pattern of behaviour (especially violence constituting a domestic violence offence) in the person's behaviour.

51. It is our experience that this is being interpreted as physical stalking.

52. The definition of stalking should be amended to include the words 'by any means whatsoever' so as to also include technology-facilitated stalking.

53. The wider definitions of these terms should allow any such practices to be prohibited under the mandatory orders of an AVO.

54. We further recommend including the conditions below to cover surveillance/technology-facilitated stalking and the sharing of intimate images in AVOs:

a) The defendant must not attempt to locate, ask someone else to locate, follow or keep the protected person under surveillance.

b) The defendant is prohibited from directly or indirectly, publishing, sharing and threatening to publish or share images or videos of the protected person of an intimate nature.

55. As part of the *Crimes (DPV) Act* legislative review process consideration should be made as to whether these additional conditions are included as part of the mandatory orders or standard additional orders.

56. By including additional order (b) above, arguably, the failure to remove material that is published online could be deemed a continuing publication and therefore a breach of the order. This could have an equivalent effect of a takedown order and be a quick, accessible and efficient means to get intimate images removed online where the defendant has the ability to remove them.

57. Currently the *Crimes (DPV) Act* allows for orders to be made that are prohibitive or restrictive,[26] but does not allow for AVO conditions that impose a positive obligation.[27] Ancillary property recovery orders are restricted to property that is clearly the property of one party.[28]

58. An option is to amend the *Crimes (DPV) Act* so that an order, such as a take down order or deliver up order, can be made at the same time as an Apprehended Violence Order (AVO) (domestic or personal). We envisage an application for these orders could be made at anytime throughout the AVO proceeding, as is the case for ancillary property orders.

59. A disadvantage of the application being tied to the AVO application is the need for the Applicant to establish fear on a reasonable basis for an AVO to be made. This may mean that a take down or deliver up order fails only because fear is not proven.

60. This further supports our argument above that the definition of intimidate in the *Crimes (DPV) Act* be amended to clarify the scope of harassing behaviour so fear of

[26] *Crimes (Domestic and Personal Violence) Act 2007* (NSW), s 35.
[27] See, eg, *Domestic and Family Violence Act 2007* (NT), s 21.
[28] *Crimes (Domestic and Personal Violence) Act 2007* (NSW), s 37.

this type of harassment can be more easily established.

NSW Police response

61. Based on the experience of our clients, sometimes NSW Police dismiss technology-facilitated stalking and abuse or tell women there is insufficient evidence to apply for an ADVO or that the investigation process is too difficult or expensive.

62. Women who are being stalked with the assistance of technology are often told the incidents are simply coincidental. It is a common experience to hear from women that they have a sense of unease that their ex-partner is following them. The ex-partner turns up at a McDonalds just as the woman and her children arrive; the ex-partner arrives at the woman's local shopping centre just as she arrives even though it may not be his local shopping centre; the ex-partner arrives at a children's playground just as the woman and children arrive; or the ex-partner in communicating with the woman alludes to places the woman has been. Often the ex-partner would have no knowledge of the woman's location except if he was monitoring the woman through her emails or phone or tracking her car.

63. In another common scenario where a couple separate, the father buys new phones for his children. The mother may refuse to accept the phones as she fears the phones will be used by her ex-partner to monitor her. On some occasions women report ex-partners buying their children toys and discovering a tracking device inside the toy. Where women have told us this has happened they also say they report this to the NSW Police and no ADVO is taken out for their protection or the protection of their children.

64. Such scenarios can also be accompanied by the receiving of many unwanted text messages from an ex-partner within a period of 24 hours, some including language such as 'dead bitch' or threats 'you'll get yours' and still an ADVO will not be taken out by Police for the protection of the woman.

65. Based on the experience of our clients, monitoring and surveillance is often a precursor to escalation of other violence, including threats and physical violence. However, an ADVO is not generally taken out for the protection of the woman and her children in the absence of a direct threat to harm the woman, the children or himself; or sexual assault.

66. We also commonly hear from women who have experienced technology-facilitated stalking and abuse that there is insufficient evidence to apply for an ADVO.

67. Women tell us that a common response from NSW Police is that the woman cannot prove her ex-partner had control of the device when he sent her the text; hacked into her Facebook page and sent offensive messages to her friends and family; or published intimate images without her consent.

Scenario 1

Susan was in a violent relationship with Thomas for a short period. During that time Susan and Thomas lived interstate with Susan's children.*

After they separated, Thomas went through Susan's friends' list on Facebook and added her friends to a fake Facebook account he created in Susan's name with her photo and personal details. Susan's friends thought she must have created a new account and accepted the requests. Thomas began posting messages as Susan. He also started private messaging Susan's friends pretending to be Susan, saying hurtful and offensive things that ruined many of her friendships beyond repair.

Once Susan realised what was happening, she contacted the police in the state she was living. The police applied for a protection order against Thomas, including a condition that Thomas refrain from any form of communication with or about Susan or her children. Susan also reported the conduct to Facebook who eventually removed the fake account after several months.

Susan lost her job and her children started being bullied at school due to the comments Thomas had spread through the fake account. Susan decided to move to NSW to give her children and herself a fresh start.

Once Susan moved, four new fake accounts were made in her name. The person posing as Susan started making comments that Susan would harm her children. Susan called the police in the state in which Thomas was located to report the breaches and provided screen shots of the comments.

The police told her there was nothing they could do because they had no proof it was Thomas creating the accounts and posting the messages nor from which state the comments were being published. They also informed her as she was in NSW, it was outside their jurisdiction and she should contact the NSW Police.

Susan contacted the NSW Police and was told there was nothing they could do and that if the person making the publications was in another state, it was that state's jurisdiction.

Susan found out that the police could put in a formal request to the US Embassy to put in a request to Facebook for the relevant information, but this would likely take several months and even if Facebook agreed to assist and pass on the information, they would not necessarily disclose where the posts originated.

To be charged with a breach of the protection order, the acts must occur within the jurisdiction in which the protection order had been made (unless the protection order is registered in the new state). The police would also need to apply for a warrant to seize the accused's computer as evidence and it would need to be processed by experts, which would also take months and be expensive.

Offensive posts continued to be made about Susan and her children, impacting upon their lives and mental wellbeing.

**Based on the experiences of clients but not their real names.*

68. Women have also reported a common NSW Police response to abuse over social media is to suggest they simply stop using social media or to ignore the abuse. Telling a victim to stop engaging in social media minimises the harm suffered and ignores the reality that many victims of domestic violence may benefit from using social media to find support networks, to feel connected to friends or family (especially if the violence had isolated them) or to rebuild their self-esteem and heal.

69. We understand that it is expensive for NSW Police to investigate technology-facilitated stalking and abuse matters and in preparing evidence in an admissible form for the court, especially where charges are laid.

70. For example, when a criminal matter is investigated that requires telecommunications records, there are costs involved in obtaining these records. We understand that the cost of this investigation process can be significant depending on the service provider. Under the *Telecommunications Act 1997* (Cth), service providers must help police as is reasonably necessary but neither profit from nor bear the cost of that help.[29] We are concerned about both a lack of oversight of the costs being charged by service providers and that costs may be a deterrent for some police investigations. We therefore recommend a review by the Australian Communications and Media Authority ('ACMA') into the current charges of service providers.

71. Another example is where technology-facilitated stalking and abuse occurs on a social media platform, such as Facebook. In our experience, some police are reluctant to investigate Facebook matters because of the expense and effort involved in obtaining evidence that will be admissible in court. In our interactions with Facebook's Australian representatives, we have been informed that there are formal and informal routes that can be accessed by police to obtain evidence. Through the informal route, police can access basic subscriber information through the Law Enforcement Online Request portal (www.facebook.com/records). However, few Police officers we have spoken with have heard of this investigation route and many have reported their station has firewalls prohibiting Facebook access.

Collection of evidence

72. In technology-facilitated stalking or abuse matters, on first glance it may appear there is more evidence available than for in-person offences. Rather than having just witness evidence, there may be modification of devices, online content, screenshots, messages or call logs. However, with technology also comes the ability to manufacture evidence, edit photos and impersonate. We acknowledge the importance of the rules of evidence to ensure evidence is presented in an admissible form. However, in our experience, an individual Police officer's lack of understanding of the technology involved or of the rules of evidence can be a barrier to them investigating the matter. Meanwhile, officers with expertise in computer forensics in computer crime units are reserved for investigating serious indictable offences rather than, for example, breaches of AVOs.

[29] *Telecommunications Act 1997* (Cth), ss 313 & 314. See also Australian Communications Industry Forum (2001) *Industry Code ACIF C537:2001, Provision of Assistance to National Security, Enforcement and Government Agencies.*

73. We believe an operational response is needed so all investigating officers are properly resourced with the tools they need to collect evidence in these matters that is in an admissible form. We believe technology could be used to assist in collecting evidence properly and consistently.

74. For example, we recommend consideration be given to establishing an encrypted electronic device in all NSW Police stations that could be used to quickly and cheaply scan a person's device for spyware or malware; access social media accounts without firewalls; and extract relevant data in an admissible form. It could have automated prompts to assist an officer to correctly gather electronic evidence which could then be produced or given in court in an admissible form.

75. We recommend that regular training for all police about the law and the nature and dynamics of domestic violence include training in the gathering of evidence with respect to technology-facilitated stalking and abuse.

Criminal law

76. There are a number of possible criminal offences available in instances of technology-facilitated stalking and abuse. However, it is our experience that they are not widely utilised and we are encountering very few cases where charges are laid.

77. Below we outline our views on some of the NSW and federal criminal sanctions available in response to technology-facilitated stalking and abuse. These provisions highlight the need for more effective criminal sanctions.

NSW

Intimidation with intent to cause harm

78. Under section 13 of the *Crimes (DPV) Act*, it is an offence to stalk or intimidate a person with the intention of causing fear of physical or mental harm. The maximum penalty is imprisonment for 5 years or 50 penalty units, or both.

79. As previously discussed, the effectiveness of this provision depends upon technology-facilitated stalking and abuse being acknowledged as intimidating behavior and the ability to prove intention to cause fear of mental or physical harm.

Voyeurism provisions

80. Sections 91J – 91M of the *Crimes Act 1900 (NSW)* deal with voyeurism and related offences. The maximum penalty for the offences is imprisonment for 2 years or 100 penalty units, or both (or imprisonment for 5 years in aggravated circumstances).

81. However, these provisions are limited in their effectiveness as they only apply where filming occurs without consent. Additionally, to establish the offence it must be shown it was done for 'the purpose of obtaining, or enabling another person to obtain, sexual arousal or sexual gratification'. This can be ineffective where offenders may engage in these activities for other purposes such as to cause harm, to humiliate, to gain social status or to receive monetary reward.[30]

[30] See Nicola Henry and Anastasia Powell, 'Sexual Violence and Harassment in the Digital Age', Presentation to Women's Legal Services NSW, 24 April 2015 www.wlsnsw.org.au/wp-

Dealing with identification information

82. Section 192 of the *Crimes Act 1900 (NSW)* makes it an offence to deal in identification information with the intention of committing or facilitating the commission of, an indictable offence. The maximum penalty for this offence is imprisonment for 10 years.

83. For example, it may be an offence under this section if a person places his ex-girlfriend's home address on a sex forum pretending to be her and saying "come over for sex, I will say no, but I mean yes. I like it really rough." While we have had clients with similar experience, the perpetrators were not charged with this offence.

Publishing indecent articles

84. Section 578C of the *Crimes Act 1900 (NSW)* outlines the offence of publishing indecent articles. The maximum sentence for an individual is 100 penalty units and/or imprisonment for up to 12 months.

85. In *Police v Ravshan Usmanov*[31] this offence was used where a man had, without consent, published intimate sexual images of his ex-girlfriend on Facebook. It was noted by the Magistrate that this was the first NSW application of the offence for this sort of situation they were aware of.[32] The offender was given a 6 month suspended sentence on appeal.

86. It appears this offence has been relied upon where intimate sexual images are non-consensually shared, only due to the absence of a more suitable offence. It is questionable whether intimidate sexual photos should be categorised as 'indecent' and what message this sends to the victim and the community. We hold concerns that framing intimate sexual images of the victim as 'indecent' encourages victim blaming and allows the perpetrator's culpability to be minimised. Sharing the images without consent is the key wrong.

87. In other jurisdictions, indecent publication offences are narrower as 'indecent' is defined to only cover, for example, where there is violence shown or excrement is involved.[33] However, in jurisdictions such as South Australia, 'indecent' in the context of 'indecent filming' is defined broadly to cover intimate sexual material. However, as a matter of semantics, that refers to the filming itself (and the perpetrator's actions) as an indecent act, rather than the images, which are often 'selfies' taken by the victim, but shared without consent.

Blackmail

88. Section 249K *Crimes Act 1900 (NSW)* outlines the offence of blackmail. The maximum penalty is imprisonment for 10 years.

89. While this provision may be relevant in the context of sharing intimate images without consent, including sharing by a third party, the requirement of proving the intention of causing gain or loss may make this offence difficult to establish when it is for example, done to harass the other party.

---

content/uploads/NSW-Womens-Legal-Services-Presentation-24_April_2015.pdf

[31] *[2011] NSWLC 40.*

[32] *Police v Ravshan Usmanov* [2011] NSWLC 40 at [10]–[11] (Magistrate Mottley).

[33] See, eg, *Criminal Code Act 1983* (NT), ss 125A & 125C.

Unauthorised access to or modification of restricted data held in a computer

90. Section 308H of the *Crimes Act 1900 (NSW)* outlines the offence of unauthorised access to or modification of restricted data held in computer. The maximum penalty is imprisonment for 10 years.

91. It is required that the prosecution proves that access was unauthorised and that the data was restricted data. We would expect this would cover things such as spyware and keystroke logging software which is used to monitor keystrokes and so break passwords, for example, to accounts. It is not clear how the courts would deal with a situation where a person is able to log into another person's account as the passwords have been saved or not changed. For example, in *Anders v Anders No.2* where Kemp FM was considering the admissibility of evidence and whether emails accessed without consent were improperly obtained, he held that using an old password to access another's emails without consent amounted to unauthorised access, but there was insufficient evidence to prove the data was restricted data.[34]

Criminal defamation

92. Under section 529 *Crimes Act 1900 (NSW)* it is an offence to publish defamatory matter, knowing it to be false with intent to cause serious harm to the victim or any other person or being reckless to the harm. The Office of the Director of Public Prosecutions ('DPP') must provide written consent for proceedings to be brought for this offence. The maximum penalty is imprisonment for 3 years.

93. This offence is unlikely to assist victims of technology-facilitated abuse. Within its elements are a number of high thresholds and prosecution is rare, being reserved for matters of public welfare.[35]

Surveillance Devices Offences

94. The *Surveillance Devices Act 2007* (NSW) contains a number of offences prohibiting the installation, use and maintenance of listening devices,[36] optical surveillance devices,[37] tracking devices[38] and data surveillance devices.[39] There are also offences relating to sharing private conversations or recordings of activities,[40] sharing information from the use of a data surveillance device,[41] and possessing a recording of private conversation or activity.[42] The maximum penalty for these offences for individuals is 100 penalty units or 5 years imprisonment, or both.

95. In relation to optical surveillance devices, it is an offence if its installation, use or maintenance requires access to premises or a vehicle or interference with an object without consent. This is limited in helping victims of technology-facilitated stalking and abuse who still live with the perpetrator of violence. For example, we had one

[34] See, eg, *Anders v Anders No.2* (2008) 220 FLR 318 at 26 - 27.
[35] Craig Burgess, 'Criminal Defamation in Australia: Time to Go or Stay', *Murdoch University Law Review* (2013) 20(1).
[36] *Surveillance Devices Act 2007* (NSW), s 7.
[37] *Surveillance Devices Act 2007* (NSW), s 8.
[38] *Surveillance Devices Act 2007* (NSW), s 9.
[39] *Surveillance Devices Act 2007* (NSW), s 10.
[40] *Surveillance Devices Act 2007* (NSW), s 11.
[41] *Surveillance Devices Act 2007* (NSW), s 14.
[42] *Surveillance Devices Act 2007* (NSW), s 12.

client where the victim was living separated under one roof with her partner. She found covert video recordings in the air-conditioned vent in her private bedroom. The police refused to lay charges (including under the voyeurism provisions or for an intimidation offence), as the device was installed in premises jointly occupied.

Commonwealth

Dealing in identification information

96. Under s 372.1 of the *Criminal Code 1995 (Cth)*, it is an offence to make, supply or use the identification information of another person to pretend to be, or to pass oneself off as another person for the purpose of committing or facilitating a Commonwealth indictable offence. The maximum penalty is imprisonment for 5 years.

97. This section is of limited use as it must be for the purpose of committing or facilitating a Commonwealth indictable offence. However, it could be argued that if the identification information was being used to harass or menace using a carriage service, this offence could apply. For example, if a person makes a social media account in his ex-partner's name, pretending to be her, and then adds her friends and begins posting offensive comments, this may be using identification information with the purpose of committing a s474.17 offence. However, we are unaware of any prosecutions under this part for this sort of technology-facilitated abuse.

Interception devices

98. Under s 474.4 of the *Criminal Code 1995 (Cth)*, it is an offence to manufacture, advertise, sell, or possess an interception device. The maximum penalty is imprisonment for 5 years.

99. This offence could be used, for example, where a person has infected another person's computer with spyware that allows them to intercept their communications, such as emails. Arguably, the perpetrator's computer which has the software to intercept the other person's computer is an interception device. However, the practicalities of proving the perpetrator has been using their computer in this way, or obtaining a warrant for the seizure of that device as evidence are barriers to this offence being prosecuted.

Use of carriage service to make a threat

100. Section 474.15 of the *Criminal Code 1995 (Cth)* outlines the offence of using a carriage service to make a threat to kill or cause serious harm to a person. This includes threats to third parties, such as a new partner. The penalty is imprisonment for 10 years and 7 years respectively.

Use of carriage service to menace, intimidate, harass

101. Section 474.17 of the *Criminal Code* 1995 (Cth) outlines the offence of using a carriage service to menace, harass or cause offence. The maximum penalty is 3 years imprisonment.

102. As noted in the ALRC's *Final Report,* only 308 successful prosecutions under this

section have been made since its introduction in 2005.[43]

Interception of telecommunications

103. Sections 7 and 105 of the *Telecommunications (Interception and Access) Act 1979* (Cth) prohibit the interception of telecommunications. The maximum penalty is 2 years imprisonment.

Copyright offences

104. We are not currently aware of any situation where charges have been laid under Division 5 of the *Copyright Act 1968* (Cth) where intimate images have been shared without consent. There is limited potential for it to be used in these circumstances.

105. Where a photo[44] or video[45] has been created by the victim (such as 'selfies'), the material may be protected by copyright. For copyright, the person who takes the photo is the author of that work,[46] while the director of a film is usually the owner.[47] Even if the victim made the photo or video of themselves and sent it to the defendant during the relationship, their copyright subsists.

106. Where the material is, for example, made by a couple consensually during their relationship, they may be classified as joint authors/makers who are tenants in common of copyright, presumably in equal shares. The test of joint authorship is the extent to which two or more people collaborate in the creation of a work and the amount of skill and labour which each contributes.[48]

107. Where this is the case, any publication or reproduction must be authorised by both authors/makers, a joint owner may sue for infringement without the participation of the other joint owner even if the infringer is the co-owner of the copyright.[49] This may provide a recourse for women, for example, where sexual material was made with consent, but shared without consent.

108. The criminal offences under the Copyright *Act 1968 (Cth)* relate to commercial dealings such as selling or hiring out an infringing copy,[50] offering an infringing copy for sale or hire,[51] and distributing an infringing copy.[52] Therefore, there is some scope for these provisions to be enforced against perpetrators who receive money for publishing naked 'selfies' their ex-partners made on 'revenge porn' websites.

Offences involving minors

109. Technology-facilitated stalking and abuse is a growing issue for young women under 18 years of age. This raises a number of issues where either the victim or the perpetrator are minors.

---

[43] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era – Final Report*, 2014 at para 15.42.
[44] *Copyright Act 1968* (Cth), s 32.
[45] *Copyright Act 1968* (Cth), s 86.
[46] *Copyright Act 1968* (Cth), s 10(1).
[47] *Copyright Act 1968* (Cth), s 98.
[48] *Cala Homes (South) Ltd v Alfred McAlpine Homes East Ltd*. [1995] EWHC 7 (Ch)
[49] *Prior v Sheldon* [2000] FCA 438, Wilcox J.
[50] *Copyright Act 1968* (Cth), s 132AE.
[51] *Copyright Act 1968* (Cth), s 132AF.
[52] *Copyright Act 1968* (Cth), s 132AI.

110. A minor who is a victim of technology-facilitated stalking and abuse may be able to seek protection through an AVO. However, only NSW Police can apply for an AVO for the protection of a person under 16 years of age,[53] but a child can be the defendant in a matter.

111. It is also an offence to assault, stalk, harass or intimidate a person while at school (without causing actual bodily harm), carrying a maximum penalty of 5 years imprisonment.[54] This offence may be relevant for technology-facilitated stalking and abuse that occurs while the victim is at school.

112. Issues also arise with young people 'sexting'. If the person depicted in a sexually explicit photograph or video is a child (or appears to be a child), Division 15A of the *Crimes Act 1900* (NSW) or Part 10.6 of the *Criminal Code 1995* (Cth) relating to child pornography and child abuse material may apply. Under the *Crimes Act 1900* (NSW), a child is someone under 16.[55]

113. Many of the photos being sent by young girls are 'selfies' where they have sent sexually explicit photos of themselves to others (for example, boyfriends). Where this is the case, they themselves could be charged with an offence such as producing or disseminating child abuse material[56] or distributing child pornography material. [57]

114. There is a risk that any child who is found guilty of an offence in these circumstances could be placed on the Child Protection Offenders Register (NSW). While a child who commits a single offence outlined in s3A(2) of the *Child Protection (Offenders Registration) Act 2000 (NSW)* will be unlikely to be included on the register,[58] a minor could become a registrable offender if they engaged in more than one single offence.

115. We also acknowledge the appointment of the Children's E-Safety Commissioner in 2015 to deal with complaints made to social media platforms about online harassment involving children under the *Enhancing Online Safety for Children Act 2015* (Cth). However, this mechanism is limited to children and requires a number of protocols to be followed before injunctions or civil penalties apply.

Other criminal jurisdictions

Victoria

116. In 2014 the offence of distributing or threatening to distribute an intimate image was introduced in Victoria.

117. The offence as outlined in s41DA of the *Summary Offences Act 1966 (Vic)* has two elements:

(1)(a) *A intentionally distributes an intimate image of another person (B) to a person other than B; and*

[53] *Crimes (Domestic and Personal Violence) Act 2007* (NSW), ss 48(3) & 48(6).
[54] *Crimes Act 1900* (NSW), s 60E.
[55] *Crimes Act 1900* (NSW) s 91FA.
[56] *Crimes Act 1900* (NSW), s 60E.
[57] *Criminal Code Act 1995* (Cth), s 474.19.
[58] *Child Protection (Offenders Registration) Act 2000* (NSW) s 3A(2).

(b) the distribution of the image is contrary to community standards of acceptable conduct.

It is not an offence if B is 'not a minor'[59] and 'expressly or impliedly consented, or could reasonably be considered to have expressly or impliedly consented'.[60]

118. 'Intimate image' is defined in s40 of the *Summary Offences Act 1966 (Vic). 'Intimate image' means a moving or still image that depicts -*

(a) a person engaged in sexual activity; or
(b) a person in a manner or context that is sexual; or
(c) the genital or anal region of a person or, in the case of a female, the breasts.

119. 'Distribute' as defined in s40 of the *Summary Offences Act 1966 (Vic)* includes -

(a) publish, exhibit, communicate, send, supply or transmit to any other person, whether to a particular person or not; and
(b) make available for access by any other person, whether by a particular person or not;

120. Section 41DA(2) provides the penalty for distribution of an intimate image is a maximum of 2 years. Section 41DB(2) provides the penalty for threatening to distribute an intimate image is a maximum of 1 year.

South Australia

121. In 2013 the offence of distribution of invasive image was introduced in South Australia.[61]

122. Section 26C of the *Summary Offences Act 1953 (SA)* provides:

(1) A person who distributes an invasive image of another person, knowing or having reason to believe that the other person -
(a) does not consent to that particular distribution of the image; or
(b) does not consent to that particular distribution of the image and does not consent to distribution of the image generally,
is guilty of an offence.

123. 'Invasive image' is defined in s26A of the *Summary Offences Act 1953 (SA).*
'*Invasive image' means a moving or still image of a person -*
(a) engaged in a private act; or
(b) in a state of undress such that the person's bare genital or anal region is visible

but does not include an image of a person under, or apparently under, the age of 16 years or an image of a person who is in a public place.

124. 'Private act' as defined in s26A of the *Summary Offences Act 1953 (SA)* means -
(a) a sexual act of a kind not ordinarily done in public; or

[59] *Summary Offences Act 1966 (Vic),* s 41DA (3)(a)
[60] *Summary Offences Act 1966 (Vic),* s 41DA (3)(b)

[61] *The Summary Offences (Filming Offences) Amendment Act 2013 (SA)* introduced s26C of the *Summary Offences Act 1953 (SA)* and s26A which includes definitions of 'invasive image' and 'private act'.

(b) using a toilet;

125. Section 26C of the *Summary Offences Act 1953 (SA)* provides the maximum penalty is $10,000 or imprisonment for 2 years.

New Zealand

126. The *Harmful Digital Communications Act 2015 (NZ)* includes an offence of causing harm by posting a digital communication. Section 22(a) provides three criteria that must be met to establish the offence:

a) A person posts a digital communication with the intention that it cause harm to a victim; and

b) Posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and

c) Posting the communication causes harm to the victim.

127. In section 4 'posts a digital communication'

(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication -
(i) any information, whether truthful or untruthful, about the victim; or
(ii) an intimate visual recording of another individual; and

(b) includes an attempt to do anything referred to in paragraph (a)

128. 'Intimate visual recording' is defined in detail in section 4 including to be an image of a person in a state of nakedness, partially exposed, solely in undergarments, engaged in an intimate sexual activity or engaged in showering, toileting or other personal bodily activity that involves dressing or undressing.

129. 'Harm' is defined in section 4 as 'serious emotional distress'.

130. Section 22(3) provides the penalty for a person is imprisonment not exceeding 2 years or a fine not exceeding $50,000.

131. The criminal provisions commenced in July 2015. It is too early to know the effectiveness of the provisions.

New criminal offence

132. In response to these uncertainties in NSW, we recommend at least a new NSW criminal offence, which captures the distribution or threatened distribution of intimate images of a sexual nature without consent. We recommend community consultation for any proposed NSW legislation addressing this issue.

133. We acknowledge and welcome the *Criminal Code Amendment (Private Sexual Material) Bill 2015* private members bill that has been proposed to amend the *Criminal Code Act 1995 (Cth)* to introduce offences relating to the use of a carriage service relating to sharing intimate sexual images without consent. We repeat our concerns about also capturing intimate images of a non-sexual intimate nature within

the context of domestic violence, such as an image of a woman without her religious headscarf which may be highly distressing or harmful to that woman.

134. We recommend introducing a state criminal offence even if a commonwealth law is passed. This could capture offences relating to sharing intimate sexual images without consent regardless of whether a carriage service is used.

135. Any criminal offence should consider and recognise the prevalence of sexting amongst minors and that children in NSW are reluctant to report non-consensual sharing of intimate images where they fear they may be prosecuted for creating and sharing such images with their boyfriend or girlfriend with whom they initially shared with consent. While there need to be consequences for non-consensual sharing of intimate images by minors, it is also relevant to be informed by the rights enshrined in the Convention on the Rights of the Child, such as Article 40 that treatment of children who come into conflict with the law must take into account the desirability of promoting the child's reintegration and the child's assuming a constructive role in society.

Civil remedies

Breach of confidence

136. At present, it is uncertain whether in NSW breach of confidence extends to situations where intimate images are shared without consent. Based on the decisions of *Giller v Procopets*[62] and *Wilson v Ferguson*,[63] it seems likely that NSW would follow Victoria and Western Australia respectively in similar cases and decide that after a relationship has ended, intimate sexual photos are implied to be confidential. However, it could be beneficial to have this principle legislated with a presumption that upon the ending of a relationship, any intimate photos are strictly confidential.

137. Traditionally, under the equitable action of breach of confidence, remedies consisted of injunctions, compensation for economic loss due to the breach or an account of profits. However, in Victoria and Western Australia this has been recently extended to include damages for emotional stress. In *Giller v Procopets*,[64] the Victorian Court of Appeal allowed damages for emotional distress. In this matter, the defendant had disseminated a sex tape that had been created while he was in a relationship with the claimant. Neave JA, with whom Maxwell JA agreed granted $40,000 for breach of confidence. Ashley JA supported the award of compensation, but under the exercise of equity's inherent jurisdiction rather than as common law damages.[65]

138. In the more recent decision of *Wilson v Ferguson*,[66] the defendant had posted multiple explicit photos and videos of his ex-girlfriend on his Facebook page after they broke up. The parties worked together and had many shared colleagues who the defendant was friends with on Facebook.

[62] (2008) 24 VR 1.
[63] [2015] WASC 15.
[64] (2008) 24 VR 1.
[65] *Giller v Procopets* (2008) 24 VR 1 at [141].
[66] [2015] WASC 15.

139. Mitchell J relied on the inherent equitable jurisdiction for breach of an equitable obligation. The claimant was awarded $35,000 damages for the significant embarrassment, anxiety and distress she suffered. Injunctive relief was also granted to prevent further publication.

140. It is uncertain whether the *Wilson v Ferguson*[67] decision will be followed in NSW. While decisions from intermediate appellate courts in other jurisdictions should be followed in relation to non-statutory law, unless the Judge is convinced the interpretation is plainly wrong,[68] it is impossible to predict what direction the court may take. We recommend that a statutory tort for serious invasions of privacy allow for damages to be awarded for emotional harm. In the event a statutory cause of action is not introduced, the courts should be empowered by legislation to award compensation for emotional distress in cases of breach of confidence.

Tort of intentional infliction of harm

141. To make out a cause of action for the tort of intentional infliction of harm a person must have wilfully done an act 'calculated' and reasonably likely to cause harm to another and in fact caused physical harm or a recognised psychiatric injury to mental health.[69]

142. This tort is based on *Wilkinson v Downton*,[70] a 19th Century case where the defendant told a woman her husband had been in a serious accident as a practical joke, and as a result she suffered physical consequences such as vomiting and weeks of incapacity.

143. In terms of an action for the intentional non-consensual sharing of intimate images, this tort is of limited use. Its limitation is its requirement that it must result in a psychiatrically cognisable injury rather than just emotional harm. However, some doubt was cast by the obiter of Maxwell P in *Giller v Procopets,*[71] where he questioned the need for the injury to be a 'recognised psychiatric injury.' He noted that our understanding of psychiatric injury has advanced with developments in medical science and so it should no longer be necessary to insist on physical proof of mental harm or to insist on proof of a 'recognised mental illness.'

Defamation

144. Defamation is of limited use in instances where intimate images are shared without consent. This is because, for example, there are extensive defences available, it may be difficult to prove the images are defamatory and because it is often necessary for both parties to have deep pockets to pursue an action. Further, while injunctive relief is available, it must be supplementary to the principal cause of action.[72]

[67] [2015] WASC 15.
[68] *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* [2007] HCA 22.
[69] [1897] QB 57.
[70] [1897] QB 57.
[71] (2008) 24 VR 1, [at 6].
[72] *Naoum v Dannawi* [2009] NSWCA 253.

145. Intimate images in and of themselves are not 'defamatory' unless they carry defamatory imputations. Photographs of private parts were deemed defamatory in *Ettingshausen v Australian Consolidated Press Limited*,[73] where the professional footballer received damages of $100,00 after a magazine published a photo showing his genitals. It was held to be a defamatory imputation that he had deliberately exposed his genitals to readers.

146. In the Queensland case of *Shepherd v Walsh & Ors,*[74] an action for defamation was brought where an intimate image was shared without consent. In this case, the defendant had taken naked photos of an ex-girlfriend without her knowledge or consent. He then had his current girlfriend send the photos into a salacious magazine with a caption and received $150 for the photo from the publisher. The plaintiff was awarded $50,000 damages and $20,000 punitive damages (which are no longer available).[75] Arguably defamation was easier to prove in this matter because the respondent had impersonated his ex-girlfriend in publishing the material and made up additional details so he could not rely on the defence of truth.

147. If images are intimate images shared without consent and they are defamatory, there is also scope for Internet Service Providers (ISPs) to become liable for damages. There is no general rule that an ISP which performs no more than a passive role cannot be a publisher.[76] For example, in *Trkulja v Google* (No 5) [2012] VSC 533, Google was unable to rely upon the defence of innocent dissemination in an image matter not removed after a takedown request was received.

148. For an action of defamation, damages for non-economic loss are capped at $250,000[77] and must be appropriate and rational to harm sustained.[78]

149. Due to its many limitations, we do not believe defamation provides an adequate remedy for a cause of action relating to intimate images shared without consent.

Copyright

150. As discussed above at paragraphs 104-108 the *Copyright Act 1968* (Cth) may be available in limited circumstances where intimate images or videos are shared without consent. However, copyright law contemplates a commercial loss of intellectual property rights rather than a private and individual loss. The fact that such commercial rights currently receive more civil protection than individual rights to privacy suggests an urgent need for law reform.

151. Where a work of copyright has been infringed,[79] civil actions can include injunctions, damages or an account of profits.[80] Damages from sharing intimate images without consent may be difficult to quantify or prove under copyright law, for example, damages are not available where the infringing party had no grounds for

[73] (1991) 23 NSWLR 443.
[74] [2001] QSC 358.
[75] *Defamation Act 2005 (NSW),* s 37.
[76] See, eg, *Trkulja v Google Inc LLC (No 5)* [2012] VSC 533.
[77] *Defamation Act 2005* (*NSW*), s 35.
[78] *Defamation Act 2005* (*NSW*), s 34.
[79] *Copyright Act 1968* (*Cth*), ss 36 & 115.
[80] *Copyright Act 1968* (*Cth*), s 115(2).

suspecting, or was unaware that its conduct constituted an infringement.[81] Further, if seeking damages for loss of reputation, evidence must be lead as the value of one's reputation or the value of the loss from the infringing conduct.[82]

152. The *Copyright Regulations 1969* (Cth) also set out mechanisms for infringement notices to be issued. If a victim's intimate images are shared without consent and the victim is the author or owner of the work under the *Act,* they can alert a carriage service provider of the infringing material via a notification of infringement,[83] which can be sent by post or email.[84] The carriage server then must expeditiously remove, or disable access to copyright material in accordance with the takedown procedure in Reg 20J.

153. This could be a quick and effective means for having still and moving images removed online, however, there is insufficient community knowledge of these procedures.

154. If a statutory tort is created for serious invasions of privacy we suggest having a schedule in accompanying regulations which sets out a clear and simple take down process, in particular, for contacting service providers, so failure to respond or take appropriate action could lead to third party liability.

Victims Support

155. In order to be eligible for support under the *Victims Rights and Support Act 2013 (NSW)* a person needs to show that they are a victim of an act of violence in NSW.

156. 'Act of violence' is defined in section 19. Section 19(8) provides the definition of sexual assault and domestic violence with s19(8)(f) including 'any other act resulting in injury that occurred in the commission of a personal violence offence (within the meaning of the *Crimes (Domestic and Personal Violence) Act 2007* (NSW)).

157. Although many cases of technology-facilitated stalking and abuse should amount to a section 13 intimidation offence[85] which is a personal violence offence, in our experience, it is difficult for victims in these situations to receive financial assistance unless there have been criminal charges laid or a breach of an AVO. They also have a further hurdle of trying to establish actual physical or psychological injury, which can be difficult to evidence unless they access counselling.

158. A personal violence offence does not include the criminal offences outlined above such as voyeurism and related offences; dealing with identification information; publishing indecent articles; blackmail; and unauthorised access to or modification of restricted data held in computer.

159. If a new criminal offence is created to address the distribution or threatened distribution of intimate sexual images it is important there is a corresponding amendment so this new offence is considered a personal violence offence for the

[81] *Copyright Act 1968* (*Cth*), s 115(3).
[82] *Facton Ltd v Rifai Fashions Pty Ltd* [2011] FCA 290
[83] The form of this infringement notice is set out in Part 3 of Schedule 10 of the *Copyright Regulations 1969 (Cth).*
[84] *Copyright Regulations 1969 (Cth),* r 20I.

purposes of Victims Support.

160. This amendment would mean that victims of such crimes will be eligible for financial assistance and recognition payments in addition to counselling.

161. We also note the where a person is a victim of technology-facilitated stalking and abuse and the other party is convicted of an offence, there may be scope for the court to make an order for the offender to pay compensation for any loss, either at their own initiative or on application by the aggrieved.[86] However, we have not seen this provision used in practice in matters of technology-facilitated stalking and abuse in part because often the aggrieved person is unaware of their rights to make such an application and also because it appears from our experience, that few of these matters are being charged in the first instance to end up in court.

Term of reference (b) should a statutory cause of action for serious invasions of privacy be introduced?

162. Both the NSW Law Reform Commission[87] and the Australian Law Reform Commission[88] have recommended the introduction of a statutory cause of action for serious invasions of privacy.

163. We support the establishment of a NSW and federal statutory cause of action for serious invasions of privacy. Due to the digital nature of technology-facilitated stalking and abuse, it often transcends State or Territory borders. Therefore, we recommend well considered, uniform laws.

164. The types of behaviour outlined in paragraph 9 should be captured by a statutory cause of action. The sharing of intimate images of a non-sexual nature in the context of domestic violence, such as an image of a woman without her religious headscarf should also be captured.

165. In the ALRC inquiry we supported having one tort which may include different types of invasion and fault. We supported the proposal that the tort include: '(a) intrusion upon the plaintiff's seclusion or private affairs (including by unlawful surveillance); or
(b) misuse or disclosure of private information about the plaintiff (whether true or not)'.

166. We are unclear if such a tort would capture instances where a threat to share private information may be made but there is no proof of publication. See Scenario 2 below.

[86] *Victims Rights and Support Act 2013* (*NSW),* ss 97(1) & 97(2).
[87] NSW Law Reform Commission, *Invasion of Privacy* Report 120, 2009, Sydney, Recommendation at 3.
[88] Australian Law Reform Commission, *Serious Invasions of privacy in the Digital Era*, Report 123, 2014, Canberra, Recommendation 4-1.

Scenario 2

X (female) and her then partner, Y (male) filmed themselves having sex. Post-separation Y allegedly sent the recording to Z (third person). X was contacted by Z who made comments that she should sleep with him if she does not want the material circulated further.

a. Would X have a cause of action in tort if there was a sex tape but it was not sent to Z and Z was informed of its existence and made empty threats?

c. Would injunctive relief be available if X is without proof of the publication?

167. It is important there are protections such that there is a remedy to the situation outlined in Scenario 2.

168. While we note the ALRC was considering a Commonwealth tort, we also see value in a similar NSW tort.

Privacy and Communication Principles

169. The ALRC Final Report includes 9 guiding principles about privacy which are listed below:
Principle 1: Privacy is a fundamental value worthy of legal protection
Principle 2: There is a public interest in protecting privacy
Principle 3: Privacy should be balanced with other important interests
Principle 4: Australian privacy laws should meet international standards
Principle 5: Privacy laws should be adaptable to technological change
Principle 6: Privacy laws should be clear and certain
Principle 7: Privacy laws should be coherent and consistent
Principle 8: Justice to protect privacy should be accessible
Principle 9: Privacy protection is an issue of shared responsibility[89]

170. We support the inclusion of guiding principles about privacy but raise the following issues in relation to the ALRC guiding principles.

171. In relation to Principle 3, privacy being balanced with other important interests, we believe these should include the right to equality, which includes the right to be free from violence; and the right to security. This is discussed in further detail in the section on balancing of human rights above.

172. In relation to Principle 9, the context of domestic and/or family violence needs to be taken into account since there will be an imbalance of power and coercive and controlling behaviour. A victim of domestic and/or family violence may not be able to change the password on her computer because, for example, her ex-partner has control of the computer and the finances. Alternatively, she may not know how to change the password and it may take time to identify the issue and seek help. Some women may have taken several steps to change their password, including changing their passwords several times and the ex-partner continues to find ways to access their private information. Responsibility should not fall to the victim to ensure their

[89] ALRC, *Serious Invasions of Privacy in the Digital Era Final Report*, Report 123, Sydney, June 2014 at 33-44.

privacy is protected. Perpetrators of violence should be held accountable for their actions.

173. The *Harmful Digital Communications Act 2015 (NZ)* (HDCA – NZ) provides both civil and criminal remedies. The purpose of the Act as outlined in section 3 is twofold – to:

> *(a) deter, prevent and mitigate harm causes to individuals by digital communications; and*
>
> *(b) provide victims of harmful digital communications with a quick and efficient means of redress*

174. The Act creates an 'Approved Agency' to receive, investigate, assess and help to resolve complaints about the harm caused to an individual by a digital communication.[90]

175. There is also the option of proceedings in the District Court, though a person should first make a complaint to the Approved Agency.[91]

176. Before the Court can consider an application for orders outlined in Section 19 of the HDCA – NZ including a 'take down or disable material order'; an order the defendant 'cease or refrain from conduct concerned'; and order 'the defendant not encourage any other persons to engage in similar communications towards the affected individual', the Court must be satisfied of two criteria outlined in section 12(2):

> *(a) there has been a threatened serious breach, a serious breach, or a repeated breach of 1 or more communication principles; and*
>
> *(b) the breach has caused or is likely to cause harm to an individual.*

177. Section 6 provides the 10 communication principles which are outlined below.

> Principle 1: A digital communication should not disclose sensitive personal facts about an individual.
>
> Principle 2: A digital communication should not be threatening, intimidating, or menacing.
>
> Principle 3: A digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.
>
> Principle 4: A digital communication should not be indecent or obscene.
>
> Principle 5: A digital communication should not be used to harass an individual.
>
> Principle 6: A digital communication should not make a false allegation.
>
> Principle 7: A digital communication should not contain a matter that is published in

[90] *Harmful Digital Communications Act 2015 (NZ), section 8*
[91] *Harmful Digital Communications Act 2015 (NZ),* section 12(1)

breach of confidence.

Principle 8: A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.

Principle 9: A digital communication should not incite or encourage an individual to commit suicide.

Principle 10: A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

178. These principles must be taken into account along with 'acting consistently with the rights and freedoms contained in the New Zealand Bill of Rights 1990' when the 'Approved Agency' and courts perform their functions or exercised their power under the HDCA - NZ.[92]

179. We support the inclusion of principles in legislation. Consideration should be given to both the principles proposed by ALRC and those in the *Harmful Digital Communications Act 2015 (NZ).*

Reasonable expectation of privacy

180. The ALRC recommended a new Commonwealth Act provide a non-exhaustive list of factors in determining whether a person in the plaintiff's position would have a reasonable expectation of privacy [ALRC Recommendation: 6-2]. The factors include:

(a) the nature of the private information, including whether it relates to intimate or family matters, health or medical matters, or financial matters;

(b) the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology;

(c) the place where the intrusion occurred, such as in the plaintiff's home;

(d) the purpose of the misuse, disclosure or intrusion;

(e) how the private information was held or communicated, such as in private correspondence or a personal diary;

(f) whether and to what extent the private information was already in the public domain;

(g) the relevant attributes of the plaintiff, including the plaintiff's age, occupation and cultural background; and

(h) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy. [93]

[92] *Harmful Digital Communications Act 2015 (NZ),* Section 6(2).
[93] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123, Sydney, June 2014, Recommendation 6-2.*

181. Scenario 3 below demonstrates the importance of also including 'the nature of the relationship'. It is important to correctly identify the primary aggressor and the primary victim.

Scenario 3

X (female) and Y (male) are in a relationship that involved domestic violence. Y recorded himself and X having sex. X was aware of the recording but did not feel she could say no in the context of a violent relationship. Y uses this video as an ongoing threat. X is isolated from her family who all live overseas. Y often threatens to send it to her family, bringing her shame if she ever left him or misbehaved. X called police after a physical altercation involving Y. X regretted calling the police, not wanting to get in trouble with Y, so X said nothing when police arrived. Both parties had injuries (X's being defensive). X was ultimately charged with assault and property damage and the police applied for an AVO for Y's protection. X consented to the AVO which had been used by Y as a coercive tool against her.

182. With respect to factor (b) 'the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology', we submit it should make no difference if the information was obtained by accessing an ex-partner's account through a password known from the relationship, auto-filled or saved on a device, pre-logged in, guessed or hacked. Upon the ending of a relationship, consent to access or share private information should be taken to be withdrawn.

183. Where access to private information is required once the relationship has ended, for example where former intimate partners run a business together, it should be presumed that explicit consent to continue accessing relevant private information is required.

184. We frequently see cases where in the context of domestic and family violence, a partner or ex-partner may deliberately invade a woman's privacy with the intention of causing emotional distress as a continuation of violence. We submit that her ex-partner's knowledge of a password should not prevent the woman from having an action under the proposed tort.

Scenario 4

X (female) and Y (male) are separated. Y logs into X's private email address using the password. Y sends emails to X's workmates and family members overseas saying rude and offensive comments. All emails are deleted after being sent so X is unaware they have been sent. X's family begins to alienate her without X understanding why. X does not find out about the abusive work emails until a colleague makes a formal complaint about her to her employer.

185. Emotional harm caused intentionally may present in ways other than a psychiatric illness. It can include damage in the form of a breakdown of relationships with family, work colleagues and/or friends as a result of efforts to alienate the woman from these

networks. It is therefore important that a serious invasion of privacy tort takes into account damage caused as a result of intentional emotional harm other than a psychiatric illness. This would echo the emerging trend in the law of breach of confidence towards expanding relief to include emotional harm, outlined above.[94]

186. We recommend the inclusion of an additional factor in relation to reasonable expectation of privacy, namely 'the nature of the relationship between the parties'.

187. We refer to section 44(2)(c) *Victims Rights and Support Act* as an example of how 'the nature of the relationship' has been considered in other contexts. That section considers 'the nature of the relationship between the victim and the person or persons by whom the act of violence is alleged to have been committed' with regards to reporting to police within a reasonable time.

188. We submit that in cases of family and/or domestic violence it is reasonable that victims of such violence should have a higher expectation of privacy. Scenario 5 below highlights this as well as the importance of including 'the nature of the relationship' as a listed factor.

Scenario 5

X (female) & Y (male) are separated. X is listed as the protected person in a final AVO against Y due to domestic violence. X fled and Y does not know X's current address which has remained undisclosed through court proceedings (hence, no orders stipulating that Y is not to come near her home). Y finds out X's address through technology, for example, logging in to X's personal accounts (such as Ebay or Centrelink), using spyware or giving their children phones with tracking software. Y parks his car outside X's house – is her address private information and if yes, is the breach serious?

Seriousness

189. As we did with the ALRC inquiry, we support a 'serious' threshold for any proposed new NSW tort of invasion of privacy.

190. The ALRC recommended that in determining the seriousness of the invasion of privacy regard be had to, amongst other things:

(a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff; and

(b) whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff.[95]

191. We submit the seriousness threshold should be met, for example, where a person shares intimate images of a non-sexual nature within the context of domestic violence, such as an image of a woman without her religious headscarf which may be

[94] See *Giller v Procopets* (2008) 24 VR 1 and *Wilson v Ferguson* [2015] WASC 15.
[95] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123, Sydney, June 2014, Recommendation 8-1.*

highly distressing or harmful to that woman.

192. We note that what is serious for one person may not be serious for another. In situations of domestic and/or family violence fear may be instilled by a look or a word which has significant meaning for a particular victim, but may seem harmless to someone else.

193. We also note that in Aboriginal and Torres Strait Islander communities it may be highly offensive or distressing or harmful to show images of a deceased person. With advances in technology it is much easier to do this. Further consideration should be given to this issue in this inquiry.

Defences

194. In any defence to a statutory cause of action for serious invasion of privacy that the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property, we recommend there be a requirement the act or conduct was proportionate, or necessary and reasonable.

Scenario 6

X (female) and Y (male) are separated; X is the protected person against Y in a final AVO due to domestic violence. X finds out Y has a new girlfriend, X contacts her to warn her that Y is a perpetrator of serious domestic violence. How would this matter be dealt with under the proposed new tort?

195. In Scenario 6 above we submit that by 'X' warning the new partner about the ex-partner this is likely conduct that is proportionate, necessary and reasonable.

196. Where an action for serious invasion of privacy is brought it should be a defence to argue a public interest test or balancing of rights test. Given it is proposed that the invasion of privacy must be serious we submit this would limit unmeritorious claims.

Remedies

197. Just as we supported in the case of a Commonwealth tort, so too a NSW statutory cause of action for serious invasion of privacy should provide that courts may pay compensatory damages, including for emotional distress.

198. We support the ALRC recommendation for 'exemplary damages in exceptional circumstances' and where the court considers the other damages awarded would be an 'insufficient deterrent'[96] as also being appropriate in a NSW Act.

199. Using exemplary damages in the context of violence against women would send a powerful message that violence against women is unacceptable in our society.

Injunctions

200. We support ALRC recommendation 12-7 that 'the Act should provide that the court may at any stage of proceedings grant an interlocutory or other injunction to

[96] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-4 and para 12.77.

restrain the threatened or apprehended invasion of privacy, where it appears to the court to be just or convenient and on such terms as the court thinks fit.'

201. We also support ALRC recommendation 12-9 that 'the Act should provide that courts may order the delivery up and destruction or removal of material.'

202. We similarly support the court having power to make such orders in a NSW statutory cause of action.

203. However, given a tort is usually a very expensive cause of action and not necessarily accessible to all, it is important to also provide an avenue for injunctive relief at the Local Court which is just, quick and cheap.

204. We recommend that Local Courts be given the power to grant stand-alone injunctive orders such as take down orders and/or deliver up orders. An alternative option is to amend the *Crimes (DPV) Act* as discussed above at 58- 60. However, a failure to establish fear under the Crimes (DPV) Act should not prevent a just, quick and cheap remedy in the form of a take down or deliver up order in the Local Court.

205. While noting that obtaining injunctive relief from a Local Court would be a significant new power, we submit the significant changes in technology and the potential to use such technology as a form of violence against women warrants such a power.

Other remedies

206. Other than monetary remedies and injunctions, we support the list of remedies recommended in the ALRC's *Final Report* as being appropriate for a NSW statutory cause of action. This includes an order requiring the defendant to apologise to the plaintiff;[97] a correction order;[98] an order for delivery up, destruction or removal of material;[99] a declaration.[100]

207. We note the HDCA – NZ empowers the court to make orders against an online content host, including orders such as take down or disable public access to material that has been posted or sent; that the identify of the author of an anonymous or pseudonymous communication be released to the court; and correction orders. We support the power to take such action.

208. Section 21 of the HDCA – NZ provides an offence not to comply with an order without reasonable excuse. The penalty for a natural person is imprisonment for a term not exceeding 6 months or a fine not exceeding $5,000. The penalty for a body corporate is a fine not exceeding $20,000.

209. We support sanctions for non-compliance with orders relating to serious invasions of privacy.

---

[97] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-11

[98] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-10.

[99] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-9

[100] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014, Recommendation 12-12

210. ALRC recommendation 12-2 sets out a list of non-exhaustive factors to consider when determining the amount of damages. One factor includes whether either party took reasonable steps to resolve the matter without litigation. This could include alternative dispute resolution (ADR).

211. In cases of domestic and/or family violence or sexual violence, ADR may not be appropriate. The ALRC acknowledges this and so does not recommend ADR as a compulsory step.[101] The same should apply in a NSW cause of action.

Support, costs, legal aid, fee waivers and exemptions

212. Where a person has a prima facie case but is an impecunious litigant there should be technical assistance available to assist them in running their case.

213. In the Local Court or in a tribunal or tribunal-like setting, each party should bear their own costs unless the matter is deemed frivolous or vexatious or a party displays unreasonable conduct during the course of the proceedings.

214. In higher courts where costs are involved, costs should follow the event.

215. Legal aid should be available, particularly in a matter that involves domestic and/or family violence or sexual violence, subject to a means test. We note a benefit of access to legal aid is the indemnity against costs for legally aided clients.

216. Fee waivers and exemptions for court fees associated with a cause of action founded on tort, such as filing fees, subpoenas and other fees, must be available.

217. We note section 15(3) of the HDCA – NZ provides that 'no filing fee is payable for an application'.

A complaints mechanism

218. We are concerned that seeking a remedy through a statutory cause of action may not be accessible for all.

219. WLS NSW supports a just, quick, cheap and accessible complaints mechanism, similar, for example, to how the Australian Human Rights Commission manages complaints.

220. WLS NSW supports the use of alternative dispute resolution (ADR) options such as mediation or conciliation in appropriate circumstances. However, we believe that it is essential that referrals to mediation or conciliation are made after an assessment that such a referral is appropriate, rather than automatically.

221. There should also be the option of lawyer-assisted ADR.

222. Matters involving serious threats or harassment relating to a person's sex, race, religion, sexual orientation, gender identity, intersex status, HIV/AIDS infection or disability should be excluded from referral to mediation or conciliation unless the applicant requests a referral.

[101] ALRC *Serious Invasions of Privacy in the Digital Era Final Report, Report 123,* Sydney, June 2014 at para 12.60-12.61.

223. WLS NSW opposes the referral of matters relating to sexual harassment or other forms of sexual violence to mediation or conciliation without representation.

224. While some people may be able to attend conciliation by telephone it is particularly important that Aboriginal and Torres Strait Islander people, people from culturally and linguistically diverse backgrounds and people with disability have the opportunity of a face-to-face conciliation, preferably in their local area.

225. The ALRC concluded an independent regulator should be able to bring proceedings on behalf of an individual or individuals. WLS NSW agrees with the ALRC that this approach may better enable access to justice for those of limited means and other vulnerable persons. We also believe that an independent regulator will be beneficial in cases where systemic breaches of privacy have occurred.

If you would like to discuss any aspect of this submission, please contact Alex Davis, Solicitor or Liz Snell, Law Reform and Policy Coordinator on .

Yours faithfully,
Women's Legal Services NSW

Janet Loughman
Principal Solicitor