Human Rights and Technology: Issues Paper

Legal Aid NSW further submission to the Australian Human Rights Commission

Technology-Facilitated Domestic and Family Violence

December 2018

323 CASTLEREAGH ST
HAYMARKET NSW 2000 /
DX 5 SYDNEY

Legal Aid NEW SOUTH WALES

About Legal Aid NSW

The Legal Aid Commission of New South Wales (**Legal Aid NSW**) is an independent statutory body established under the *Legal Aid Commission Act 1979* (NSW). We provide legal services across New South Wales through a state-wide network of 24 offices and 221 regular outreach locations, with a particular focus on the needs of people who are socially and economically disadvantaged.

We assist with legal problems through a comprehensive suite of services across criminal, family and civil law. Our services range from legal information, education, advice, minor assistance, dispute resolution and duty services, through to an extensive litigation practice. We work in partnership with private lawyers who receive funding from Legal Aid NSW to represent legally aided clients.

We also work in close partnership with LawAccess NSW, community legal centres, the Aboriginal Legal Service (NSW/ACT) Limited and pro bono legal services. Our community partnerships include 29 Women's Domestic Violence Court Advocacy Services.

The Legal Aid NSW Domestic Violence Unit (**DVU**) is a specialist unit helping clients who have experienced domestic and family violence with both their legal and non-legal needs.

The DVU is made up of specialist lawyers and social workers who connect with clients at crisis point. It provides legal advice and representation in a range of areas including: Apprehended Domestic Violence Orders, family law, care and protection, housing, social security, credit/debt problems, victims' support, financial assistance matters and criminal law.

On behalf of National Legal Aid, the DVU is currently developing a national website with legal information and practical help with domestic and family violence, family law, child protection and civil protection orders. The website also includes content on technology-facilitated domestic and family violence and staying safe online.

The DVU also provides Community Legal Education and Legal Education on technology-facilitated domestic and family violence and safety planning.

Legal Aid NSW welcomes the opportunity to make a further submission to the Human Rights and Technology Issues Paper. Should you require any further information, please contact:

Alex Davis
Senior Solicitor
Domestic Violence Unit
[redacted]

or

Damien Hennessy
Senior Law Reform Officer
Strategic Law Reform Unit
[redacted]

Introduction

Legal Aid NSW welcomes the opportunity to provide a further submission to the Human Rights and Technology Issues Paper on the subject of technology-facilitated domestic and family violence (**TFDFV**). The submission is based primarily on the experience of Legal Aid NSW's Domestic Violence Unit (**DVU**), which is a specialist unit helping clients who have experienced domestic and family violence with both their legal and non-legal needs.

The DVU is made up of specialist lawyers and social workers who connect with clients at crisis point. It provides legal advice and representation in a range of areas including: Apprehended Domestic Violence Orders, family law, care and protection, housing, social security, credit/debt problems, victims' support, financial assistance matters and criminal law.

On behalf of National Legal Aid, the DVU is currently developing a national website with legal information and practical help with domestic and family violence, family law, child protection and civil protection orders. The website also includes content on technology-facilitated domestic and family violence and staying safe online.

The DVU also provides Community Legal Education and Legal Education on technology-facilitated domestic and family violence and safety planning.

All case studies in this submission have been de-identified by changing names, rare characteristics and unique combinations of identifying factors.

Consultation Question 1: What types of technology raise particular human rights concerns? Which human rights are particularly implicated?

In this submission, we refer to 'technology-facilitated domestic and family violence' (**TFDFV**) to describe a broad range of behaviours including the misuse or exploitation of technology as a tactic of domestic or family violence and we use gendered language in this submission to reflect the gendered nature of TFDFV.[1] TFDFV mirrors the in-person, offline sphere where women are overrepresented as victims of domestic and family violence.[2]

TFDFV is a form of gender-based violence, which is a form of discrimination within Article 1 of the Convention on the Elimination of all Forms of Discrimination Against Women

[1] See, e.g., Nicola Henry & Anastasia Powell (2015) Embodied Harms: Gender, Shame and Technology Facilitated Sexual Violence in Cyberspace *Violence Against Women,* 21(6), 758-779; Delanie Woodlock. The Abuse of Technology in Domestic Violence and Stalking. Violence Against Women 2017, Vol. 23(5) 584–602.
[2] ABS, Personal Safety Survey 2017.

(**CEDAW**).[3] Article 2 of CEDAW obliges state parties to legislate to prohibit all discrimination against women.

TFDFV is a common tactic used by perpetrators of domestic and family violence. A 2015 study found 98% of domestic and family violence workers reported they had clients who had experienced TFDFV.[4]

Most technology is neutral and, as acknowledged in the Issues Paper, can be used to help or to harm. For example:

- A 'Smart Home' and house security cameras can make victims feel safer in their home after leaving a violent relationship, while the same technology may have been used to monitor and control them while they were in a violent relationship.
- GPS tracking tiles can be used to find lost keys, while they can also be slipped into a person's car or bag to track their location.
- A person's telephone can be a safety line to help, or can be used to send hundreds of abusive texts, or used to covertly monitor a person.
- Cars can have security systems installed that allow you to track the car and disable the engine if stolen, but can also be used to hinder a person trying to flee violence.
- Drones can be used for leisure, but may also be used to harass or keep a person under surveillance.
- Social media can keep victims connected to friends and support, but can also be a means for intimidation and harassment.
- Some mobile telephone applications can be used for safety and providing victims with critical information, however others can be misused to stalk and abuse victims.

The dual nature of technology means the technology itself may not raise human rights issues, but rather its intentional misuse.

The behaviours that make up TFDFV are not new, but a modern extension of perpetrator behaviour. In particular, they provide more extensive tools for stalking and coercive controlling behaviours.[5] These behaviours can include:

- Harassing a person through their telephone or over the internet. For example, through repeated calls, text messages, emails or over social media.
- Installing surreptitious spyware on a person's device to get their private information, passwords, photos, texts or emails, and to track them. Some spyware can secretly record conversations or access inbuilt cameras.

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

[4] ReCharge: Women's Technology Safety - National Study Findings 2015, www.smartsafe.org.au/sites/default/files/National-study-findings-2015.pdf

[5] See, e.g., Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock & Bridget Harris (2018), Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms, *Feminist Media Studies*, 18:4, 609-625, 611.

- Posting personal information about a person or defaming them online. For example, 'doxxing' involves posting a person's address, phone number or email and encouraging others to harass them, including physically.
- Account takeovers, for example locking a person out of their email, social media or other account. Sometimes this access may be used to interfere with the person's life, such as impersonating them to send offensive messages to work colleagues or family members, to isolate and ostracise them.
- Demanding access to a person's technology, for example by checking call-logs, internet browsing histories, messages, or demanding passwords. This can be used to monitor them to ensure they are not getting help or considering leaving.
- Tracking a person's movements. This can be done through GPS devices, or inbuilt GPS settings on a device or their child's device. In the experience of the DVU, this is a very common tactic and can lead to physical violence.
- Using covert recording devices such as hidden cameras, microphones or webcams to record a person without their consent.
- Recording or sharing intimate images of a person without their consent, or threatening to do this (image based abuse). This may be images made consensually within the context of a relationship, or recorded without consent. For example, using hidden cameras or editing images to make it look like a person is in a compromising position.
- The DVU has had clients who have been sexual assaulted or subjected to sexual servitude where their abuse has involved technology. For example, clients have had their sexual assault recorded, and then hold concerns those recordings may have been distributed.
- Misusing or manipulating technology required to support people with a disability to further isolate the victim.
- Using a combination of social engineering and technology to orchestrate abuse, as shown in Cathy's case:

Case Study 1 – Cathy

Cathy obtained a Police Apprehended Domestic Violence Order (**ADVO**) against her ex-partner Josh, who was emotionally and physically violent towards Cathy throughout their relationship. Josh then initiated a private cross-application for an ADVO for his protection against Cathy.

Attached to Josh's ADVO application were screenshots of threatening messages, allegedly from Cathy's old phone number. Cathy switched telephone numbers some time ago and was unsure how these messages came about.

The DVU agreed to assist Cathy in defending the ADVO against her. Through advocacy to Police, Police investigated the source of the threatening messages. The Police investigation found that Josh had called up Cathy's old mobile service provider, asking for another SIM card for her prior number to be sent to his address. Josh had sent himself these messages to make it look like Cathy was harassing him.

Police charged Josh under s 474.17 of the *Criminal Code 1995* (Cth). The DVU was successful in having his ADVO application dismissed.

These tactics of TFDFV are used to shame, humiliate, intimidate, harass or harm a person. In a context of domestic and family violence, they provide perpetrators with tools to blackmail, deter their victims from leaving or reporting to Police, and can be used to seek retribution, control a person and cause devastating emotional harm.

There is also a link between technology-facilitated stalking and physical harm. For example, the NSW Domestic Violence Death Review Team has identified stalking, including technology-facilitated stalking, as a key risk factor of male-perpetrated intimate homicide.[6]

Therefore, TFDFV can be incompatible with the following human rights:

The right to:

- Life[7]
- Equality[8]
- Privacy[9]
- Not be subjected to slavery or servitude[10]
- Liberty and security of the person[11]
- Not be subjected to torture and other cruel, inhumane, or degrading treatment or punishment.[12]

Many of the technologies that are implicated are everyday technologies and devices. More consideration needs to be placed on how technologies of convenience can be manipulated and misused to extend stalking and coercive controlling behaviours. However, there are some technologies that raise particular human rights concerns, and which are less neutral in design.

[6] New South Wales Domestic Violence Death Review Team (NSW DVDRT) (2015) *Annual Report: 2013 –2015.* NSW Government: Sydney.
[7] *International Covenant on Civil and Political Rights (ICCPR)* ratified by Australia on 13 August 1980, Articles 3 and 6.
[8] Ibid, Articles 2 and 3.
[9] Ibid, Articles 3 and 17.
[10] Ibid, Articles 3 and 8.
[11] Ibid, Articles 3 and 9. Also see 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 – *"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…For example, States parties must respond appropriately to…violence against women, including domestic violence…"*
[12] *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.

Spyware

Legal Aid NSW holds particular concerns about the use of spyware in a context of domestic and family violence.

Spyware is malware that can be installed on devices such as computers, tablets and smart phones to secretly monitor a person's private information. Spyware may access keystroke logging (all typed information including passwords), photos/videos, social media accounts, applications, contacts, notes, browsing history, call logs, text messages, email, location, activate your camera, microphone or record calls. It may be used to delete things from a device, block certain websites or numbers and may be remotely deleted. Some spyware is remotely installed onto a device, some requires access to the device, and some devices can be bought with spyware pre-loaded on it.

Spyware is commonly advertised as a means for parents to make sure their children are safe or for business to protect against embezzlement. However, it is the experience of the DVU that spyware is commonly used in domestic and family violence situations to covertly monitor a person. Even if these products were used for their advertised purpose, there could still be serious human rights implications.

The use of surveillance devices is prohibited to different degrees through a patchwork of State and Territory legislation.[13] The sale[14] and use[15] of spyware is also arguably prohibited through Commonwealth laws. Despite this, spyware continues to be available in Australia, and can be accessed by people lacking any technological savviness with relative ease. A simple Google search reveals numerous available products such as mSpy, FlexiSpy, TruthSpy, Highster Mobile, Hoverwatch, and Mobile Spy.

In a context of domestic and family violence, spyware could be very dangerous. It is difficult to detect and difficult to remove from a device. It is challenging to provide evidence of, especially as it can often be deleted from the device remotely. Obtaining information from the manufacturers can be challenging as most of them are located outside Australia.

It is a unique form of abuse as victims may be completely unaware it is happening. This makes it challenging to screen for and to 'safety plan' around, making the victim more vulnerable to harm, as can be seen in Grace's case:

[13] See, e.g., *Listening Devices Act 1992* (ACT); *Crimes Act 1900* (ACT), s 61B; *Surveillance Devices Act 2007* (NSW), *Surveillance Devices Act 2007* (NT), *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).
[14] See, e.g., *Criminal Code 1995* (Cth), s 474.4.
[15] See, e.g., *Telecommunications (Interception and Access) Act 1979* (Cth), s 7.

Case Study 2 – Grace

Grace was in a long-standing violent relationship with her husband Steve. She also has an illness that requires extensive treatment. Steve moved out of their house a year ago but continued to turn up uninvited. Neighbors told Grace they often see Steve hiding outside her house and watching her from a car parked outside the house. Grace received many harassing and controlling messages from Steve.

Before Steve moved out, he set up Grace's iPhone for her. She's not sure what her Apple ID is to change her iCloud password. She was worried about how Steve is getting information about her as he seems to know about private conversations she had with her daughters in the house. One evening, he turned up at the restaurant where she was having a date and he caused a scene. She thought Steve may have bugged her house.

When Grace separated from Steve, he withdrew all of their joint savings including money Grace had saved for her treatment. Steve told Grace he would give her back the money for her surgery if she agreed to return to him.

Grace started a new relationship with another man. She sent a nude picture of herself to her new boyfriend. Within minutes, Steve sent her a text message that contained the photo she sent to her new boyfriend. Grace was confused how Steve could have this image. Her new boyfriend had never met Steve, and she could not imagine him sharing it.

Grace was scared Steve would circulate this photo, including to her children. A DVU lawyer gave her advice and informed her the most likely scenario is that Steve has spyware on Grace's phone. The DVU lawyer set Grace up with a free WESNET Smart Connections phone.

When the DVU followed up with Grace, she told them she reconciled with Steve because she was scared of what he will do. She said she felt safer being with him, compared to the constant state of fear and anxiety she experienced while separated.

Spyware is incompatible with the right to privacy under Article 17 of the *International Covenant on Civil and Political Rights.*[16] General Comment No 16 on Article 17 notes, '*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'*.[17] While Australia has laws that regulate, companies continue to sell these products to perpetrators of violence. Perpetrators continue to use these products with

[16] *International Covenant on Civil and Political Rights (ICCPR)* ratified by Australia on 13 August 1980.
[17] 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.

relative impunity. The DVU has had multiple matters where there has been evidence of spyware use, and no police action was taken.

Spoofing

Another technology that can be challenging for people affected by domestic and family violence is the use of spoofing applications and websites. Spoofing technology can be used to create false evidence (for example, screenshots of fake messages) or to make it look like a different number has sent a message or made an incoming call (for example, making the phone display 'mum' when it is someone else calling). Some spoofing technology can change the sound of a person's voice on a call.

This blurs borders of what is real, and creates challenges for evidence in court proceedings. Some spoofing technology exists to allow businesses to make calls without displaying a personal number. However, in the experience of the DVU, the majority of the expanding range of spoofing products are not targeted at any legitimate business purpose.

Case Study 3 – Azra

Azra is a young Pakistani woman from a traditional family. She had a boyfriend, but was keeping this secret from her family as she knew they would not approve.

Azra's boyfriend was controlling and his behaviour began to scare her. He was pressuring her sexually and wanted her to run away with him and get married. Azra told her family about the relationship because she became fearful he would come to her house and do something. With the support of her family, Azra ended the relationship.

After ending the relationship, Azra began receiving strange messages from her ex-boyfriend. They looked like screenshots of WhatsApp message conversations between her mother and her ex-boyfriend. The messages looked real, but their content was unusual. The messages suggested that Azra's mother was deeply disappointed and ashamed of Azra and was planning to force her to marry her cousin. Her ex-boyfriend tried to use these messages to convince Azra to get back with him and run away.

Azra confronted her mother, and together they realised her ex-boyfriend was using a program called 'WhatsFake' to create these screenshots of fake messages. Azra reported the matter to Police, who supported her to get an ADVO for her protection, including a no contact order.

After Azra had an ADVO made for her protection, she began receiving calls on her phone that came up on her phone as 'mum.' When Azra picked up the phone, she discovered the call was in fact from her ex-boyfriend. As the call logs on her phone said the call had come from her mother, she had difficulty reporting breaches of the ADVO

to Police. Azra had to change her phone and number to stop her ex-boyfriend contacting her.

Consultation Question 2:
What are the key issues regarding new technologies for particular groups of people?

As outlined below, TFDFV presents a range of complex issues for women experiencing domestic and family violence.

Lack of understanding of TFDFV as a form of domestic and family violence

As TFDFV is a relatively new concept, victims may be less able to identify they are experiencing a form of domestic or family violence, or the services working with them. Difficulties can be compounded when the victim is experiencing other forms of disadvantage.

Lack of legal recognition

TFDFV is not always recognised in legal frameworks as a crime or a distinct form of domestic or family violence. Legal definitions may allude to controlling and coercive behaviour, but not specify technology-facilitated abuse.[18] Some forms of technology-facilitated abuse, such as image based abuse, have only recently been criminalised in some jurisdictions.[19] Western Australia, Tasmania and Queensland are yet to introduce any specific legislation to criminalise this form of abuse.

There are also resourcing challenges for Police to assist in some TFDFV matters, even where the behaviours are legally recognised as crimes, as can demonstrated in the cases of Yasmin and Pip:

Case Study 4 – Yasmin

Yasmin was in a 10-year marriage with Cyrus. During the relationship, there was frequent physical violence and Cyrus often threatened to kill himself to get Yasmin to comply with his demands. Cyrus coerced Yasmin to participate in various sex acts which he often recorded. Yasmin did not want to make these recordings, but felt she had little choice as she feared what Cyrus would do to her, and himself, if she did not comply. He

[18] See, e.g., *Family Law Act 1975* (Cth) s 4AB. However, see ALRC*, Review of the Family Law System.* Discussion Paper No 86 (2018), Proposal 8-1, which proposes to clarify the definition of family violence includes technology facilitated abuse.
[19] See, e.g., *Crimes (Intimate Image Abuse) Amendment Act* 2017 (ACT); *Crimes Amendment (Intimate Images) Act 2017* (NSW); *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth).

often threatened to send the recordings to her family members and community if she ever tried to leave him.

One evening, Cyrus prepared Yasmin a drink. She felt very woozy and fell asleep. Yasmin woke up the next day on the ground in their lounge room with serious injuries. She had difficulty getting up and was haemorrhaging blood from her vagina. She was covered in unexplained cuts and bruises, and later discovered she had a broken rib.

Yasmin found Cyrus' phone on a table near her and picked it up to check the time. She unlocked it and found a page open on a Tor (Dark Web) browser on a 'Rape Porn' website, where there were messages between users negotiating a price for one user to send a video of a 'violent gang rape of his wife.' Yasmin sent herself a screenshot of the message, but was too scared to take his phone. She took their shared laptop and fled. A week later, she reported to Police and tried to hand over the laptop. She feared Cyrus had assaulted her and filmed it.

Police charged Cyrus with other domestic violence offences but told Yasmin it would be too difficult to prove anything related to Cyrus soliciting the video, the possible sexual assault, or to check for encrypted videos. His other devices were not seized.

Police told Yasmin it would be too expensive to do a forensic sweep of the shared laptop. Yasmin has spent over $20,000 of her own money on having a computer specialist do a forensic report. This has not led to any further evidence or charges.

Case Study 5 – Pip

Pip has a maths tutoring business with an online website. Her ex-partner, Mark, set up a website with a very similar URL to Pip's business website. Mark used his website to denigrate Pip. He included edited images where her head had been superimposed onto images of women in embarrassing and compromising positions. However, none of these images depicted any nudity.

He also used the website as a platform to defame Pip, making wild accusations about her being a paedophile, a thief and a danger to children. This had a significant impact on Pip's income, work and mental health. He updated it with new accusations daily.

Mark copied and pasted Pip's work email group while they were together. He sent the URL of his website to her client list. He also made business cards that looked like hers, but which have his website's URL and an email address that is similar to Pip's, but which is not her actual email address. Mark distributed these business cards around Pip's suburb, including in her letter box. Pip also started receiving at least 10 harassing emails each day, all from what appear to be fake email accounts.

Pip reported this to Police. However, she was told there was no way of proving Mark was responsible for these actions and there was nothing they can do. The DVU offered to help Pip with pursuing a private ADVO against Mark. However, Pip said she was too tired to fight and planned instead to move interstate.

Not knowing the abuse is happening

Victims may be completely unaware they are subject to TFDFV until it has in-person implications. For example, they may not realise their or their child's device is affected by spyware, the other party has access to their passwords and accounts, has set up mail-forwarding on their email or is using the in-built GPS settings of their smartphone to track them via Find My Phone.

This can present challenges for effective safety planning and make it more difficult to predict future harm. The following case studies demonstrate not only how technology can distort a victim's self-assessment of risk, but also how it can magnify the victim's perception of the perpetrator's capabilities. Some victims lose trust in all technology and 'disconnect,' which may escalate their level of risk.

Case Study 6 – June

June left Bob two months ago after a long relationship involving domestic violence. She relocated with the children to an address unknown to Bob.

June was asked about the safety of her devices by her social worker, but she was convinced they were secure. She also changed her passwords as a precaution.

Bob sent June a screenshot of a letter she received in her email inbox which included her new address. Nothing else was written in the message. June reported this to Police as she was terrified Bob would come to her home and harm her. Police told her the screenshot did not amount to 'stalking' or 'harassment' and there was no way to prove how Bob got this letter. June decided to relocate again.

June was still not convinced her devices were being covertly monitored through spyware, or that mail forwarding could be set up on her email. She told her lawyer and social worker that he is just "well connected" to people who can access her information for him. Police inaction has made her suspicious that he may know someone in the Police who accessed her email account for him, and she said she "wouldn't bother" going to the Police again.

Case Study 7 – Maria

Maria has been in a high-risk domestic violence relationship for 14 years. She has a high-school age daughter. She fears for her safety and that of her child, and decided to leave with the help of a DVU social worker.

As it was school holidays, and she had no family in Australia and no money for a baby-sitter, Maria brought her child into the DVU office. The social worker set her child up in a separate room with some activities while she helped Maria organise emergency money, accommodation and conduct safety planning.

While Maria was there, her husband called their daughter on her smartphone, demanding to know why they were at Legal Aid. Maria and her daughter were unaware that her husband had been using the smartphone he set up for their daughter as a means to monitor and track them.

Not understanding how the abuse is happening

The victim may suspect her technology has been compromised, but not know how the abuse is happening, which can exacerbate her concerns that she will not be believed. For example, she may not know how the person is accessing her texts or emails, or how they know her location. There are further issues with this form of violence being trivialised and minimised, as it is often perceived as less serious than physical violence.[20] This can lead to inadequate responses from law enforcement, the community and the victim themselves. Some service providers may not be aware of the current capabilities of technology, which may lead to the victim not being believed.

Fear of retribution through technology

If a victim is concerned a person will share intimate images of her without her consent, she may be reluctant to disclose domestic and family violence to service providers out of fear the perpetrator will carry out those threats. If a victim is concerned about spyware on her device, she may be reluctant to disclose due to concerns the perpetrator may be covertly monitoring her.

Practical difficulties of improving technology safety

The *COAG Final Report* acknowledged that while some women's services offer safety advice, victims are typically expected to take steps themselves to increase their digital

[20] See, e.g., Tammy Hand, Donna Chung & Margaret Peters (2009) *The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation.* Australian Domestic & Family Violence Clearing House, Stakeholder Paper 6.

safety.[21] There can be a tension between empowering victims to increase their own technology safety and the practical difficulties of expecting them to action advice without assistance. Further, if frontline responders recommend that women experiencing TFDFV simply disconnect from technology where the abuse is taking place, this can be a form of victim-blaming. Victims also have the right to access and use technology safely.

There are a number of potential barriers to victims actioning technology safety advice without help. For example, they may:

- lack sufficient technology expertise to update their accounts or devices themselves
- have no access to a safe device to change their account settings or look up how to do this
- not appreciate how changing her settings, passwords or accounts will improve their safety, or the real-world ramifications of not following advice
- be overwhelmed by the steps involved
- find it difficult to navigate while experiencing trauma.

There are further barriers for women at the intersection of multiple forms of disadvantage. Research suggests that Aboriginal women, culturally and linguistically diverse women, and women with disabilities are overrepresented as victims of TFDFV.[22] This can exacerbate existing technical challenges of actioning technology safety advice because of, for example, language barriers or having even less access to safe technology.

An absence of practical hands-on assistance in making a woman's technology safer may increase her level of risk. She may ignore advice and become increasingly fearful of technology, including protective forms of technology, or shut down and avoid all forms of technology. Disconnecting from technology may increase a person's sense of isolation, create difficulties in contacting support services or, in some instances, escalate violence.

The case study of Hanzi below provides an example of a person who was experiencing trauma, in crisis and had limited skills and English, and found overcoming the barriers to increase her technology safety too great. Increasing technology safety can often place a lot of responsibility on a victim who may not be able to take the necessary steps.

Hanzi may have benefited from ongoing help through digital empowerment lessons to increase her safety in a staggered and trauma-informed way.

Case Study 8 – Hanzi

Hanzi is from Taiwan and speaks no English. Her ex-partner set up her iPhone for her and she is unaware what the Apple ID is to change the settings on the device. Her ex-

[21] COAG Advisory Panel on Reducing Violence against Women and their Children, *Final Report* (2016), 48.
[22] ReCharge: Women's Technology Safety - National Study Findings 2015, www.smartsafe.org.au/sites/default/files/National-study-findings-2015.pdf

partner seemed to know where she is, and began turning up where she is. Once he turned up when she was unloading her groceries at a shopping centre far away from her home, and began yelling at her and pushed her up against the car.

The DVU gave Hanzi a new WESNET Telstra Smart Connection Phone, helped her set it up and gave her technology safety planning advice. However, Hanzi found the phone too dissimilar to her old device. Hanzi said it was easier to keep using her old phone because all her contacts were on that phone and she understood how it worked.

Practical difficulties for frontline workers

While excellent training is offered by eSafety Women and WESNET to build frontline worker's skills, there remains some hurdles for workers in assisting clients with increasing their technology safety. These challenges have been explored in some recent American research, and include:

- professionals feeling they lacked sufficient expertise to assist clients, even with training on TFDFV
- professionals feeling training on TFDFV often focused on awareness raising on the types of tactics, rather than building skills to manage risks
- a lack of practical resources and guides with actionable advice, identifying that many resources were too vague or out-of-date
- keeping up with the pace at which technology changes
- needing to 'Google-as-they-go' to look up how to change online settings, and then not knowing whether the information they have found is reliable or trustworthy
- TFDFV not being embedded into organisational screening, risk assessment or safety planning protocols or tools
- trying to avoid telling clients what to do and working from an empowerment model
- difficulties in helping clients understand the importance of improving their technology safety. [23]

In addition to these barriers, the Victorian *Royal Commission into Family Violence* has also highlighted challenges for domestic and family specialist services that can impact upon service delivery. These include a lack of funding and resourcing, high staff turnover, short term contracts, time constraints, access to professional development and vicarious trauma.[24]

[23] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing Article 46. Publication date: November 2017.

[24] Royal Commission into Family Violence (2016), *Summary and recommendations*, Parliamentary Paper No 132

Technology being used to 'set-up' victims

The DVU has encountered many clients who present as primary victims of domestic and family violence, but end up as defendants in criminal or ADVO matters where technology has been used against them. For example, where their ex-partner has had access to their online accounts and sent themselves threatening emails, to make it look like they are the victim. Research suggests it is not uncommon for women experiencing domestic and family violence to be misidentified as an aggressor in police matters,[25] as demonstrated in Jin's case:

Case Study 9 – Jin

Jin is originally from China. She has been with her husband for 1.5 years, and he subjected her to ongoing physical and emotional violence. She tried to leave a number of times, but has no family and limited support in Australia. Jin and her husband had an argument, which led to him strangling her. Jin was scared and when she broke free from him, she ran out of the apartment.

Jin was crying outside her apartment on the steps when the Police arrived. She had not called them and was confused. Jin did not want to get her husband into trouble, so she did not tell the Police about him strangling her. She is also on a temporary partner visa and was worried about him "having her deported", as he had threatened in the past.

After Jin refused to give the Police a statement, they arrested her. While Jin was outside, her husband had sent himself an email from her account on their shared computer – he emailed 'I will kill you, you will see.' Jin was charged with intimidation, and a Provisional ADVO was made against her for her husband's protection.

Jin received legal assistance from the DVU and support from the DVU social worker to make a statement to the Police.

Consultation Question 3:
How should Australian law protect human rights in the development, use and application of new technologies?

To assist victims of TFDFV, we recommend the following actions:

[25] Julia Masour, Women Defendants to AVOs: What is their experience of the justice system? *Women's Legal Services NSW,* March 2014.

Recommendation 1 **Review of stalking provisions, civil protection order legislation and conditions in each State and Territory to ensure TFDFV captured**

Despite civil protection orders now being nationally recognised, each State and Territory has different legislation and different conditions available on orders. Some jurisdictions address TFDFV better than others.

Across Australia, specific conditions can be drafted to suit the circumstances of a civil protection order. Some jurisdictions like NSW, ACT and Queensland have set conditions available to stop a person trying to locate or find the protected person, while other jurisdictions like the NT do not. Conditions that prohibit a person from trying to locate the protected person are helpful in TFDFV matters, where victims may be under covert surveillance. South Australia and Victoria have an express condition to prohibit a person being followed or kept under surveillance.

Some jurisdictions do not currently include forms of technology-facilitated stalking in their legal definitions of stalking for a civil protection order, such as the NT and NSW. Some jurisdictions, like WA, have explicitly incorporated cyberstalking into their definition of family violence.[26]

In NSW, Parliament has recently enacted changes to the *Crimes (Domestic and Personal Violence) Act* to address cyberbullying.[27] The amendments include expanding the definition of stalking to include '*contacting or otherwise approaching a person using the internet or any other technologically assisted means*.' However, it remains unclear whether the use of spyware would be considered an 'approach' to satisfy this definition.

Some jurisdictions have expanded criminal definitions of stalking to include technology-facilitated stalking. For example, Tasmania[28] and Victoria[29] include technology-facilitated behaviours in their criminal stalking definitions. However where spyware or tracking devices have been used, and the intention is for the victim to remain unaware of its use, this may create issues due to the requirement of intent to cause physical or mental harm or apprehension of fear.[30]

Recommendation 2 **Review each State and Territory's surveillance devices legislation**

Each State and Territory currently has a patchwork of legislation that covers surveillance devices. For example, the ALRC found that *"optical surveillance devices are not regulated by the surveillance devices laws of ACT, Queensland, SA or Tasmania… Tracking devices*

[26] See *Restraining Orders Act 1997 (WA),* s 5A.
[27] *Crimes (Domestic and Personal Violence) Amendment Act 2018* (NSW), section 8.
[28] *Criminal Code 1924* (Tas), s 192.
[29] *Crimes Act 1958* (Vic), s21A.
[30] See, e.g., *Gale v the Queen* (2014) VSCA 168.

are not regulated by the surveillance devices laws of ACT, Queensland, SA or Tasmania."[31]

In some jurisdictions, like NSW, it is an offence to record a private conversation without consent, but there are exceptions such as to protect a lawful interest.[32] This legislation sometimes affects victims of domestic and family violence. For example, the DVU has had many clients who have recorded potential breaches of AVOs on their device. Despite the exception, clients have been warned by Police that by making the recording, they may have committed a criminal offence and they could be arrested. This acts as a deterrent for some women reporting ongoing violence. The ALRC has previously proposed that surveillance devices laws be made uniform throughout Australia. [33]

Recommendation 3 **Utilising existing laws against companies selling spyware and private use of surveillance devices to perpetrate TFDFV**

As previously mentioned, there are existing laws to prohibit the use of surveillance devices to perpetrate domestic and family violence, and the sale of such devices. We recommend these laws be utilised and that stronger measures be taken to prevent companies supplying or advertising spyware. Options to improve compliance with subpoenas by offshore companies could also be considered.

Recommendation 4 **Continue to review and consider image based abuse laws**

Each State and Territory except Queensland, [34] Western Australia[35] and Tasmania has introduced specific image based abuse offences. The Commonwealth Criminal Code has also recently introduced aggravated offences relating to image based abuse.[36] We recommend each jurisdiction have specific image based abuse offences and that these be regularly reviewed to ensure they are effective.

Recommendation 5 **Supporting proposed amendments to the *Family Law Act***

The Australian Law Reform Commission has recently proposed amendments to the section 4AB definition of family violence in the *Family Law Act 1975* (Cth).[37] This includes adding technology-facilitated abuse into the list of non-exhaustive examples of family

[31] ALRC, *Serious Invasions of Privacy in the Digital Era.* Discussion Paper 80 (DP 80). March 2014.
[32] *Surveillance Devices Act 2007* (NSW), s7
[33] ALRC, *Serious Invasions of Privacy in the Digital Era.* Discussion Paper 80 (DP 80). March 2014.
[34] However, see *Criminal Code Act 1899* (Qld), ss 227A & 227B.
[35] However, see *Police Offenders Act 1935* (Tas), ss 13A, 13B & 13C.
[36] *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth).
[37] See ALRC, *Review of the Family Law System*. Discussion Paper No 86 (2018), Chapter 8.

violence.[38] We support this proposal in principle, subject to further consultation on specific wording.

We also note an emerging trend of parents involving their children in TFDFV. An example is putting GPS location devices in children's toys, gifting children with devices that have been set up with spyware or Find My Phone activated to find the other parent's address, or asking a child to record their other parent covertly. [39] These acts may expose children to family violence, and therefore may sometimes be considered as a form of child abuse under section 4 of the *Family Law Act 1975* (Cth). Further consideration is required of this emerging trend.

Recommendation 6 **Evaluation and consideration of laws that protect victims placing offenders under electronic monitoring**

We note that in some jurisdictions such as Tasmania and NSW, electronic monitoring of domestic violence offenders is being trialled or used. We support the continued evaluation of these measures.

Recommendation 7 **Streamlining legislation, regulations and policies around victims using AVL facilities and other means to give evidence remotely**

We support legislation that protects vulnerable witnesses, such as victims, giving evidence in court proceedings, including through AVL and other technologies. Ready access by victims to such facilities should be prioritised. In the experience of the DVU, there are some practical hurdles for victims to access AVL, especially in NSW Local Court AVO and criminal matters where Police Prosecutors may not view an application to appear via AVL as necessary.

Recommendation 8 **Ensuring proper consultation with domestic and family violence service providers for proposed law reforms**

It is critical that domestic and family violence services continue to be involved in meaningful consultation on law reform efforts, especially those relating to data collection and retention, which have may have unforeseen consequences for victims (such as metadata laws and My Health Record).

We support the recent expansion of the eSafety Commissioner's powers in relation to the civil penalty regime for image based abuse.[40]

[38] Ibid, [8.33].
[39] See, e.g., Heather; Burdon, Mark --- "Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence" (2018) 41(1) *University of New South Wales Law Journal* 157; *Heaton & Heaton* (No 2) [2017] FCCA 557, *Chalmers & Chalmers* [2015] FCCA 2103.
[40] *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth).

Consultation Question 4:
In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?

Below are some suggestions to help promote and protect human rights in the context of TFDFV.

Training, risk assessment guides and workforce development

Education and training regarding TFDFV should be provided to all frontline services that come into contact with people affected by domestic and family violence.

We note eSafety Women and WESNET already provide training in-person and online. This program includes in-depth training and practical tips for frontline workers to help them better help their clients, and online training is widely accessible to most frontline workers. However, we suggest that TFDFV should be better incorporated into mainstream training and resources around domestic and family violence, including in risk assessment practice guides and training around risk assessment tools.[41] Embedding TFDFV into standard domestic and family violence training is supported by the *COAG Final Report,*[42] which noted that training should consider the dangers and opportunities of technology where appropriate.[43]

Despite the fact that the ANROWS Risk Assessment Principles Companion Resource acknowledges technology-facilitated abuse as a form of domestic and family violence, TFDFV is not well acknowledged in Australia's publically available[44] risk assessment frameworks or practice guides. [45] A recent review of the Victorian CRAF recommended its redevelopment address TFDFV,[46] and the Victorian Multi-Agency Risk Assessment and Management (MARAM) Framework Practice Guide is still in development.

[41] For example, in the Northern Territory, the Family Safety Framework involves a one-day training seminar, in South Australia, Government Departments are responsible for training their staff in their Family Safety Framework and some training is funded for specialist services. In Victoria, there was training through the eCRAF and face-to-face training by Child Youth and Family Services for Common Risk Assessment and Risk Management Framework (CRAF). There are opportunities to integrate TFDFV into training such as this.
[42] COAG Advisory Panel on Reducing Violence against Women and their Children, *Final Report* (2016). Recommendations 1.4 and 2.2.
[43] Ibid, 48.
[44] For example, the Tasmanian Risk Assessment Safety Tool (RAST) used by Police, and the Queensland Domestic and Family Violence Common Risk and Safety Framework, and their associated practice guides are not publically available.
[45] See, e.g., NSW Government, *Domestic Violence Safety Assessment Tool (DVSAT) Guide*, June 2015; NT Family Safety Framework Manual; SA Family Safety Framework Manual. Also see Jennifer E. McIntosh and Claire Ralfs (2012). The DOORS Detection of Overall Risk Screen Framework. Australian Government Attorney-General's Department, Canberra and its accompanying Handbooks, Parent Self-Report Form and Practitioner Aide Memoire. However, see the Western Australian Family and Domestic Violence Common Risk Assessment and Risk Management Framework (2nd ed., 2015), which includes examples of TFDFV.
[46] McCulloch, J., Maher, J., Fitz-Gibbon, K., Segrave, M., Roffee, J., (2016) *Review of the Family Violence Risk Assessment and Risk Management Framework (CRAF).* Monash University, Recommendation 12.

We acknowledge that risk assessments tools are often actuarial in nature and based on risk factors garnered through extensive domestic violence homicide research. We do not suggest changing reliance on evidence-based risk factors. Rather, we suggest that TFDFV should be acknowledged as an extension of stalking and coercive controlling behaviour and incorporated into each framework's updated practice guides and associated training.

For frontline workers, it is important that they have the skills required to respond to TFDFV, especially in providing technology safety planning. TFDFV should be integrated into workforce capability plans, which only happens rarely at present. For example, the Victorian Government's Responding to Family Violence Capability Framework was developed in response to the Victorian Royal Commission into Family Violence. However, this framework contains no explicit mention of TFDFV. The Australian Association of Social Workers have also developed a Capability Framework that also does not mention TFDFV.[47]

The ALRC has recently proposed a workforce capability plan for the family law system.[48] We suggest that specialist domestic and family violence workers and other frontline workers such as Police require advanced skills in TFDFV. This should be reflected in capability plans and through resourcing training and development opportunities.

Education on TFDFV is also required for the legal profession, judiciary, young persons and the community more broadly. The DVU lawyers also operate the Family Advocacy and Support Service (**FASS**) in NSW Family Courts (Sydney, Parramatta, Wollongong and Newcastle Registries). All DVU/FASS lawyers have had training around TFDFV and technology safety planning, the benefits of which are demonstrated in Alice's case:

Case Study 10 – Alice

Alice came to see Sydney FASS about her family law issues. She also mentioned that her partner seemed to know where she was going and what she was doing. The FASS lawyer identified this TFDFV issue and assisted Alice to work through possible vulnerabilities and ways her ex-partner could be getting this information.

Through their discussions about her technology, what her ex-partner had access to and the situations that had happened recently, the FASS lawyer recommended Alice check her car for a GPS tracking device.

Alice later took her car to get checked by a mechanic. The mechanic found a GPS tracking device wired into the car. Alice called the FASS lawyer to let her know.

[47] Australian Association of Social Workers, *AASW Family Violence Capability Framework,* 2018 <https://www.aasw.asn.au/document/item/10951>

[48] Australian Law Reform Commission, *Review of the Family Law System*, Discussion Paper No 86 (2018)

Digital empowerment workshops for victims of domestic and family violence

Digital empowerment workshops could be developed as a standalone program, or be incorporated into existing healing and group work sessions for women who have experienced domestic and family violence. This would fill an identified service gap, as a recent study found that '*many clients expressed frustration at how challenging it was to learn how to protect themselves with respect to technology, describing how they would spend hours searching for information on Google, but "get nowhere."*'[49]

Digital safety aids for TFDFV

Across the US, New Zealand, Canada and Australia, 'digital safety aids' have been developed, underpinned by significant research.

In Australia, I-DECIDE[50] is an example of a 'digital safety aid.' The website allows a person affected by domestic and family violence to log-in and complete a free online self-assessment. It asks the user questions to undertake a detailed risk assessment. After completing the survey, the user is given information about her level of risk, her safety needs and a tailored safety plan. Evaluation of digital safety aids such as this have shown promising results.[51]

Presently, I-DECIDE does not provide any safety assistance specific to TFDFV. More work is required to explore how digital safety aids such as this could be adapted for TFDFV. For example, whether they could provide technology safety planning assistance and step-through technical support.

To keep up with evolving technologies, there are opportunities for telecommunication providers, computing technology companies and social media companies to assist with the development of a digital safety aid for TFDFV. For example, an issue identified by recent research is that victims find it difficult to find reliable and easy-to-follow information about updating settings on their device[52]. These companies could help by providing updated safety information or guides on their products as they evolve, which could be updated on the digital safety aid.

---

[49] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. *Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders*. PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing Article 46. Publication date: November 2017, 11.

[50] www.idecide.org.au

[51] See, e.g., Glass. N. "The Longitudinal Impact of an Internet Safety Decision Aid for Abused Women." *American Journal of Preventive Medicine*. 2017;52(5):606–615.

[52] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. *Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders.* PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing Article 46. Publication date: November 2017.

This idea is consistent with recommendations from reports for technology innovations. For example, the *COAG Final Report* recommended alliances between government and national corporates to address violence against women, in particular, to '*safeguard their products and services from being used to facilitate violence*.' [53]

Further research is required into the costs, usability, accessibility, risks and technological requirements for the development of a digital safety aid for TFDFV.

[53] COAG Advisory Panel on Reducing Violence against Women and their Children, *Final Report* (2016). Recommendations 1.2.