# Submission to the Select Committee on Social Media and Online Safety

***This submission focuses on online harms to which domestic and family violence (DFV) victim-survivors are subjected. It emphasises that coercive and controlling behaviours enacted by perpetrators through technology cannot be viewed as isolated instances but must be understood as part of a pattern of abusive behaviours that intend to entrap those who are targeted. It is vital that digital coercive control (also referred to as technology-facilitated coercive control) is understood in the context of DFV. Some acts of digital coercive control may be readily and easily recognised by police, courts, platforms, and the tech industry, and may be outlined in user code of conducts or criminalised. However, other acts may be overlooked and, consequently, victim-survivors dismissed when they disclose, report, or seek assistance.***

***We recommend that there is recognition of digital coercive control and for state agencies and tech companies and platforms to enhance their identification and response to this issue. There are extensive and devastating impacts of digital coercive control on a victim-survivor's physical, psychological, and emotional wellbeing and health and sense of security. Offline harms cannot be divorced from online harms. Our lives are inextricable from the digital world and technology plays key roles in our lives, enabling education, employment, social interactions, civic participation and entertainment, leisure as well as management of health, finance, and household affairs. Furthermore, technology provides access to information and support – such as survivor collectives – which are highly valued by victim-survivors and can assist in help-seeking and accessing support. Additionally, digital coercive control can potentially signal 'homicide flags' – risk of fatal violence – such as obsessive behaviours, coercive control and stalking. We stress that it is not only intimate partners who are affected and targeted, but their children, other family members, friends, and new partners.***

***Governments and social media companies have a responsibility to address digital coercive control. Victim-survivors expend significant time, energy, and resources in efforts to reduce, prevent and respond to these harms. However, too often there is a failure to address and support victim-survivors and they are expected or encouraged to engage in this 'safety work'. We emphasise that 'doing safety work' in fact limits women's ability to exercise and enjoy the same freedoms as men in our society. This signals that communities are failing to meet standards of gender equality/equity – gendered drivers of violence against women – and continues to place the burden on women, preventing our independence being exercised and our participation in private and public decision-making. Thus, gendered drivers of violence are exacerbated. Additionally, victim-survivors they may feel as though they need to or are told to change their use of social media and the internet or to disengage completely from technologies. This is highly problematic and unreasonable.***

***The submission is authored by Bridget Harris, members of the Independent Collective of Survivors, Molly Dragiewicz, Delanie Woodlock***

*Bridget Harris* is an Associate Professor, Australian Research Council DECRA Fellow[1], Queensland University of Technology (School of Justice) and Adjunct in Criminology, University of New England.

*The Independent Collective of Survivors* is a national independent body that seeks to enable and empower victim survivors' use of their lived expertise to reduce gendered violence by improving real world outcomes across prevention, early interventions, response, and recovery.

*Molly Dragiewicz* is Associate Professor, Criminology and Criminal Justice, Griffith University

*Delanie Woodlock* is a Research Fellow in Criminology at the University of New England

*This submission draws directly on some sections of: Harris, Dragiewicz & Woodlock's Submission on Online Safety Legislative Reform (2021) and Harris, Woodlock & Dragiewicz (2020), but does not replicate these submissions.*

[1] Her current DECRA research, referred to in this submission, seeks to enhance responses to technology-facilitated DFV.

# Table of Contents

## a) The range of online harms that may be faced by Australians on social media and other online platforms, including harmful content or harmful conduct;

This response focuses on the harms to which DFV victim-survivors are subjected. Technology can be weaponised and damaged by perpetrators in a range of ways. These behaviours do not exclusively occur online, using social media or other online platforms, but for the purposes of this inquiry, we focus on these channels in the pages that follow.

**Technology is deployed by DFV perpetrators - during relationships and post-separation - to enact abuse and to engage new forms of abuse. 'Offline' and 'online' abuse are not distinct categories** (Barter et al., 2017; Dragiewicz et al., 2019; Draucker & Martsolf, 2010; Fraser et al., 2010; Harris & Woodlock, forthcoming; Marganski & Melander, 2015; Woodlock, 2013). Emotional, psychological, financial, and sexual abuse and in-person stalking can be facilitated by or performed using technology. For example, perpetrators might send social media messaging or posts to gaslight or demean, which constitute psychological and emotional abuse, respectively. Financial abuse (such as control accounts) can be achieved through online banking. Using technology, intimate images and video (real or 'deep fakes') can be created and/or distributed (or there may be a threat to distribute), without the consent of victim-survivors. Posting or sharing (or threatening to post or share) these images (and / or images of sexual assault) through social media or internet sites can result in attempted sexual coercion. Monitoring and surveillance (stalking) using technology (such as through social media and internet usage) can enable in-person stalking (McLachlan & Harris, forthcoming).

Technology can also be used to enact digital harms. ***Technology-facilitated DFV*** is an umbrella term, which can include (but is not limited to):

- **Sending or posting abuse or harassment** (intended to distress or defame) using information communication technologies;
- Publishing a private and identifying information (**doxing**);
- Creating and/or publishing / distributing sexualised content (**image-based sexual abuse**) without consent of persons pictured / recorded. This may include the

creation and or publishing / distribution of synthetic media (deepfakes) in a person's likeness or using part of their image;

- **Impairing the function of a device or account or causing an unauthorised function on a device or account** (including hacking an account);
- **Impersonation** of a victim-survivor or another person in efforts to intimate, abuse, harass, defraud or steal a target's identity;
- **Stalking**; using technology to monitor the movements, activities or communications of a target (Harris, 2020: 1; see also Dodge & Johnstone, n.d.; Douglas, Harris & Dragiewicz, 2019).

**Perpetrators can obtain access to victim-survivor's passwords, email and social media accounts** and use this access **to monitor and track survivors.** They **use harassment to place victim-survivors under surveillance and pressure victim-survivors** to report on their activities and movements (Harris & Woodlock, forthcoming a).

The **abusive messages** that women receive during relationships and post-separation are often **gendered and sexualised**. These include messages related to their bodies, their sexual history, sexually violent threats, and attacks on their mothering. There is often a high volume of messages (such as several hundred in a brief time period) despite existing intervention orders prohibiting contact (Harris & Woodlock, forthcoming a).

Perpetrators use technology in attempts to **humiliate and punish victim-survivors**. This tactic is not new. However, technology enables perpetrators to now do this with **more ease and greater reach and immediacy.** This is frequently attempted through social media and **image-based sexual abuse** (IBSA). In recent work on technology-facilitated DFV in non-urban Australia, almost half the women consulted reported IBSA, with one woman experiencing this in two different relationships (Harris & Woodlock, forthcoming a). IBSA was used during the relationship, to control victim-survivors through threats to distribute images, but most often was used by perpetrators to threaten and punish women when they separated.

Definitions and taxonomies - such as that outlined above - can be useful in aiding victim-survivors, advocates, and practitioners to identify, recognise and address technology-facilitated

DFV. However, it is by no means a comprehensive or complete list of acts that occur using the internet or online platforms. **Technologies, the features and functions of platforms, and perpetration strategies evolve**. Thus, it is important not to consider technology-facilitated DFV as a fixed category of behaviours and **we should be attentive to the dangers posed by digital media and the tactics in which perpetrators engage on an ongoing basis** (Harris & Woodlock, forthcoming b; Woodlock et al., 2020a and b).

Additionally, we note that t**echnology-facilitated DFV must be recognised in the context in which it occurs**. Identical behaviours may present in both non-abusive and abusive relationships. Platforms that enable geo-location, for example, may be viewed as useful or non-threatening and result in both parties feeling safer. However, for a DFV victim-survivor, technologies that enable tracking of movements can assist a perpetrator in surveillance and stalking activities and occur alongside other online and offline efforts to control, coerce and entrap a victim-survivor. However, the motive of the parties using the technology, the impact of the technology and the relational dynamics for each example is starkly different.

**DFV perpetrators use a range of techniques to abuse victim-survivors and individualised approaches.** Thus, while certain words may be regarded as offensive or flagged by platforms or AI regulation systems, there can be other words, phrases or images used to insult, demean or threaten or contact at certain times which hold meanings for a victim-survivor that are not problematised or picked up by tech industries or justice agents. Focusing only on flagged content results in these abuses being overlooked. While victim-survivors may report or seek assistance with an individual message, the message does not exist in isolation. It is menacing and upsetting both because of the individual incident *and* because it represents one of a series of acts of violence and entrapment to which they are subjected.

**Having incidents minimised or deemed not to breach a code/regulation relating to abuse can re-traumatise victim-survivors and exacerbate trauma**. Indeed, this mimics perpetrator's gaslighting and their attempts to minimise, deny, justify, and excusing abuse, which is a common feature of DFV (Bancroft, 2002). When external agencies (such as platforms and police) minimise the harms of technology-facilitated DFV then, they are both **replicating DFV**

**and seemingly legitimise and support abuse and perpetrators**. Negative responses when disclosing DFV can also **result in victim-survivors not help-seeking or reporting future harm**.

The above shows the **contextual, relational, and individual features of technology-facilitated abuse that can be overlooked in a single list of behaviours**. To understand the complete range of harms and the context in which it occurs, we believe that technology-facilitated DFV should be conceptualised as ***digital coercive control*** or *technology-facilitated coercive control.* **Here, we are foregrounding the channel used (digital / technology) the intent of the perpetrator (coercion) and impact and effect on a victim-survivor (control and entrapment).** A more inclusive lens ensures we capture both the acts that are more readily identified, problematised (and sometimes criminalised) as well as those which are frequently missed, dismissed, or seen as not 'serious' (Dragiewicz et al., 2018; Dragiewicz et al., 2019; Harris 2020a; Harris & Woodlock, 2019; Woodlock et al., 2020).

**Current or former intimate partners are frequently the target of DFV perpetrators but are not the only targets.** We stress that children too are commonly subjected to digital coercive control and should be recognised as victim-survivors. Many perpetrators use children as a core tactic to target their mothers (Bancroft et al., 2012; Harne, 2011; Jaffe et al., 2003). Increasingly, this involves technology (Dragiewicz et al., 2020; Dragiewicz et al., 2021). Victim-survivors report that **abusers use children in efforts to elicit a response from them and re-establish contact** and feel or are concerned that children are given devices by perpetrators to **facilitate monitoring and abuse**. Perpetrators may contact children via information communication technology, social media or gaming platforms in efforts to **destabilise the non-abusive parent's relationship with their children** (Harris & Woodlock, forthcoming a).

There are a range of behaviours perpetrators may subject children to, including (not limited to):

- Using digital communication platforms, gaming systems, technology gifted to children, or devices hidden in their property to **stalk and gain intelligence about victim-survivors**;
- **Hacking children's social media accounts**;

- **Monitoring children**; tracking children's use of technology, movements and recording children;
- **Impersonation** of another real or fictional child for the purposes of contacting children (and often gaining information about a victim-survivor) through social media accounts (sometimes referred to as 'catfishing');
- **Commissioning children** to contact victim-survivors using technology, to provide device or account access, or to engage in digital abuse;
- **Contacting children** when contact was prohibited, or impersonating a real or fake person on a social media platform to contact children;
- **Restricting children's access to technology** in efforts to restrict their access to a victim-survivor (see Dragiewicz et al., 2019; Dragiewicz et al., 2020; Harris & Woodlock, 2019; Harris & Woodlock, forthcoming).

Dragiewicz et al's 2020 study for The eSafety Commissioner[2] found that **social media was heavily engaged by perpetrators targeting children**. Professionals in the DFV sector reported that

- Facebook was present in 59% of cases
- Snapchat was present in 43% of cases
- Instagram was present in 33% of cases
- Twitter was present in 17% of cases
- **Gaming devices** were present in 26% of cases.

**Additionally, family members, friends and new partners can be targeted and victimised,** as has been highlighted by survivors consulted for Harris's ongoing DECRA research. This can occur during relationships and start or escalate during separation, as there is diversification of abusive tactics to include victim-survivor networks (DeKeseredy, Dragiewicz & Schwartz, 2017).

[2] The researchers conducted a survey and focus groups of professionals who work with DFV cases and interviews with: mothers who are victim-survivors of DFV, young people impacted by technology-facilitated domestic violence and fathers in men's behavioural change programs.

**Proxy perpetrators may also target victim-survivors, their children, friends and family and new partners.** Proxy perpetrators are other persons in a perpetrator's familial or social networks (real world or digital) may elect or be commissioned to engage in digital coercive control, contacting and harming against a perpetrator's intimate partner and their children and the friends and family of their current or former partner (see also Dragiewicz et al., 2020; Harris & Woodlock, forthcoming a). This could be, for instance, in sending abusive messages via social media or contributing to digital campaigns to shame or harass victim-survivors or challenge their account of DFV on social media. For victim-survivors in regional, rural, or remote communities (where perpetrators were often well-known) this can serve to further socially isolate them from their networks (Harris & Woodlock, forthcoming a).

Key to note is that while perpetrators (or proxy perpetrators) may use accounts featuring their name to enact digital coercive control, they will also use **fake names and accounts to contact their targets and can benefit from the anonymity of social media to harass and harm**.

**Digital coercive control can occur during relationships but often begins or escalates at separation** (Dragiewicz et al., 2019; Harris & Woodlock, forthcoming), as has been found in DFV research more broadly, which finds escalated risk at the time of separation (DeKeseredy, Dragiewicz & Schwartz, 2017).

Victim-survivors who share children with perpetrators have flagged that they **continue to be exposed to digital coercive control** because channels of communication remain open. Where digital abuse from perpetrators includes mention of the children, police and magistrates have reportedly been **reluctant to recognise this as DFV, instead suggesting it is a 'family law' matter** (George & Harris, 2014).

## (b) evidence of: (i) the potential impacts of online harms on the mental health and wellbeing of Australians;

DFV is one of Australia's most pressing social problems. It is under-reported and under-recorded, yet available data speaks to the extent of the issue. Approximately one quarter of Australian women experience at least one incidence of DFV from the age of 15 (ABS, 2017) and, on average, one woman is killed in the context of DFV each week of the year (Australian Domestic and Family Violence Review Network, 2018).

Technology **amplifies the harm of DFV and creates new forms and avenues of abuse** (Dimond, Fiesler & Bruckman, 2011; Fraser et al., 2010; Hand, Chung & Peters, 2009; Mason & Magnate, 2012; Southworth et al., 2005).

Rates of digital coercive control are hard to determine, but **research indicates that technology is commonly weaponised by perpetrators of DFV**, as has been documented in large-scale national surveys of practitioners in two studies (Woodlock, 2015; Woodlock et al., 2020).

Violence often continues or escalates post-separation and perpetrators **may commit multiple forms of systems abuse or an abuse of processes in efforts to reassert their power and control over a victim-survivor**. This could involve applications and complaints made through various legal channels, the courts, Child Support Agency, Centrelink that adversely impact a victim-survivor's wellbeing, resources and ability to undertake studies, employment or care for children (Douglas, 2018; Douglas & Chapple, 2019; Douglas & Walsh, 2009). **Reporting victim-survivors to platforms or telecommunications agencies or, reporting their use of technology** (such as social media posts) **to justice agencies can, we contend, be regarded as another form of systems abuse.**

**As victim-survivors have emphasised and available research documents, digital coercive control has extensive impacts on victim-survivors' mental, emotional and physical health and feelings of safety and freedom.**

*In our own words: the impacts of digital coercive control:*

> *…you can't keep up with it [digital coercive control] and you've done so much, when you're going through so much pain and trauma and you're trying to get your life back together, that's just something else to have to think about… trying to keep your children's emotions together as well, so you're like the backbone again* (Fiona, not her real name, DFV victim-survivor)

> *…I feel like I'm in prison. Because I can't – going out I'm thinking, on I'm not going to go there and I think I'm dead, I'm not going to go there. You know what I mean and you – I have to watch always at my back all the time. I feel really terrible* (Josie, not her real name, DFV victim-survivor)

> *He was going on Facebook… He kept saying [in Facebook messages] 'I know where you are'. They [support workers] said to look for flags [that my safety and security was threatened] and it was psyching me out* (Teresa, not her real name, DFV victim-survivor)

> [speaking about harassment on Facebook] *Scared. Really scared because you don't know what to expect. It just feels wrong. You just don't know what to expect. You think Facebook would have something there to be more safer, to make it more safer* (Lily, not her real name; DFV victim-survivor with cognitive or intellectual impairment).

> *I hadn't seen or spoken to my biological father in over 28 years, not since the abuse. We had managed to escape decades earlier, He managed to track down my Facebook profile (even though I had changed my name) through family members and contacted me directly. Reading his message made me re-live all the vile and violent things he did to me, my mum and my sister. My complex PTSD and related anxiety has never been so bad. I thought I was safe.* (Jaimee; child sexual abuse and DFV victim-survivor with a psychosocial and physical disabilities)

*Advocate statement:*

> *It's just this technology stuff that's occurring that people are saying 'just block them on Facebook'...but you can't really do that because they go and create a whole new account and start this basically bombardment of this persons that even when they do block them, their family and friends then send the messages from a different account. I find that… a huge barrier is the police willingness to actually do something about the technology stuff… She [my client] was put into hospital because it was affecting her mental health so badly and the police still wouldn't do anything* (frontline worker assisting women with disabilities who experience DFV)[3]

### *Exacerbating the impacts of DFV*

Technology is used to enact other forms of abuse and engage in stalking as well as to enact digital abuse. Digital coercive control **amplifies and exacerbates the impact of DFV during relationships and post-separation** (Dragiewicz et al., 2019; Fraser et al., 2010; Mason & Magnet, 2012). The majority of victim-survivors (74%) consulted by Woodlock in 2013 felt they had to be cautious of where they went and what they did because of the abuser's reach and harm enacted using technology. Fiolet et al (2021) found, in their research with advocates, that digital coercive control amplifies levels of fear.

**The possibility of 'escaping violence' and 'feeling safe' no longer has the same geographic boundaries it did before technology came to occupy such a significant role in our lives**. Victim-survivors can be subjected to digital coercive control anywhere and anytime they access digital media or a device; it is *spaceless*, and a new domain of violence perpetration not confined to a particular place but wherever the victim-survivor is. Digital coercive control moves beyond real-world sites and technologies enable immediate contact, constant overt or covert surveillance and monitoring. Thus, digital coercive control can seem to be inescapable – particularly given the many ways we use technology to navigate our lives – and perpetrators may seem omnipresent and omnipotent, especially where there is no end to or regulation of their

[3] These are all victim-survivor or advocate statements made to the authors, also reported in various reports by the authors.

behaviours. This can instil a pervasive and oppression condition of entrapment and **'unfreedom' for those who are attacked** (Hand, Chung & Peters, 2009; Harris, 2018; Harris & Woodlock, 2019; Harris & Woodlock, forthcoming a; Woodlock, 2013; see also Fiolet et al., 2021).

*Mental, emotional and physical health impacts*

Woodlock's 2013 SmartSafe study asked 46 victim-survivors about the effect of the abuse on their lives, with 84% indicating that technology-facilitated stalking and abuse had a **detrimental impact on their emotional and mental health** (such as nightmares, panic attacks, anxiety, and depression). Similarly, in George and Harris's 2014 study, victim-survivors in regional and rural Victoria reported anxiety and trauma-related symptoms because of digital coercive control. **We note that there are physical effects associated with the conditions that victim-survivors identified and with how trauma manifests**. Likewise, in Harris's current Australian Research Council DECRA research, friends and family of victim-survivors have highlighted impacts on their mental and emotional health and how this also has huge impacts on their physical health too.

It is important to **flag that the functions of platforms too can distress victim-survivors**. As a woman subjected to DFV explains:

> Things like Facebook have, 'this time last year' reminders and pictures of happy couples coming up and it's like, I don't want to remember this. Everytime I wrote a status update about when we were fighting but it was really cryptic. It's like, I don't remember what thighs was about, but it was a bad time, I don't like it. I don't want to see any of that (in Harris & Woodlock, forthcoming a).

**Platforms will generally assume that users want to remember posts and also that potential contacts are friendly or neutral, but this may not be the case for a DFV victim-survivor**. Prompts to connect with others due to mutual associations (such as through Facebook's 'people you may know', Instagram's 'suggested for you' and Twitters 'who to follow list' can serve to recommend people in a perpetrator's network (or even perpetrators themselves, see Bivens 2015. Harris 2020b).

There must be renewed effort to address and prevent digital coercive control, as well as the impacts associated with digital coercive control

> *[we need] better psychological and mental health supports for victim-survivors of this type of abuse – increasing mental health care plan sessions, training for mental health workers to specialise in advanced psychological torture and tech-facilitated abuse, complex PTSD and PTSD* (anonymous DFV victim-survivor).

*Sense of safety and security*

**Victim-survivor wellbeing, safety, and sense of security is undermined by the abuse, harassment and stalking to which they were and are subjected**. High volumes of and continuous exposure to abuse, harassment, harm and stalking via technology (including post-separation and after intervention orders had been obtained, police engaged, or assistance sought from telecommunications agencies or platforms) **takes a toll on victim-survivors**. **Fear** is reported by many and the spacelessness of digital coercive control can make it feel overwhelming and as though perpetrators are everywhere.

*Impacts on children*

Children who are exposed to or subjected to DFV can have a raft of "serious negative psychological, emotional, social and developmental impacts to their well-being" (Australian Domestic and Family Violence Clearinghouse, 2011: 1) and erosion of their sense of safety (UNICEF, 2006). In Dragiewicz et al's 2020 study for The eSafety Commission, DFV professionals identified a **range of negative impacts associated with digital coercive control**, estimating that:

- **Children's mental health was affected** in 67% of cases
- **Children were fearful** in 63% of cases
- **Children felt guilty if they disclosed information** in 59% of cases
- **Children's relationship with their non-abusive parent was negatively impacted** in 59% of cases
- **Children's routine activities were disrupted** in 49% of cases
- **Isolation from family and friends occurred** in 48% of the cases

The young people interviewed in the study described the impacts of digital coercive control:

- **Isolation** (particularly when access to technology was restricted in efforts to reduce incidents of abuse)
- **Fear**
- **Hypervigilance** in seeking to try and prevent and identify digital coercive control (both for themselves and their mothers, the non-abusive parent)
- **Disruption** to their daily lives (including their education and social lives)
- **Negative impacts on their relationship with both the non-abusive and the abusive parent**

*Lethal violence*

Digital coercive control can also precede and signify risk for lethal violence. Recognised 'homicide flags' (coercive control, obsessive behaviours, threats to kill or self-harm, attempts to isolate a victim-survivor and stalking) can be observed using technology and have been identified as emerging trends in DFV partner homicide and filicide cases (Death and Family Violence Review and Advisory Board 2017, see also 2021; Dwyer & Miller 2014). In their latest report the NSW Domestic Violence Death Review Team found **over two-thirds of the 47 cases reviewed where stalking was part of the abuser's behaviour involved technology**. This included "persistent text messaging, checking the victim's phone, covertly recording on the victim's activities, installing keylogger software on the victim's computer, and **engaging with the victim on social media / dating sites under a false identity**" (2017-2019: 155).

*Victim-survivors in regional, rural and remote communities*[4]

While digital coercive control is 'spaceless', **place matters and shapes experiences, impacts, and responses** to digital coercive control. Perpetrators' use of technology (and efforts to restrict women's uptake of technology) can **extend women's geographic and social isolation**.

The **omnipresence of digital coercive control** created a sense for victim-survivors that they **could never 'escape' the perpetrator**. Many women consulted in our work reported that the technological aspect of the abuse transcended boundaries and invaded their private spaces in ways that other abuse did not. Victim-survivors felt they could remove themselves physically from perpetrators, but technology enabled abusers to keep tormenting them, ultimately maintaining coercion and control. While **all victim-survivors face barriers when seeking help, these are exacerbated in regional, rural and remote places**. In smaller communities where many abusers are well-known and well-liked, women reported not being believed or helped when disclosing violence. This is especially true where women encountered the involvement of proxy perpetrators and peer support networks that fostered and facilitated the harm of DFV.

[4] This section draws on Harris & Woodlock's forthcoming report on women's experiences of digital coercive control in regional, rural and remote Australia and George & Harris's 2014 work on women's experiences of DFV in regional and rural Victoria.

## (ii) the extent to which algorithms used by social media platforms permit, increase or reduce online harms to Australians;

Machine learning algorithms, in theory, provide "an opportunity to effectively predict and detect negative forms of human behaviour" (Al-Garadi et al., 2019: 70701). However, developing a text classification approach and lexicon is challenging given DFV perpetrators use individualised strategies to target a particular victim-survivor. A lexicon may help in the identification of derogatory or profane words, but these may not be used by perpetrators and there are cultural and contextual differences in words used to threaten, demean, and harass. A more effective approach (trialled by some banking institutions) is to consider trying to develop systems that can identify coercive control and obsessive behaviours (including high-level contact), but the content, duration and volume of messages sent can differ and there will be digital coercive control that is missed. **It is imperative that social media platforms that are using algorithms are considering how to identify digital coercive control and the limits of algorithms to do so. Importantly, they must consult with victim-survivors, advocates, and practitioners in this process**. Importantly, algorithmic regulation cannot occur in isolation; **human regulators need to be trained about DFV and digital coercive control so that victim-survivors reporting abuse can receive assistance**.

## (c) the effectiveness, take-up and impact of industry measures, including safety features, controls, protections and settings, to keep Australians, particularly children, safe online;

## (d) the effectiveness and impact of industry measures to give parents the tools they need to make meaningful decisions to keep their children safe online;

Current approaches of social media platforms are limited because they do not generally recognise that an ***intimate threat model*** (Dragiewicz et al, 2019) needs to be deployed.

Domestic relationships involve the sharing of intimate knowledge, account and device ownership and access, and unique relational dynamics that enable insider threats to digital security in the hands of abusers (Doerfler, 2019; Dragiewicz et al., 2019; Levy & Schneier, 2020). Intimate threats to cybersecurity and privacy arise from the material conditions of intimate and domestic relationships and are often characterised by power differentials within the household or relationship (Levy & Schneier, 2018), exacerbating the potential outcomes of cybersecurity breaches. Sometimes - especially early in relationships - perpetrators frame control and oversight of technology as benign, generous or helpful. This might involve setting up a victim-survivor's technology, gifted technology or reviewing their use of technology and provides perpetrators with opportunities to control and monitor their digital footprints (Dragiewicz et al., 2019; Harris & Woodlock, forthcoming).

*Intimate threat model for cybersecurity*

Includes risk created by:

- intentional sharing of accounts and devices;
- intimate knowledge that can facilitate guessing of passwords or answering security questions;
- physical access to passwords, networks, and devices (Dragiewicz et al., 2019).

This means that some account protections – such as third-party authentication – will have limited or no effectiveness for DFV victim-survivors. **Functions like third-party authentication that are designed to protect against cybersecurity threats from strangers can be used by abusers to increase coercive control in the context of domestic violence**. For example, by taking or destroying mobile phones, **abusers can prevent victim-survivors' access to critical accounts they need for work, education, financial services, and government services** like Centrelink, the National Disability Insurance Scheme, immigration accounts, the Australian Taxation Office, and Medicare. Accordingly, it is essential that Safety by Design (discussed further in this submission) consider the intimate threats posed by domestic violence perpetrators as those from as well as strangers and acquaintances.

Platforms do not account for how accounts could be compromised, which can mean victim-survivors lose access to their account, as this statement from an anonymous victim-survivor shows:

> *if you change your phone number due to escaping violence you can't get back into your Facebook account if you had two-step verification setup and your old number was disconnected due to violence reasons* (anonymous DFV victim-survivor).

*The burden of safety work*

> *There is no 'contact us' or family violence support in social media* (anonymous DFV victim-survivor).

Digital coercive control can complicate experiences of DFV how victim-survivors respond to DFV. As outlined above, this has huge impacts on their wellbeing, sense of security and safety. Victim-survivors **invest extensive time, effort, and money to reduce or prevent violence and safely use technology** in the absence of effective responses to DFV more broadly and digital coercive control, specifically (Dragiewicz et al., 2019; Harris & Woodlock, 2019; Harris & Woodlock, forthcoming a). Victim-survivors undertake 'safety work' (Kelly, 2012) in efforts to plan, strategise and seek to prevent men's violence, which requires constant labour, energy, and

vigilance. Despite decades of awareness-raising, women are still expected to assume the responsibility for managing DFV. Perpetrators may escalate the abuse in response to women's attempts to manage their technology security or restrict access to devices or accounts (Dragiewicz et al., 2019; Harris & Woodlock, 2019; Harris & Woodlock, forthcoming a). The work of leading Australian agencies **WESNET and the eSafety Commission are key** here, providing guides, resources and training for women subjected to digital coercive control and the advocates supporting them. Victim-survivors maintain that DFV **sector expertise and resourcing in this area is vital and needs to be extended, that there needs to be connection to other agencies, and that assistance should be accessible including for those with disabilities** (see also Harris & Woodlock, 2021). As an anonymous contributor to this submission stated:

> *there need to be workers in all specialist family violence services who can help you to work through online abuse and hacking (in partnership with IDCARE) and have technical knowledge and an IT staff member employed to help keep your devices safe. Currently family violence services won't help with this; ID care will email you heaps of complicated information that is not disability accessible.*

Victim-survivors experiencing digital coercive control respond in varied ways. They may **decide to disengage from technology,** in efforts to avoid harm and protect themselves. However, given the role technology plays in our lives – in education, employment, civic and social engagement, and leisure – this can have profound effects on their lives (Harris, 2020) and human rights to digital inclusion (Dragiewicz et al, 2018; Suzor et al., 2019).

Friends, family members and criminal justice agents **frequently encourage or instruct victim-survivors to change their online behaviours or stop using technologies 'for their own safety'**(Dragiewicz et al, 2019; Harris & Woodlock, 2019). This is problematic given:

- the role technologies play in our lives;
- the onus placed on victim-survivors (as opposed to perpetrators);
- it inhibits women from sharing in and enjoying the same freedoms and liberties as men and exacerbates gendered driver of violence against women[5];

[5] It is a form of gendered inequality, preventing women's full independence, participation in public and private lives. This expectation on women to change their behaviours or stop using technology

- the typically incorrect assumption that cutting off access will deter perpetrators from engaging in future abuse on and offline.

Unfortunately, **disengaging from technology will not necessarily end violence**. If perpetrators are engaging in sustained campaigns and efforts to coerce and control victim-survivors or demonstrating obsessive tendencies (such as through high volume contact such as social media messages or monitoring of victim-survivors on or offline) they are unlikely to desist from their abusive behaviour. Instead, when one channel (technology) is cut they may seek new channels such as in person stalking and other forms of DFV (Dragiewicz et al., 2019; Fraser et al., 2010; Harris, 2020; Harris & Woodlock, forthcoming b). Moreover, **other family members, friends and new partners are sometimes targeted when perpetrators cannot reach the women** who are their targets (Dragiewicz et al., 2019; Harris & Woodlock, forthcoming a). This reinforces our earlier work (George & Harris, 2014), which found that perpetrators sometimes engaged in physical assault or in person stalking where technological access to women was shut down. Thus, **exposure to violence and risk may not be alleviated but could instead escalate if digital access is severed. The risks include fatal violence.**

**We have heard of victim-survivor devices being taken on the grounds that they are used for evidence collection of 'for the safety' of the victim-survivor**.

- Djirra (then the Aboriginal Family Violence Prevention and Legal Service) had previously received anecdotal reports of Indigenous women's **phones being seized by police officers to use evidence of digital coercive control in DFV matters**, thereby removing their means to call for assistance and access advocacy (see George & Harris, 2014).

- **Victim-survivors with cognitive or intellectual impairments, victim-survivors who are mentally unwell and elderly victim-survivors often have others** (family,

exacerbates the gendered driver of violence against women and thus actually perpetuates the likelihood of DFV continuing more broadly across society than reducing it at all.

> police, aged care) **remove their mobile phone, computer, tablet, or internet access** (see also Harris & Woodlock, 2021). This is, as victim-survivors contributing to this submission have lamented "extremely unsafe if the victim is experiencing family violence and this policy needs to be reformed so victims are not having their mobile phones taken off them".

Our work has demonstrated that some victim-survivors "strategically used ICT [information and communication technologies] as part of the safety work they did to protect themselves and their families" (Dragiewicz et al., 2019: 20; see also Harris & Woodlock, forthcoming a). Some **women in our studies kept some technological channels open or endured digital coercive control** such as ongoing electronic monitoring and communication **in efforts to monitor and mitigate dynamic risks, reduce, or prevent violence**, as the accounts below show:

> *So I have always kept the same Apple phone that I had, and I know that - i just accept that it's a device that he watches and he stalks, because my concern is that if I go offline that he will just turn up in person. So I still text from that… I have to have a number that he knows about because otherwise he will go looking for me elsewhere* (Sarah, not real name, DFV victim-survivor).

> *I'm scared to cut off communication because he'll get very angry… he was angry [when] I stopped communication. That is why he is going to kill me* (Priya, not her real name, DFV victim-survivor).

In Dragiewicz et al's 2020 research for The eSafety Commissioner, **young people also reported using protective strategies to deal with digital coercive control**, by changing account settings, not responding to perpetrator's messages or contact, blocking accounts and numbers, collecting evidence, and withholding information from perpetrators. Non-abusive parents spoke about their efforts to restrict their children's exposure to digital coercive control, such as by blocking the abusive parent from their children's social media, changing their children's phone number or account information, and stopping their children from using some technology.

Victim-survivors and their children have spoken about **investing time and money to replace devices, engage telecommunications agencies and platforms in efforts to stop abuse** (Dragiewicz et al., 2019; Dragiewicz et al., 2020; Harris & Woodlock, forthcoming a). Women victim-survivors bear the burden and costs of men's violence against them, which prevents the full use and enjoyment of their money and income because it is spent to 'protect' themselves. This may contribute to uneven gender distributions of assets and access to resources, which again promote gender inequality, coming full circle to perpetuating the conditions necessary for violence against women to be perpetrated.

On children and protections, we note that **victim-survivors consulted for this submission have called for more protections for disabled children who are victim-survivors of DFV and technology-facilitated abuse**, suggesting this should be explored by the Children's Commissioner and regulatory bodies.

*The roles and responsibilities of platforms and Safety by Design*

> *Family violence and corporate social responsibility. The developers of tech who benefit billions of their tech; they need to take responsibility to make their devices safe for victims in a [disability] accessible and easy English way* (anonymous DFV victim-survivor)

While advocating for the primary prevention of DFV (and recognising how values, inequalities and power differentials can foster and facilitate DFV), we contend that the **burden of designing, developing, and regulation to address and prevent digital coercive control should be on platforms and the tech industry, not victim-survivors.** To that end, we call for the adoption of The eSafety Commissioner's Safety by Design initiative, which has three tenets (see also https://www.esafety.gov.au/industry/safety-by-design; Harris, 2021; PenzeyMoog, 2021):

1. **Service providers are responsible for ensuring user safety is their number one priority**. Platforms and tech companies should pre-empt how their products might facilitate, increase or encourage harm. Thus, the burden of safety and 'safety work' should not fall solely on the user.

2. **Users should have the power and autonomy to make decisions in their best interest**. Platforms and services can and should engage in meaningful consultation with users (such as victim-survivors, and ensuring they are engaging with diverse groups in doing so) to ensure their features and functions are accessible and helpful to all.

3. **Platform transparency and accountability about operations and published safety objectives is vital**. There should be, for instance, open reporting about responses to safety issues and sharing of strategies between platforms about effective safety strategies (as is currently occurring in the Australian banking sector in regard to digital coercive control and DFV more broadly).

*The eSafety Commissioner has published resources to assist platforms and tech companies to assess their approach* and "'embed safety into the culture, ethos and operations of their business - from the ground up" (n.d, n.p. See: https://www.esafety.gov.au/industry/safety-by-design/assessment-tools)

**Technology design, development and regulation does not occur in a vacuum**. Effective approaches need to acknowledge how intersecting or overlapping forms of structural or systemic oppression shape an individual's experience of technology and can extend social inequalities. **Greater diversity in the tech field and, including and centring victim-survivors, advocates and practitioners in the design, development, and regulation process would be transformative**. We recognise that some platforms are doing this to some degree (for example Facebook has consulted with the National Network to End Domestic Violence in the US and IBM has published a guide to 'coercive control resistant design' ) but suggest it needs to happen on a broader level and as a matter of course (not an afterthought) and not only with DFV advocates

but victim-survivor collectives too. Additionally, we believe **it is not enough for platforms to engage with Safety by Design in theory; we must continually assess and reflect on *how* they do this, and they must seek to continually enhance their policies and practices**.

Recognition of DFV is important. Platforms may be **designing and developing features that pose cause risks to victim-survivors**. Additionally, **platforms and apps will often change the function and options of social media without considering impacts on victim-survivors**. It is imperative that any changes are **opt-in as opposed to automatically applied / default.**

*Experiences with telco and platform regulation*

Perpetrators will take advantage of the functions and features of platforms to enact digital coercive control. Victim-survivors have emphasised that, **generally, telecommunications bodies and platforms do not understand digital coercive control and how it manifests**. Thus, there is a **reluctance or failure to address and prevent issues** reported or, **no clear mechanism** through which to report digital coercive control, and this is particularly true where there are not human regulators reviewing complaints. **Too often victim-survivors are not advised of an outcome of a complaint and there is no way to appeal platform decisions** (Dragiewicz et al., 2019; Harris & Woodlock, 2021; Harris & Woodlock, forthcoming a)**.**

Victim-survivors and advocates have emphasised that **privacy and security protections on social media accounts are not accessible or simplified enough**, including for those with disabilities. The account below, from an anonymous victim-survivor emphasise issues with navigating platforms:

> *If you get locked out of your Facebook account due to disability reasons, Facebook doesn't help you get back on it.*

Work completed by Harris and Woodlock (2021) for The eSafety Commissioner has found that women with cognitive or intellectual disabilities experience high levels of unwanted contact and harassment via social media platforms. **Women are often unsure who to contact to assist them**

**and have emphasised that platforms such as Facebook could and should do more to ensure their platforms and platform users are safe to interact with and this includes addressing harassment, abuse, identity theft and catfishing**. They have also suggested that **platforms offer easy to understand and navigate reporting mechanisms that are communicated using images and videos, as well as text**. Women called for **quick resolution** to reports they lodged or requests for assistance. As Lily (not her real name) says: "

> *people who have disabilities are more vulnerable to the system than anyone else and they should be acknowledged like if they're having a problem, they should be getting help straight away*.

This need to be **extended to disabled victim-survivors in prisons and institutions** who have extremely limited access to assistance to respond to DFV, digital coercive control and online abuse.

**Advocates have likewise described their experiences of engaging platforms or telecommunications companies as "unhelpful"**, "like banging your head against a wall… pointless". Subsequently, they "don't bother [reaching out for assistance now" (Dragiewicz et al., 2019: 36). They have **also called for telecommunications providers and platforms to take DFV into consideration** and to **improve the safety and regulation of their services and apps**.

## (e) the transparency and accountability required of social media platforms and online technology companies regarding online harms experienced by their Australians users;

## (f) the collection and use of relevant data by industry in a safe, private and secure manner;

**Platform governance** – the ways that platforms shape and regulate information and social environments and how they regulate themselves – **requires more attention** (Dragiewicz et al., 2018; Gillespie, 2017; Suzor, 2019; Suzor et al., 2019). **Social media organisations have a responsibility to prevent and address digital coercive control and to be open and accountable to users about their regulatory processes**. This is a fundamental component of the 'Safety by Design' initiative promoted by The eSafety Commissioner (see online resources: https://www.esafety.gov.au/industry/safety-by-design).

We (Dragiewicz et al., 2019: 6) have made the following recommendations for platforms and telecommunication agencies:

> *Regulation to require, monitor, and enforce:*
>
> - **Safety by design** via mechanisms to make it more difficult for GPS tracking devices, recording devices, and apps to be used without the targets' knowledge or permission
> - **Providing high-visibility platform privacy options with plain-language notification to users of changes and regular reminders** requiring active user approval
> - **Actively informing platform users of the data collected** about their movement and activities and potential **safety and privacy risks**
> - Requiring telcos to provide **hardship plans for domestic violence survivors**, high-visibility advertising about their availability, and publicly report uptake of these services

- **Creation of dedicated, in-person contact phone numbers for telco and platform staff to respond to domestic violence related complaints**
- Ensuring platforms **inform survivors of actions taken in response to complaints and establishing an appeal process.**

Ultimately, *the operations and response of platforms and telecommunications agencies to digital coercive control needs to be improved, urgently*.

## (g) actions being pursued by the Government to keep Australians safe online; and

*The justice system and digital coercive control*

The justice system is said to be a cornerstone in addressing and combatting DFV, with police, courts and corrections contributing to violence prevention and "playing a pivotal role in increasing victim safety and ensuring perpetrator accountability" (Coroners Court of Victoria, 2012: 45). **However, justice responses to digital coercive control are limited and failing victim-survivors**. When seeking to identity, prevent and respond to digital coercive control, police and magistrates may:

- Express difficulty in defining digital coercive control and the harm involved;
- Regard digital coercive control as distinct from other forms of abuse and traditional stalking;
- Discount or dismiss reports of digital coercive control and breaches of orders by technology;
- Provide conflicting / confusing advice as to what digital evidence is legally admissible, required to secure an intervention order and recognised as constituting a breach of an intervention order;
- Do not consistently recognise and record threats to kill issued by technology;
- Commonly pressure victim/survivors to disengage from technology (which can escalate risk);
- Struggle with resourcing responses to technology-facilitate harms, particularly in regional, rural and remote areas (George & Harris 2014; Harris, 2016, 2018).

**Advocates have suggested that police are reluctant to intervene when digital coercive control involves platforms**, as this frontline worker expressed:

> *When we talk about the technology stuff the police have a brilliant out which 99% of the time is…. If it's on Facebook, if the abuse or the control is on Facebook or Instagram or whatever, they can't do anything because it's Facebook. They can't do*

> *anything because they don't control Google. It's just… the things that people do electronically to other people and put it out there… they say 'oh well, even if it was harassment or intimidation… they can't prove that it was that particular person because it's a Facebook page and they can't control what happens on Facebook* (in Harris & Woodlock, 2021: 30).

It is **imperative that justice agencies (police, courts, corrections) are trained in relation to DFV more generally and digital coercive control, specifically.**

Victim-survivors have also called for **more resourcing to target specific elements of digital coercive control**, for instance, proxy perpetration of DFV

> *Where perpetrators send other men after the victim; there needs to be better investment in resources to police these. Especially where there is stalking, digital-facilitated abuse, hackings, trying to find locational information and attempted abductions and stalking, there needs to be police resources given to this as it is highly under-resourced and impossible to get police to investigate* (anonymous DFV victim-survivor).

*Police perpetrators*

We note, now, **the complexities faced and vulnerabilities of victim-survivors with a police perpetrator and that victim-survivors and advocates are leading calls for reform and research on this issue** (see, for instance, work by Victorian Policing Family Violence Project, now based at Flat Out). Internationally, research has indicated that **rates of officer-involved domestic violence (OIDV) are between two and four times higher than general population rates**, with perpetrators estimated at between 28% (Fukuroda, 2015), 30% (International Association of Chiefs of Police, 2003; Wetendorf, 2006) 37-41% (Neidig, Russell & Seng, 1992) or 40% (Johnson, 1991 for the US House of Representatives) of police cohorts (see also Goodmark,

2015; Larsen & Guggisberg, 2009; Lonsway, 2006; Mennicke & Ropes, 2016). In Ryan's (2000) survey of 210 law enforcement officers, 54% said they knew officers involved with DFV, 16% new of unreported OIDV, 31% knew members of their department were disciplined for OIDV (see also Russell & Pappas, 2018).

Given narrow definitions of DFV in various studies, underreporting in perpetrator surveys (see also Hester, 2012) and barriers faced by victim-survivors (including increased isolation, and avoiding service systems, as reported by the Policing Family Violence Project, 2020), **it is likely rates of OIDV are significantly higher than has been reported** (see also Goodmark, 2015). Freedom of Information requests by Australian journalists (see Gleeson 2020a, b) reveal that, between 2015 and 2020, at least 89 Victoria Police officers were charged with DFV related offences. Systemic failings in Victoria Police responses to OIDV were uncovered by the Independent Broad-based Anti-Corruption Commission (IBAC) in 2020.

OIDV perpetrators are "skilled abusers. **The very skills that police need in their work make abusive police officers particularly dangerous to their partners**" (Goodmark, 2015: 114). They have **high-level knowledge of legal and justice systems; access to intel (via databases and records); firearms and other weapons; strong support networks in the police which can be loyal to the perpetrator** (see Goodmark, 2015; Gorrie, 2021; McCulloch, 2001). This **elevates risk to victim-survivors and increases power differentials between victim-survivors and perpetrators**, as has been documented by the Policing Family Violence Project and in recent work by Harris & Woodlock (forthcoming, a & b) and Harris's DECRA research. Australian analyses of OIDV reveals that there are significant differences in arrest, charge, and caution rates of officers (20%) as compared to other alleged perpetrators (80%, see McKenzie & Tozer, 2020). Goodmark (2015: 118) contends that, in addition to the camaraderie, the 'blue wall of silence', support and loyalty from other officers, OIDV perpetrators may disparage the victim-survivor to their colleagues "making them less likely to take her claims seriously". This can result in a **lack of response in accordance with policy and procedure**. In addition to this cultural reluctance, it has been contended that **prioritising of member wellbeing (in relation to mental health and suicide risk) in internal systems – and approaches to addressing workplace harms**

**– has hampered the ability of police organisations to hold officers accountable for DFV perpetration**. This serves to further endanger victim-survivors of OIDV.

> *He intimidates, stalks, monitors, surveils me [including on social media and online]. They [other officers] did everything to help him avoid accountability and consequences* (Mandy, not her real name, victim-survivor of OIDV)

In Harris and Woodlock's work on digital coercive control in regional, rural and remote Australia (forthcoming a) and Harris' DECRA research, victim-survivors of OIDV have reported that:

- **Police did not follow institutional DFV policies or procedures** when responding to their case;
- **Police informed victim-survivors that they had investigated DFV and technology-related offences when they had not**, as noted by other officers, later;
- **Police informed victim-survivors that they could not investigate DFV matters or that there were not breaches of orders** when subsequently, other officers and/or DFV services challenged this;
- **Police informed victim-survivors that action** (investigations, pursuit of orders, breaches) **was not taken at certain times, so as not to alert the perpetrator that he was under investigation** (yet this was also challenged by other officers at later date);
- The justice system has been engaged but **the perpetrator continues to engage in social media and online stalking and monitoring;**
- **Perpetrators appear to have obtained their social media and online account information** (which should not have been possible).

The need for independent oversight into complaints against policing of DFV has been called for by victim-survivors and advocates (see, for instance, Flat Out, 2015; Flemington & Kensington Community Legal Centre, 2015) and **the need for independent investigation and complaint procedures called for, in cases of OIDV.** As the statement below shows, victim-survivors have also called for reform and resources to investigate OIDV, police corruption and collusion with perpetrators:

> *Corruption in the police force for tech-facilitated abuse needs to be reformed and IBAC better resourced, and the Police Commissioner better sourced to deal with the amount of police corruption. Law reform needs to make it easier for people to prosecute the police, especially where they are a perpetrator of family violence or have assisted in colluding with family violence [perpetrators]* (anonymous DFV victim-survivor).

**Victim-survivors have also called for greater onus on the perpetrator's behaviour and checking of the perpetrator's technology**.

## (h) any other related matter.

**Technology can provide key channels to seek assistance, support and connection with others and overcome the social isolation** that perpetrators attempt to impose**. The Independent Collective of Survivors (ICOS)** is an example of where victim-survivors have connected with each other from across Australia through Facebook, Twitter and LinkedIn. These platforms have allowed victim-survivors to collaborate on victim-led advocacy initiatives and provide each other with peer-support. For victim-survivors in regional, rural or remote Australia or, whose social and/or familial networks are primarily based overseas, **technology can also help overcome geographic isolation**. Women with **cognitive or intellectual impairments and/or physical disabilities have also emphasised that technology provides is central in maintain their contact with others and sense of community**. Given the important role technology has in these settings, as well as enabling civic engagement and the pursuit of employment and education opportunities, it is imperative that victim-survivor rights to use technology are protected (Harris et al., 2020; Harris & Woodlock, 2021; Harris & Woodlock, forthcoming a).

Advising or instructing victim-survivors to stop using a platform or block people inhibits victim-survivors' use of public and semi-public spaces. This **extends gender inequality, with men continuing to dominate these spaces; replicating patriarchal structures while further marginalising and excluding of women's voices**.

**Anonymity is important for victim-survivors to participate publicly and privately on social media**. Victim-survivors provide key commentary and critique of responses to DFV and can use platforms to talk about their experiences in ways that would be possible if identify verification was required. Victim-survivors have **called for platforms to assist them in regaining control of accounts and with anonymity**:

> *Facebook also can't change the name you started your Facebook account in to your new name (removes older names from your profile). If you want to try to make sure perpetrators can't find you Facebook makes that very difficult* (anonymous DFV victim-survivor).

If identity documentation had to be provided to platforms there would be **sensitive identity information provided to platforms. This could potentially be accessed by perpetrators** at platforms or with contacts at platforms or perpetrators with power to compel information from platforms (such as police, noting our earlier section on police perpetrators). There have been data breaches at major platforms and technology companies which does not instil confidence in data management.

While pseudonymity can be exploited by DFV perpetrators, we agree with van der Nagel's submission to this inquiry, that **pseudonymity can be "a safety feature of social media platforms"** for some groups including "victim-survivors of domestic abuse avoiding their abuser" and "victim-survivors revealing abuse, especially from powerful people" (2020: 3). **Identity verification would likely result in a silencing of victim-survivors** because they would be pursued by their perpetrator (or proxy perpetrators) including through 'systems abuse' (see earlier discussion) including: reporting them to platforms or justice agents or engaging in litigation by challenging a victim-survivor's account of abuse (and making allegations of defamation, for example).

## References

Al-Garadi, M. A., Hussain, M. R., Khan, N., Murtaza, G., Nweke, H. F., Ali, I. Mutjaba, G., Chiroma, H., Ali Khattak, A. & Gani, A. (2019). Predicting cyberbullying on social media in the big data era using machine learning algorithms: review of literature and open challenges. *IEEE Access*, *7*, 70701-70718.

Australian Domestic and Family Violence Clearinghouse (2011). *The impact of domestic violence on children: A literature review.* Sydney: Australian Domestic and Family Violence Clearinghouse.

Australian Domestic and Family Violence Death Review Network. (2018). *Australian Domestic and Family Violence Death Review Network 2018 data report*. Australia: Domestic Violence Review Team.

Australian Bureau of Crime Statistics (ABS). (2017). *Personal safety survey.* Canberra: ABS.

Bancroft, R. L., Silverman, J. G., & Ritchie, D. (2012). *The batterer as parent: Addressing the impact of domestic violence on family dynamics* (2nd ed). California: SAGE Publications

Barter, C., Stanley, N., Wood, M., Lanau, A., Aghtaie, N., Larkins, C., & Øverlien, C. (2017). Young people's online and face-to-face experiences of interpersonal violence and abuse and their subjective impact across five European countries. *Psychology of Violence*, *7*(3): 375-384.

Bivens, R. (2015) Under the hood: the software in your feminist approach. *Feminist Media Studies*, *15*(4): 714–717.

Coroners Court of Victoria. (2012). *Victorian systematic review of family violence deaths: First report.* Victoria: Coroners Court of Victoria.

Death and Family Violence Review and Advisory Board. (2017). *Domestic and Family Violence Death Review and Advisory Board: 2015-2017 annual report*. Brisbane: Death and Family Violence Review and Advisory Board.

DeKeseredy, W. S., Dragiewicz, M., & Schwartz, M. D. (2017). *Abusive endings*. California: University of California Press.

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with computers*, *23*(5): 413-421.

Dodge, A. & Johnstone, E. (n.d.) *Using fake video technology to perpetrate intimate partner abuse*. California: Domestic Violence Deepfake Advisory.

Doerfler, P. (2019, January, 30). *Something you have and someone you know—Designing for interpersonal security*. Enigma 2019, San Francisco, USA. https://www.usenix.org/conference/enigma2019/program

Douglas, H. (2018). Legal systems abuse and coercive control. *Criminology & criminal justice*, *18*(1): 84-99.

Douglas, H., & Chapple, K. (2019). *National domestic and family violence bench book*. Australia: Australian Institute of Judicial Administration.

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*, *59*(3): 551-570.

Douglas, H., & Walsh, T. (2009). Mothers and the child protection system. *International Journal of Law, Policy and the Family*, *23*(2): 211-229.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4): 609-625.

Dragiewicz, M., O'Leary, P., Ackerman, J., Bond, C., Foo, E., Young, A., & Reid, C. (2020). *Children and technology-facilitated abuse in situations of domestic and family violence*. Australia: eSafety and Griffith Criminology Institute.

Dragiewicz, M., Woodlock, D., Salter, M., & Harris, B. (2021). "What's Mum's Password?": Australian mothers' perceptions of children's involvement in technology-facilitated coercive control. *Journal of Family Violence*, online first, 1-13.

Dragiewicz, M., Harris, B., Woodlock, D., Salter, M., Easton, H., Lynch, A., Campbell, H., Leach, J. Milne, L. (2019). *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.* Australia: The Australian Communications Consumer Action Network (ACCAN), Australia.

Dwyer, J., and Miller, R. (2014). *Working with families where and adult is violent: Best interest case practice model specialist practice resource*. Victoria: Department of Health and Human Services.

The eSafety Commissioner. (n.d.). *Safety by Design assessment tools.* https://www.esafety.gov.au/industry/safety-by-design/assessment-tools

Fiolet, R., Brown, C., Wellington, M., Bentley, K., & Hegarty, K. (2021). Exploring the impact of technology-facilitated abuse and its relationship with domestic violence: A qualitative study on experts' perceptions. *Global qualitative nursing research*, *8*, 23333936211028176.

Flat Out. (2015). *Submission to the Royal Commission into Family Violence.* Victoria: Flat Out.

Flemington & Kensington Community Legal Centre. (2015). *Submission by Police Accountability Project of Flemington & Kensington Community Legal Centre to the Royal Commission into Family Violence (Victoria).* Victoria: Flemington & Kensington Community Legal Centre.

Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The new age of stalking: Technological implications for stalking. *Juvenile and family court journal*, *61*(4): 39-55.

Fukuroda, M. L. (2005). *Murder at Home: An Examination of Legal and Community Responses to Intimate Femicide in California. Volume One*. California: California Women's Law Center.

George, A., & Harris, B. (2014*). Landscapes of violence: Women surviving family violence in regional and rural Victoria.* Geelong: Deakin University.

Gillespie, T. (2017). Governance of and by platforms. In J. Burgess, T. Poell & A. Marwick (Eds.), *SAGE handbook of social media* (254-278). London: Routledge.

Gleeson, H. (2020a) Abusers in the ranks. *ABC News* (19th October) https://www.abc.net.au/news/2020-10-25/kate-was-charged-with-assaulting-her-police-officer-partner/12758060?nw=0

Gleeson, H. (2020b) No one will believe you *ABC News* (25 October) https://www.abc.net.au/news/2020-10-19/police-in-australia-are-failing-to-take-action-against-domestic/12757914?nw=0&r=HtmlFragment

Goodmark, L.S. (2015). Hands up at home: Militarized masculinity and police officers who commit intimate partner abuse. *Faculty Scholarship.* 1515: 101-163.

Gorrie, V. (2021). *Black and blue: A memoir of racism and resilience.* Melbourne: Scribe.

Hand, T., Chung, D., & Peters, M. (2009). *The use of information and communication technologies to coerce and control in domestic violence and following separation*. Sydney: Australian Domestic and Family Violence Clearinghouse, UNSW.

Harne, L. (2011). *Violent fathering and the risks to children: The need for change*. Bristol: Bristol University Press.

Harris, B. (2018). Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice administration. In K. Fitz-Gibbon, S. Walklate, J. McCulloch, J.M. Maher (Eds.), *Intimate partner violence, risk and security* (52-70). London: Routledge.

Harris, B. (2020a). Technology, domestic and family violence: Perpetration, experiences and responses. *Centre for Justice Briefing Paper*, *4*: 1-4.

Harris, B. (2020) Technology and violence against women. In S. Walklate, K. Fitz- Gibbon, J. McCulloch and J.M. Maher (Eds.), *The Emerald handbook of feminism, criminology and social change* (317-336) Bingley: Emerald.

Harris, B. (2021). Technology-enabled abuse: How 'Safety by Design' can reduce stalking and domestic violence. *The Conversation.*

Harris, B., Dragiewicz, M. & Woodlock, D. (2021) *Harris, Dragiewicz & Woodlock Submission on Online Safety Legislative Reform (Australian Government Department of Infrastructure, Transport, Regional Development and Communications Consultation on a Bill for a new Online Safety Act).* Australia: The Authors.

Harris, B., Dragiewicz, M., & Woodlock, D. (2021). Technology, domestic violence advocacy and the sustainable development goals. In J. Blaustein, K. Fitz-Gibbon, N. Pino & R. White (Eds.), *The Emerald handbook of crime, justice and sustainable development*. (295-313) Bingley: Emerald.

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, *59*(3): 530-550.

Harris, B. & Woodlock, D. (2021). '*For my safety': experiences of technology-facilitated abuse among women with intellectual disability or cognitive disability*. Australia: The eSafety Commissioner.

Harris, B. & Woodlock, D. (forthcoming a). *Spaceless violence: Technology-facilitated abuse, stalking and advocacy*. Final report. Canberra: Australian Institute of Criminology

Harris, B. & Woodlock, D. (forthcoming b). 'You can't actually escape it: Policing the use of technology in domestic violence in rural Australia. *International Journal for Crime, Justice and Social Democracy*.

Harris, B., Woodlock, D. & Dragiewicz, M. (2020) *Harris, Woodlock & Dragiewicz Submission to the Australian Parliament Standing Committee on Social Policy and Legal Affairs inquiry into and report on family, domestic and sexual violence.* Australia: The Authors.

Hester, M. (2012). Portrayal of women as intimate partner domestic violence perpetrators. *Violence against women*, *18*(9), 1067-1082.

International Association of Chiefs of Police. (2003). *Domestic Violence by Police Officers*. USA: National Law Enforcement Policy Centre.

Jaffe, P. G., Lemon, N. K., & Poisson, S. E. (2003). *Child custody and domestic violence: A call for safety and accountability*. California: Sage.

Johnson, L. (1991). *On the front lines: Police stress and family well-being.* Washington, DC: US Government Printing Office.

Kelly, L. (2012). Standing the test of time? Reflections on the concept of the continuum of sexual violence. In J. Brown & S. Walklate (Eds.), *Handbook on sexual violence* (pp. xvii–xxvi). London: Routledge.

Larsen, A., & Guggisberg, M. (2009). Police officers, women and intimate partner violence: Giving primacy to social context. *Australian Journal of Gender and Law*, *1*: 1-18.

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1), tyaa006. https://doi.org/10.1093/cybsec/tyaa006

Lonsway, K. A. (2006). Policies on police officer domestic violence: Prevalence and specific provisions within large police agencies. *Police Quarterly*, *9*(4): 397-422.

Marganski, A., & Melander, L. (2018). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of interpersonal violence*, *33*(7): 1071-1095.

Mason, C. and Magnate, S. (2012). Surveillance studies and violence against women. *Surveillance & Society*, *10*: 105–118.

McCulloch, J. (2001). *Blue army: Paramilitary policing in Australia*. Melbourne: Melbourne University.

McKenzie, N. & Tozer, J. (2020). 'Hidden crisis': When your domestic abuser is also the local police officer *Sydney Morning Herald.* (December 6th) https://www.smh.com.au/national/hidden-crisis-when-your-domestic-abuser-is-also-the-local-police-officer-20201203-p56k6r.html

McLachlan, F. & Harris, B. (forthcoming). Intimate risks: Examining online and offline abuse, homicide flags and femicide. *Victims & Offenders.*

Mennicke, A. M., & Ropes, K. (2016). Estimating the rate of domestic violence perpetrated by law enforcement officers: A review of methods and estimates. *Aggression and violent behavior*, *31*: 157-164.

Neidig, P. H., Russell, H. E., & Seng, A. F. (1992). Interspousal aggression in law enforcement families: A preliminary investigation. *Police Studies*, *15*, 1: 30-38.

NSW Domestic Violence Death Review Team. (2017). *NSW Domestic Violence Death Review Team Report 2015-2017*. NSW: Domestic Violence Death Review Team

Nuttall, L., Evans, J., Franklin, M., Burne James, D. for IBM (2019). *Coercive control resistant design.* New York: IBM Corporation.

Russell, B.L. & Pappas, N. (2018). Officer involved domestic violence: A future of uniform response and transparency. *International Journal of Police Science and Management*, *20*(2): 134-142.

Ryan, A. (2000). *The prevalence of domestic violence in police families*. http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4951188/FID707/Root/New/030PG297.PDF

PenzeyMoog, E. (2021). *Design for safety.* USA: A Book Apart.

Southworth, C., Dawson, S., Fraser, C., & Tucker, S. (2005). A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy. *Violence Against Women Online Resources*.

Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge: Cambridge University Press.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online. *Policy & Internet*, *11*(1): 84-103.

Unicef. (2006). *Behind closed doors: The impact of domestic violence on children*. New York: Unicef.

Wetendorf, D. (2004). *When the batterer is a law enforcement officer: A guide for advocates.* USA: Battered Women's Justice Project.

Woodlock, D. (2013). *Technology-facilitated stalking: findings and recommendations from the SmartSafe project*. Collingwood: Domestic Violence Resource Centre Victoria.

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women*, *23*(5): 584-602.

Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracilio, A. (2020a). *Second National Survey on Technology Abuse and Domestic Violence in Australia*. Australia: WESNET.

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020b). Technology as a weapon in domestic violence: Responding to digital coercive control. *Australian Social Work*, *73*(3): 368-380.