Volume **4** (1) 2022 https://doi.org/10.5204/lthj.2160

Technology-Facilitated Domestic and Family Violence: Protecting the Privacy and Safety of Victim-Survivors

Lyria Bennett Moses, Jan Breckenridge, Joshua Gibson and Georgia Lyons
UNSW Sydney, Australia

Abstract

Technology and privacy can be a double-edged sword for those experiencing domestic and family violence (DFV). Technology can be a mechanism for abuse and coercive control but is also offered to victim-survivors as a 'solution' to reduce risk and protect their safety. In theory, the law protects the privacy rights of victim-survivors, but poor practice and lapses in security mean that their information is often shared with those who seek to harm them. Perpetrators, particularly alleged perpetrators, also have a right to privacy, making it more difficult to protect victim-survivors. This paper analyses technology-facilitated domestic and family violence (TFDFV) through a privacy lens—drawing on privacy and DFV literature (and the little that lies at the intersection) and doctrinal analysis of Australian and New Zealand privacy and related laws applied to TFDFV. Recommendations are provided to better protect victim-survivors at the intersection of safety, technology and privacy. While the paper focuses on the Australian and New Zealand context, it hopes to motivate similar questions in other jurisdictions.

Keywords: Technology-facilitated domestic and family violence; privacy; safety; coercive control; information sharing; Internet of Things (IoT); Australia; New Zealand

Introduction

This paper brings together three themes—privacy, technology and DFV. While there is extensive literature covering each area, there is little exploration of the intersection, incorporating the effect of privacy-protective laws on TFDFV and the influence of privacy rights on those providing services to victim-survivors.[1] This exploratory study addresses two research questions: (1) How do existing laws and policies in Australia and New Zealand manage the privacy and safety of victim-survivors and alleged perpetrators of TFDFV? (2) What would bring about better outcomes for victim-survivors?

Given the legal embeddedness of protections for privacy and against DFV, our research questions cannot be analysed both deeply and globally. Therefore, this exploratory study focuses on the laws, policies and practices of Australia and New Zealand, providing some ability to compare across jurisdictions without spreading the analysis too thinly. We nevertheless hope that our findings here will generate further research into how these issues are managed internationally.

[1] Suk, At Home in the Law; Bailey, "It's Complicated"; Kelly, Domestic Violence and the Politics of Privacy; Douglas, "Legal Responses to Non-Consensual Smartphone Recordings."

The Intersection of Technology and DFV

Domestic and Family Violence—Framing the Problem

DFV is a prevalent issue in both Australia and New Zealand. Approximately one in six women and one in sixteen men have experienced physical or sexual violence from a current or former partner in Australia.[2] In New Zealand, approximately 30% of ever-partnered women have experienced at least one episode of physical intimate partner violence, and 13.1% have experienced sexual intimate partner violence.[3] In both countries, gaps in data collection hide the full extent of perpetration; however, these figures are commensurate with international prevalence.

Terminology also contributes to defining what is and is not DFV. Not all DFV is perpetrated in intimate partnerships, and, therefore, not all DFV is intimate partner violence. The term 'family violence' is preferred by Aboriginal and Torres Strait Islander and Māori communities to acknowledge violence perpetrated in a range of kinship relationships.[4] However, legal and social welfare responses designed to enhance victim-survivor safety may only be available in specific relational circumstances. Each Australian jurisdiction has a different definition of DFV, some of which include violence and abuse perpetrated by family members and carers. In contrast, other jurisdictions may limit their definition to intimate partnerships. Flowing on from this, legal definitions may also determine who is eligible for a social welfare/health service or response.

Physical and sexual violence are the most widely recognised manifestations of DFV, arguably because they are criminal offences but also because media reports of DFV lethality shape community perceptions.[5] Often less visible, but also damaging, are experiences of DFV, including emotional, social, spiritual, cultural, psychological and economic abuse.[6] The range of these behaviours creates a context of coercive control,[7] which is central to DFV and establishes a pattern of abuse over time, resulting in limitations on movement and restrictions on liberty. Indeed, a growing body of literature recognises that coercive control has specific dimensions when expressed through digital mediums.[8] This forms part of the growing literature on TFDFV.[9] Yet, TFDFV often remains removed from definitions of DFV, which leads to gaps in protection.

Technology in DFV—Both Problem and Solution

The use of technology in DFV is often characterised in binary terms as either extending opportunities to facilitate harassment and abuse or as a set of effective response strategies designed to enhance victim-survivor safety. Emerging evidence supports both positions. Technology can significantly intensify the perpetration of DFV and extend opportunities for harassment and surveillance of the victim-survivor rendering the perpetrator 'ever present'.[10] Yet recent evaluations of technology responses in DFV demonstrate an increase in victim-survivors' perceptions of safety and is now regularly offered as a solution by some DFV services to manage perpetrator risk and enhance client-survivor safety with technology options including, but not limited to, safety devices, cyber sweeps and audits and CCTV cameras installed in housing to avoid or record violence.[11]

The term 'TFDFV' is an umbrella term that covers one part of this binary, referring to a wide range of behaviours using technology to perpetrate abuse.[12] The victim-survivor is often a current or ex-partner, but TFDFV can also target the victim-survivor's children, family members, friends or new partners. The Australian e-Safety Commissioner describes technology-facilitated abuse as including abusive messages or calls, taking over someone's online accounts, sharing or threatening to share an intimate image without the person's consent, using fake social media accounts to harass the person or tracking someone through a phone or device.[13] TFDFV may also include image-based sexual abuse as a means of harassment and control, including non-consensual sharing of sexual images of a person online or threatening to distribute such images.[14] Concerningly,

[2] ABS, Personal Safety, Australia.
[3] Fanslow, "Change in Prevalence Rates," 5.
[4] Cripps, Communities Working to Reduce Indigenous Family Violence, 2.
[5] Valentine, "Responses to Family and Domestic Violence," 30–44.
[6] Gordon in Cripps, Communities Working to Reduce Indigenous Family Violence, 2.
[7] Stark, Coercive Control.
[8] Woodlock, "Technology as a Weapon in Domestic Violence"; Harris, "Digital Coercive Control."
[9] Douglas, "Technology-Facilitated Domestic and Family Violence"; Essert, "Addressing Imperfect Solutions to Technology-Facilitated Domestic Violence Notes"; Harris, "Spacelessness, Spatiality and Intimate Partner Violence"; Henry, "Beyond the Sext"; Henry, "Technology-Facilitated Sexual Violence"; Powell, "Technology-Facilitated Sexual Violence Victimization Results from an Online Survey of Australian Adults."
[10] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 158–159, 162–163.
[11] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 159–160, 168–170.
[12] Harris, "Technology, Domestic and Family Violence," 1–2.
[13] eSafety Commissioner, "What is Technology-Facilitated Abuse?"
[14] Woodlock, Second National Survey of Technology Abuse and Domestic Violence in Australia, 10.

the 2019 National Community Attitudes Survey found that nearly one in three people believed that if a woman sends a nude image to her partner, she is partly responsible if it is shared without permission.[15]

Recent research suggests that TFDFV is an increasingly prevalent issue. For example, a 2020 survey of 442 frontline domestic violence practitioners in Australia found that almost all had clients who had experienced TFDFV. The most common technologies were text messages, smartphones and Facebook.[16] Survey respondents also noted that increasing reliance on technology due to COVID-19 had opened new avenues for abuse. In New Zealand, Netsafe reported a 36.5% increase in reports of 'personal harm' from April to June 2020 compared to the previous quarter, with personal harm including harassment and bullying, threats and intimidation[17] via digital communications.

An Australian study on image-based sexual abuse found that 11.1% of participants had engaged in some form of image-based sexual abuse perpetration during their lifetime.[18] However, this may underestimate prevalence, as the data was based on the perpetrator's self-reported behaviour. An analysis of image-based sexual abuse offences in Victoria, Australia, found that 58% were perpetrated in the context of DFV.[19] In New Zealand, Netsafe found that nearly 5% of participants reported experiencing such abuse during their lifetime, while approximately 4% had been threatened with such abuse.[20]

Conversely, a range of technology devices and strategies have been developed to ensure the safety of victim-survivors of DFV. Most DFV programs in Australia now provide some form of personal safety device for victim-survivors. Some programs have been successful, such as the Staying Home Leaving Violence program in NSW, which includes an SOS Response System involving a duress alarm and mobile phone with GPS tracking, with participants reporting an increase in feelings of hope and a decrease in fear as well as greater confidence.[21] The Keeping Women Safe in their Homes program in Queensland includes duress alarms, home safety cameras and cyber safety audits as technology responses resulting in women and children reporting they generally felt safer and more secure in their accommodation.[22] The evaluation also found that privacy was a concern among stakeholders, affecting participation. For example, some participants did not want to disclose to their strata or property managers their request for security cameras, fearing consequences for their tenancy. Others were anxious that their personal information would be shared. Stakeholders raised concerns that security camera footage could also be subpoenaed.

Technology may also be used to assess the risk posed by perpetrators of DFV, for example, through electronic location devices monitored by police. Advocates argue that these methods more reasonably attribute responsibility for increasing safety with the perpetrator. However, limitations of this approach include privacy implications, stigmatisation, the potential for 'false' alerts and deficiencies in the monitoring system.[23]

Policy and TFDFV

While there are substantial differences between jurisdictions, there is an emerging recognition of the need to address TFDFV as part of broader policies for addressing DFV.

In Australia, the fourth (current) Action Plan of the *National Plan to Reduce Violence against Women and their Children 2010–2022* (the Action Plan) begins to provide a more nuanced understanding of the intersections between DFV and technology. The Action Plan recognises that technology creates better access to information, including referral to services for victim-survivors. However, technology also facilitates the perpetration of violence, such as online sexual harassment, stalking and non-consensual sharing of intimate images. The Action Plan did adopt a definition of 'technology-facilitated abuse', noting the use of communications technology to control, abuse, harass, punish or humiliate an individual.[24]

Each Australian state and territory, despite different policy approaches to DFV, have begun to recognise TFDFV, albeit in different ways. For example, the Northern Territory framework includes technology-facilitated abuse within their definition of DFV and includes a range of behaviours such as sending abusive text messages or emails, making continuous phone calls,

[15] Parton, Attitudes Towards Violence Against Women and Gender Equality Among People in NSW, 19.
[16] Woodlock, Second National Survey on Technology and Domestic Violence, 18.
[17] Netsafe, "Netsafe Quarterly Report April–June 2020."
[18] Powell, "Image-based Sexual Abuse," 397.
[19] Sentencing Advisory Council, Sentencing Image-Based Sexual Abuse Offences in Victoria, 38.
[20] Pacheco, Image-based Sexual Abuse, 1.
[21] Breckenridge, Staying Home Leaving Violence Evaluation, 101.
[22] Gendera, Evaluation of the Technology Trial (Keeping Women Safe in Their Homes), 3.
[23] Nancarrow, Electronic Monitoring in the Context of Domestic and Family Violence, 2.
[24] Commonwealth of Australia, Fourth Action Plan, 60.

abusing victim-survivors on social media and sharing intimate photos without consent.[25] Similarly, the Victorian framework recognises that perpetrators can use technology to control, intimidate, stalk and harass victim-survivors.[26] The Tasmanian framework identifies technology-facilitated abuse as a new and emerging area requiring attention from policymakers.[27] Policy frameworks in New Zealand have also begun to recognise TFDFV, defining 'online abuse' as the use of technology to stalk, harass or intimidate someone.[28] This may include social media smear campaigns, using smart technology to track a person, sending unwanted explicit photos or messages to a person, or posting explicit pictures of a person online without their consent. Another New Zealand framework outlines key priority areas for responding to family violence and states that more work is needed to develop initiatives that address the effects of technology.[29]

Legislation that directly refers to DFV (or that uses similar terminology) does not refer to TFDFV as such. For example, New Zealand does not refer to technology within its legislative definitions of DFV under the *Family Violence Act 2018*. However, many jurisdictions have legislative prohibitions on specific strands of TFDFV, prominently image-based abuse.[30] Despite the inconsistent use of terminology across jurisdictions, one constant is the lack of attention given to how dimensions of privacy are affected by TFDFV.

Privacy in the Context of TFDFV

What is Privacy

There is extensive scholarship on the meaning and value of privacy. Early on, privacy was viewed as an individual's 'right to be let alone'.[31] Later, Westin's *Privacy and Freedom*[32] offered a definition of privacy that remains at the core of contemporary privacy data protection laws: 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[33] Privacy has been considered an essential part of our humanness,[34] as a 'foundational good'[35] that is important for maintaining relationships. Reflecting the breadth of this vision, it has also been described as a 'notoriously protean concept',[36] which makes it 'hard to capture'.[37] Substantively, privacy has been linked to many different benefits, including (but not limited to) independence of thought and judgment,[38] freedom,[39] consent,[40] equality,[41] personal liberty,[42] human dignity and identity formation,[43] democracy and safety.[44]

In more recent times, privacy scholars have expressed concern about new features of the digital and technology landscape.[45] Cloud platforms,[46] data analytics and poor design,[47] the Internet of Things (IoT)[48] and smart homes[49] are identified as privacy

[25] Northern Territory Government, Domestic, Family and Sexual Violence Reduction Framework 2018–2028, 31.
[26] Victoria State Government, Ending Family Violence, 2.
[27] Department of Communities Tasmania, Safe Homes, Families, Communities, 4.
[28] New Zealand Government, Family Violence Risk Assessment and Management Framework, 21.
[29] New Zealand Government, Pasefika Proud: Pathways for Change, 47.
[30] *Crimes Act 1900* (ACT) ss 72C–72E; *Crimes Act 1900* (NSW) ss 91P–91R; *Criminal Code Act 1983* (NT) Division 7A; *Criminal Code Act 1899* (Qld) ss 207A, 223, 227A, 227B, 229A, 229AA; *Summary Offences Act 1953* (SA) Part 5A; *Police Offences Act 1935* (Tas) ss 13A–13C; *Summary Offences Act 1966* (Vic) Div 4A; *Criminal Code Act Compilation Act 1913* (WA) ss 221BA–221BF.
[31] Warren, "The Right to Privacy," 193.
[32] Westin, Privacy and Freedom.
[33] Westin, Privacy and Freedom, 7.
[34] Fried, "Privacy," 475, 484.
[35] Allen, Unpopular Privacy, 21.
[36] Froomkin, "Privacy as Safety," 145.
[37] Koops, "A Typology of Privacy," 487.
[38] Finn, "Seven Types of Privacy," 9.
[39] Westin, Privacy and Freedom.
[40] Peppet, "Regulating the Internet of Things"; Solove, "Introduction."
[41] Bailey, "Towards an Equality-Enhancing Conception of Privacy."
[42] Fried, "Privacy," 483.
[43] Privacy International, "What is Privacy?"
[44] Froomkin, "Privacy as Safety."
[45] Massey, "Getting to October"; Richards, "The Dangers of Surveillance Symposium."
[46] Kilgore, "Your Head is in the Cloud."
[47] Everson, "Privacy by Design"; Clarke, "The Resistible Rise of the National Personal Data System Focus on Australia"; Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms"; Cavoukian, "Privacy by Design"; Naughton, "Augmented Humanity"; Selvadurai, "Protecting Online Information Privacy in a Converged Digital Environment"; Froomkin, "The Death of Privacy?"
[48] Peppet, "Regulating the Internet of Things"; Jones, "Privacy Without Screens & the Internet of Other People's Things."
[49] Ducich, "These Walls Can Talk!"

threats. It is in this digital space that privacy intersects with TFDFV. Given that the relationship between privacy and TFDFV is newly emerging, it is important to consider how privacy has been considered in the context of DFV.

While steadily growing, there has been limited research regarding DFV and privacy and its benefits and harms in the specific context of TFDFV.[50] Early conceptions of privacy's intersection with gender was driven by feminist thought, which criticised privacy for protecting perpetrators who commit violence *in private*. As Bailey suggests, '[b]ecause privacy was historically used to shield batterers from state intervention, its benefits for domestic violence victims have been ignored'.[51] The ways in which privacy has reinforced gendered violence is what Schneider refers to as the 'dark and violent side of privacy'[52] While some feminist scholars are wary of privacy as a solution for victim-survivors, other scholars raise privacy's role in facilitating safety.[53]

Given the many dimensions to privacy, there have been several typologies or taxonomies that aim to construct distinct categories of privacy, treating and unpacking privacy as pluralist[54] rather than unitary.[55] A recent model,[56] relied on here to discuss different interactions with TFDFV, is that offered by Koops.[57] Koops introduces eight basic types of privacy[58] (i.e., bodily, intellectual, spatial, decisional, communicational, associational, proprietary and behavioural privacy), with 'informational privacy' being the prevention of information being collected or used in non-legitimate circumstances, overlapping but not coinciding with the eight.[59] The eight are also divided into types of privacy that focus on freedom *from* (i.e., the right to be let alone) and those that focus on freedom *to* (i.e., to pursue one's own self-development). The typology is illustrated in Figure 1.[60]

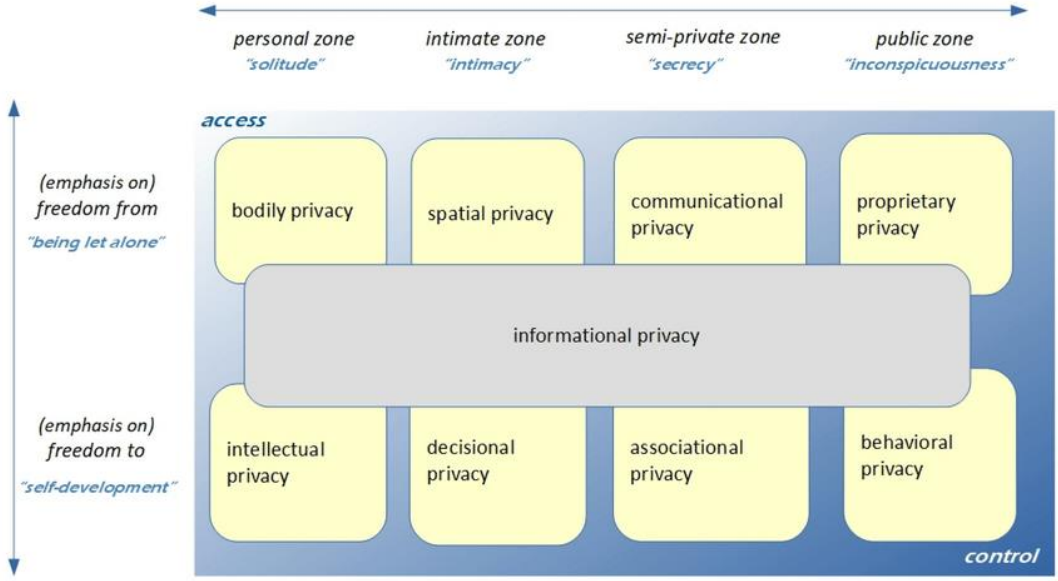

Figure 1. Typology of privacy

[50] Bailey, "It's Complicated"; Suk, At Home in the Law; Kelly, Domestic Violence and the Politics of Privacy; Gotell, "When Privacy is Not Enough"; Arief, "Sensible Privacy"; Goldfarb, "Violence Against Women and the Persistence of Privacy"; Schneider, "The Violence of Privacy Symposium."
[51] Bailey, "It's Complicated," 1780. See also Goldfarb, "Violence against Women and the Persistence of Privacy," 5.
[52] Schneider, "The Violence of Privacy Symposium," 974.
[53] Froomkin, "Privacy as Safety."
[54] Solove, Understanding Privacy, 101–170, 187–195; Finn, "Seven Types of Privacy."
[55] Nissenbaum, Privacy in Context; Moore, Privacy Rights; Cohen, "What Privacy is For."
[56] Koops, "A Typology of Privacy," 487.
[57] Compare Cohen, "What Privacy is For"; Cohen, "Turning Privacy Inside Out"; Finn, "Seven Types of Privacy"; Solove, "A Taxonomy of Privacy"; Solove, "The Myth of the Privacy Paradox."
[58] Koops, "A Typology of Privacy," 567–569.
[59] Koops, "A Typology of Privacy," 568.
[60] Koops, "A Typology of Privacy," 484.

In addition to the above categories, this article additionally includes and considers locational privacy[61] (i.e., knowledge about where an individual is or has been[62]), a particularly important and relevant category to TFDFV.

Conceiving of Victim-Survivors' and Perpetrators' Privacy

In this section, we use Koops' typology to focus on the categories of privacy (of both victim-survivors and perpetrators) that affect TFDFV. We demonstrate that, while 'ICT security and privacy are essential to domestic violence survivors',[63] privacy can also frustrate the efforts of victim-survivors and support agencies to capture or monitor violent or threatening behaviour.

Privacy offers victim-survivors practical protection in certain circumstances. The clearest example of this is in relation to locational privacy. Locational privacy is particularly important for victim-survivors of TFDFV, where perpetrators actively deploy technology to cause psychological distress or create opportunities for physical violence.[64] Locational privacy can be lost through applications like Apple's *Find My iPhone* or *Find My Friends*, which can lead to unwanted physical encounters, fear of encounters and potential physical danger for victim-survivors.[65] Unauthorised access to locational information can lead to infringements against bodily privacy[66] and spatial privacy. When victim-survivors regain control over their personal information,[67] including locational data, their physical safety is likely to increase.[68]

Informational privacy more broadly is also a key concern for victim-survivors, particularly due to the routine sharing that occurs in intimate relationships. If two people are joint account holders with a bank, the bank will, both regularly and on request, share information about transactions with both. Similarly, if a perpetrator has an account with a telecommunications provider and the victim-survivor's mobile phone number is part of that account, the perpetrator can not only access information about the use of that mobile phone, but they can also disrupt or commandeer services.

There are a variety of 'structural problems'[69] that lead to even well-informed individuals lacking the requisite knowledge for managing informational privacy, all of which can have more serious consequences for victim-survivors of TFDFV. Often, the security, integrity and protection of data is unclear, usually due to privacy policies being vague, complex or sometimes unread.[70] For example, some COVID-19 sign-in protocols, particularly early in the pandemic, used platforms that sold data or were not secure, and domestic violence survivors were warned to find other means to facilitate contact tracing.[71] Victim-survivors may also lose control of their data through data breaches, which are frequent.[72] When a breach occurs, information about a victim-survivor, such as location, communications channels (including email addresses), habits, health, transactions and passwords, may become available to anyone, including perpetrators. Depending on the data that a perpetrator can access, this might compromise locational, spatial, communicational and/or informational privacy, as well as eventually bodily privacy.

Victim-survivors are also at risk where devices are compromised, which may affect spatial privacy given that compromised devices often exist physically in the home space. This is particularly the case in relation to the IoT, often through smart home appliances. Smart home technology is on the frontier as a new form of 'harassment, monitoring, revenge and control'.[73] As Froomkin and Colangelo note:

> [a]lready, domestic abuse victims have reported that former partners used remotely controlled devices to change electronic locks, ring the doorbell, change the behaviour of thermostats or lights, set smart speakers to blare music or spy on them via security cameras.[74]

[61] Blumberg, "On Locational Privacy"; Froomkin, "Privacy as Safety," 163–165.
[62] Froomkin, "Privacy as Safety," 158.
[63] Dragiewicz, "Domestic Violence and Communication Technology," 11.
[64] Dragiewicz, "Domestic Violence and Communication Technology," 24–25, 33, 36.
[65] Froomkin, "Privacy as Safety," 163–174; Dragiewicz, "Domestic Violence and Communication Technology."
[66] While the risk of physical violence in domestic violence situations is high, the focus of this paper is on the technological aspect and, therefore, we do not go into more detail about bodily privacy.
[67] Fried, "Privacy," 482.
[68] Froomkin, "Privacy as Safety"; Blumberg, "On Locational Privacy."
[69] Solove, "Introduction," 1881.
[70] Levy, "Intimate Surveillance," 690.
[71] Safetynet, "Covid-19 QR Code Scanners."
[72] Mele, "Data Breaches Keep Happening."
[73] Bowles, "Thermostats, Locks and Lights."
[74] Froomkin, "Privacy as Safety," 199.

The coercive gaslighting of victim-survivors through digital control of devices from afar exacerbates the isolation and helplessness felt by victim-survivors within their homes, making them feel 'as if they were going crazy'.[75] This may infringe on an individual's behavioural privacy when this occurs to victim-survivors in public spaces. Alternatively, when IoT invasions occur in the home they may affect victim-survivor's spatial privacy by altering the way victim-survivors' might access, use, or function in such spaces. Thus, IoT control by perpetrators may compound pre-existing violence. Victim-survivors may have little recourse in these kinds of scenarios, as contractual rights and consumer protections are often linked to the person *purchasing* the device, not those living with it. From a practical perspective, few information security measures will be effective against a person with physical access to a device in additional to legal rights to control access.

While it is common to think about the invasion of a TFDFV victim-survivor's right to privacy, it is important to recognise that a victim-survivor may seek to protect themselves in ways that may compromise an offender's privacy. Examples include (1) the use of CCTV cameras as a deterrent, which may be used to document violence for protection orders or provide evidence of their breach, (2) surreptitiously recording an offender on a personal device to prove an act of violence and (3) seeking to track the location of an offender to avoid crossing paths. Government agencies that support DFV victim-survivors, including law enforcement and support agencies, may seek to share information to better protect victim-survivors and hold perpetrators to account. Further, as a report from the Council of Europe explains,[76] orders removing an alleged perpetrator from their home or preventing contact with children infringe on rights otherwise protected in international human rights law (such as the right to family life and the right to property).

Thus, it is not the case that enhancing privacy protections across the board would necessarily promote the safety and interests of DFV victim-survivors or be otherwise justifiable. Often there are challenges in balancing privacy rights against other competing rights.[77] Consider, for example, the right to erasure in Europe's General Data Protection Regulation (GDPR), also known as the 'right to be forgotten'.[78] This allows an individual to, for example, request Google to remove links to stories about them. While victim-survivors can use this (e.g., to make it harder to find information about them that might compromise their safety), perpetrators can also use it (e.g., to make it harder for future potential victim-survivors to find online warnings published by an ex-partner). Calls for adopting GDPR-style protections in Australia, which may offer broad benefits to the community at large, need to be weighed against potential harms in the specific context of DFV.

Legal Protection for Privacy and Intersection with TFDFV Scenarios: Australia and New Zealand

Law is an imperfect instrument in protecting the privacy of victim-survivors of TFDFV. Privacy laws govern the collection and use of personal information, which may affect informational and communicational conceptions of privacy. Civil and criminal laws prohibit certain interferences with communications and computers. Legislation may also prohibit particular conduct, from 'peeping' to non-consensual sharing of intimate images. All these privacy-protective laws protect the privacy of victim-survivors of TFDFV *as well as* the rights of alleged perpetrators. Unlike the law around apprehended violence orders, these laws are not specifically directed to DFV and, thus, are not specifically focused on assisting victim-survivors. Stalking and intimidation laws, like DFV laws, operate in a single direction. Because privacy-protective laws are generally technology-agnostic and often context-agnostic, they are not directed specifically at the privacy harms associated with TFDFV. Given the rapid escalation of TFDFV, it is worth considering their applicability and effectiveness in that context.

Privacy

Australian law does not include a constitutional right to privacy. While privacy is recognised as a human right in Victoria,[79] the ACT[80] and Queensland,[81] these human rights charters are more applicable to state action that may infringe privacy rather than one person infringing on another's privacy. There is no well-recognised tort of privacy in Australia.[82] The primary statutory source for protection of informational privacy is the *Privacy Act 1988* (Cth) and equivalent state and territory laws. The Commonwealth legislation applies to most government agencies and large private organisations while excluding small businesses.[83] While the Commonwealth legislation does not explicitly regulate the conduct of individuals, such as perpetrators of TFDFV, it will affect the ability of individuals to receive information about another person, such as a victim-survivor, from

[75] Bowles, "Thermostats, Locks and Lights."
[76] Logar, Emergency Barring Orders in Situations of Domestic Violence, 19–20, 24–27.
[77] Clapham, Balancing Rights.
[78] *General Data Protection Regulation 2018* art 17.
[79] *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(1).
[80] *Human Rights Act 2004* (ACT).
[81] *Human Rights Act 2019* (Qld).
[82] Australian Law Reform Commission (ALRC), Serious Invasions of Privacy in the Digital Era.
[83] *Privacy Act 1988* (Cth) s 6C.

a third party. For example, data breach notification means victim-survivors will often know when their information has been compromised.[84] This is an example of where institutions recognise that informational—and communicational—privacy may be considered to protect victim-survivors.

In New Zealand, the *Bill of Rights Act 1990* includes a right to be secure against unreasonable search and seizure[85] but no express general right to privacy. Thus, as is the case in Australia, protections are found in statute and common law. New Zealand's *Privacy Act 2020* applies to New Zealand residents, most New Zealand public sector agencies, private sector bodies established or managed/controlled in New Zealand and, in some circumstances, overseas bodies and non-residents. Like the Australian equivalent, the focus is on informational privacy. Information privacy principles in the Act regulate the processes through which agencies can collect, use and disclose personal information. While individuals are technically subject to the Act, the Act is more relevant to organisations (except in the context of surveillance in a domestic context, addressed below). As discussed in relation to the Australian context, the main relevance of this law is the ability for victim-survivors to take protective measures where their data has been compromised due to data breach notification requirements.[86]

Further, actions related to breaches of the Act can be brought by the Director of Human Rights Proceedings (or alternate) or, in some circumstances, by individuals. Unlike Australia, the common law of New Zealand does include a tort of invasion of privacy. However, this tort is focused on publicity or publication of material in which the plaintiff has a reasonable expectation of privacy.[87] This might include the non-consensual posting of private images, for example, but not cyberstalking or other conduct that is solely between the perpetrator and victim-survivor.

Computer Crimes and Surveillance Devices

Australian criminal legislation also regulates other behaviour regarding informational privacy. This includes the unauthorised access of 'restricted data'[88] and the more serious offence of unauthorised access to data with the intention to commit or facilitate the commission of a serious offence.[89] In the context of TFDFV, individuals who hack locational information about others may commit the more serious offence. Those who impair electronic communications, cutting off access to friends or family, may also be in violation of the law.[90] While challenges remain with shared telephone accounts, as outlined above, there are provisions that reduce the ability of a perpetrator to 'port' a victim-survivor's telephone number.[91] This is in addition to a general prohibition on telecommunications interception.[92] Legislation guiding the behaviour of surveillance devices applies across Australia but is jurisdiction specific.[93] An expanded outline of the situation of surveillance in each state and territory (analysed in the context of DFV) can be found on WESNET's legal guide to surveillance legislation.[94] These laws are used in deciding whether a recording is admissible as evidence, including in proceedings where DFV is alleged. However, evidence can be admitted in some circumstances despite having been obtained in breach of these laws.[95]

As in Australia, there are criminal consequences for crimes involving inappropriate access to computers in New Zealand.[96] For example, it is an offence to access a computer system without authorisation, although it is not an offence if a person who is otherwise authorised accesses a system for a purpose other than the one for which that person was given access.[97] This suggests that an individual who is generally authorised to use a shared computer does not commit the offence if they access files on that computer (e.g., emails) that are not within the authorisation given. A more serious offence applies if a system is accessed without authorisation and, dishonestly or by deception and without claim of right, an individual either obtains a benefit or causes loss to another person[98] or intends to do so.[99] As in Australia, the main difficulty with such offences in the context of

[84] *Privacy Act 1988* (Cth) Part IIIC.
[85] *Bill of Rights Act 1990* (NZ) s 21.
[86] *Privacy Act 2020* (NZ) Part 6.
[87] *Hosking v Runting* [2004] NZCA 34.
[88] *Criminal Code Act 1995* (Cth) s 478.1.
[89] *Criminal Code Act 1995* (Cth) s 477.1.
[90] *Criminal Code Act 1995* (Cth) s 477.3.
[91] *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*.
[92] *Telecommunications (Interception and Access) Act 1979* (Cth).
[93] *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2016* (SA); *Surveillance Devices Act 1998* (WA); *Listening Devices Act 1992* (ACT); *Listening Devices Act 1991* (Tas); *Invasion of Privacy Act 1971* (Qld); *Surveillance Devices Act 1999* (Vic).
[94] WESNET, "Women's Legal Guides on Tech-based Abuse."
[95] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 170, 176–177.
[96] *Crimes Act 1961* (NZ) ss 248–252.
[97] *Crimes Act 1961* (NZ) s 252.
[98] *Crimes Act 1961* (NZ) s 249(1).
[99] *Crimes Act 1961* (NZ) s 249(2).

TFDFV is the question of the scope of 'authorisation' in the context of shared devices. Such laws recognise the real harms that could be caused by inappropriate access to such information, inherently protecting informational and communicational privacy, which may inevitably protect bodily privacy. New Zealand law also regulates communications privacy.[100] Separate legislation further prohibits devices used to intercept private communications.[101]

New Zealand does not have separate surveillance device legislation (except with respect to police and private investigators). Instead, this is regulated under the *Privacy Act 2020* (NZ) and through the prohibition on intimate visual recordings.[102] Because the *Privacy Act 2020* (NZ) applies to individuals, there is a specific exception for individuals collecting or holding information 'solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs', provided that this would not be 'highly offensive to an ordinary reasonable person'. A perpetrator using devices to record the actions or location of a victim would generally be collecting information contrary to the terms of the Act, which, because it is 'highly offensive' would not fall within the exception. Conversely, a victim-survivor using devices to record the violent actions of the perpetrator for evidence purposes would likely be able to rely on the exception. However, much will be left to interpretation in the context of particular facts.

Institutions Regulating Online Behaviour

Australia has an e-Safety Commissioner equipped with the legislative responsibility of promoting online safety.[103] Recent legislation introduces a cyber abuse scheme for all Australians, providing authority for the Commission to require adult cyber abuse material be taken down from social media if the material is posted with the likely intention of causing serious harm.[104] It also provides strengthened provisions to respond to image-based abuse,[105] including in the context of DFV.[106]

In New Zealand, the *Harmful Digital Communications Act 2015* (NZ) sets out specific communication principles that apply in relation to communications. Netsafe, a private organisation, is an 'approved agency' under the law,[107] which provides it with the authority to assess and investigate complaints[108] of individuals who have suffered, or will suffer, harm because of digital communication.[109] Netsafe can also request take-down or advise, negotiate, mediate and persuade others. After the process of engaging with Netsafe, there is an option to apply to the District Court.[110] The Act also creates an offence of causing harm by posting a digital communication with intention to cause harm.[111] Prohibitions on making and the publication of intimate visual recordings is regulated by the criminal law.[112]

Privacy and Information Sharing

As with the rise of data and technology, an increasingly important area of concern is the use, misuse and sharing of data. The inevitable fear of this information in violent hands may lead to the most severe infringements of bodily privacy of victim-survivors. Victim-survivors of DFV may benefit from integrated service provision. Most jurisdictions have, thus, introduced integrated service meetings of organisations and workers to share information about clients assessed to be at high risk of serious physical violence or potential lethality, which is located within relevant domestic violence legislation.[113] Risk assessments may also be shared between organisations for medium to low-risks clients. Information sharing has been recognised as important in the context of DFV by Australian Law Reform Commission,[114] in the *National Plan to Reduce Violence against Women and their Children 2010–2022* and the Fourth Action plan under it, and in New Zealand's *Family Violence, Sexual Violence and Violence within Whānau: Workforce Capability Framework* and *Pasefika Proud: Pathways for Change 2019–2023.*

---

[100] *Telecommunications Industry Privacy Code 2020*.
[101] *Crimes Act 1961* (NZ) Part 9A.
[102] *Crimes Act 1961* (NZ) s 216H.
[103] *Online Safety Act 2021* (Cth)*; Enhancing Online Safety Act 2015* (Cth).
[104] *Online Safety Act 2021* (Cth) s 7.
[105] *Online Safety Act 2021* (Cth) Part 6.
[106] Explanatory Memorandum, Online Safety Bill 2021 (Cth) 15, 53, 56.
[107] *Harmful Digital Communications Act 2015* (NZ) ss 7–10.
[108] *Harmful Digital Communications Act 2015* (NZ) s 8(1)(a),(b).
[109] *Harmful Digital Communications Act 2015* (NZ) s 11(1)(a).
[110] *Harmful Digital Communications Act 2015* (NZ) s 8(5).
[111] *Harmful Digital Communications Act 2015* (NZ) s 22.
[112] *Crimes Act 1961* (NZ) Part 9A.
[113] *Domestic Violence Agencies Act 1986* (ACT) s 18; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) ss 98D–98N; *Domestic and Family Violence Act 2007* (NT) s 125; *Domestic and Family Violence Protection Act 2012* (Qld) ss 169D–169O; *Family Violence Act 2004* (Tas) ss 37, 39; *Family Violence Protection Act 2008* (Vic) Part 5A–Part 5B; *Restraining Orders Act 1997* (WA) s 70A; *Intervention Orders (Prevention of Abuse) Act 2009* (SA) s 38.
[114] ALRC, Family Violence.

In some jurisdictions, there are specific rules for the ways in which information is to be shared in the context of family violence, often overriding privacy laws. These are generally framed in terms of confidentiality and confidential information as well as in terms of privacy. New Zealand law encourages family violence agencies and social services practitioners to request, use or disclose personal information for purposes related to family violence.[115] Agencies and practitioners are authorised to disclose information where they believe on reasonable grounds that the disclosure will help the recipient agency make a family violence risk or need assessment or ensure that a victim-survivor is protected.[116] The *Privacy Act 2020* (NZ) also has provision for approved information sharing agreements between or within agencies that can authorise activities such as collecting, storing, checking, using, disclosing and exchanging information including personal information. There are similar provisions in Australian states and territories.[117] These laws are recognised by the Office of the Australian Information Commissioner as a reason for not needing to notify an individual (perpetrator) that information is being collected about them.[118]

The Complexity of Practice

Despite laws that purport to protect victim-survivor's privacy and safety, lack of training, mistakes and poor risk management can undermine the privacy of victim-survivors in ways that compromise their safety. In this section, we explore the challenges of law in action and the reasons why the system can fail to protect the privacy (and hence the safety) of victim-survivors. This section draws on published decisions of privacy commissioners in response to complaints involving disclosure of personal information about a victim-survivor to a perpetrator. While case outcomes published by privacy commissioners represent a small fraction of actual privacy infringements, it is noticeable that many relate to situations where personal information about a victim-survivor is made available to the perpetrator, or in other words, where informational and communicational privacy was breached.

The cases illustrate the ways in which poorly designed systems, insufficient staff training and inadequate security create hazards for victim-survivors. In one case, the records of the complainant and her former partner were not immediately delinked, despite the complainant's attempts to do so, because forms were not *correctly* completed and *insufficient* evidence was provided.[119] The continued linking meant that the former partner was automatically notified of the complainant's change of address. Failure of business rules to factor in risks associated with DFV can be corrected once discovered, although greater awareness of DFV by those creating the rules in the first place would be a significant step forward. Many cases involve human error, for example, not redacting locational information,[120] disclosure outside business rules[121] and sending correspondence to an old email address.[122] In these situations, the rules (legal and/or operational) were not followed, suggesting a need for employee training that focuses on the importance of following procedures and the potentially deadly consequences of compromising an individual's communicational and informational privacy by not doing so.

Employees not following procedures is risky when combined with an active attacker seeking to compromise socio-technical information systems to obtain personal information about their victim-survivor. In one case, personal information was provided without asking for a password (despite the woman concerned having set this procedure up to protect herself);[123] in another, a man asked a female friend to represent herself as his former wife, which she did to obtain the wife's credit card statements (again, no password check was conducted).[124] In such contexts, perpetrators are active security threats to the system; to protect victim-survivor privacy in such scenarios requires an approach to security (likely involving strong passwords) that factors in an attacker profile of someone with access to substantial general personal information about a victim-survivor. Better processes, training and security would have prevented all the above cases, each of which posed a threat to the victim-survivor's life, safety or health (including mental health).

[115] *Family Violence Act 2018* (NZ) Part 2.
[116] *Family Violence Act 2018* (NZ) s 24.
[117] *Domestic Violence Agencies Act 1986* (ACT) s 18; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) Part 13A; *Privacy Code of Practice (General) 2003* Part 8 (Domestic Violence Intervention Court Model); *Domestic and Family Violence Act 2007* (NT) Part 5A; *Domestic and Family Violence Protection Act 2012* (Qld) Part 5A; *Intervention Orders (Prevention of Abuse) Act 2009* (SA) s 38; *Family Violence Act* 2004 (Tas) ss 37–39; *Family Violence Protection Act 2008* (Vic) Part 5A; *Restraining Orders Act 1997* (WA) s 70A.
[118] Office of the Australian Information Consumer (OAIC), Chapter C: Permitted General Situations.
[119] *WZ and CEO of Services Australia (Privacy)* [2021] AICmr 12 (13 April 2021).
[120] *'ST' and Chief Executive Officer of Services Australia (Privacy)* [2020] AICmr 30 (30 June 2020).
[121] *Complainant B v Statutory Entity* [2003] VPrivCmr 2 (20 June 2003).
[122] *Case Note 300915* [2020] NZPrivCmr 2.
[123] *Case Note Annual Report 2001/02 (settlement)* [2002] NZPrivCmr 15.
[124] *Case Note Annual Report 2004/05 (disclosure)* [2005] NZPrivCmr 7.

Paths Forward

There are both synergies and tensions in looking at the issue of DFV through the lenses of technology, safety and privacy. In some circumstances, privacy can be imperative to ensure victim-survivors safety by protecting their information from those who would use it to cause them harm. Conversely, keeping information about victim-survivors and perpetrators secure can undermine efforts of integrated service provision and collaboration between workers that might support safety for victim-survivors and monitor perpetrator risk. Technology such as mobile phones and computers can be a lifeline for victim-survivors, reducing isolation and allowing further support options but can also lead to loss of privacy and safety by allowing perpetrators to follow their movements.

The opportunity to explore the intersections of these threads in the context of TFDFV suggests some possible ways forward. In this section, we explain some preliminary recommendations in the Australian and New Zealand context, with the hope that they may lead further research to consider whether similar measures would be effective elsewhere.

Law Reform

While New Zealand has recently updated its privacy laws, a variety of law reform processes are currently underway in Australia, including in the contexts of privacy law and cyber security.[125] Therefore, there is the possibility that Australian privacy laws will be strengthened and security standards mandated, particularly in relation to IoT devices. We focus here on reforms in Australia and New Zealand that would be of specific benefit to victim-survivors. The three main areas for reform are surveillance device legislation, information sharing rules and data breach notification laws.

Surveillance device legislation needs to balance the different interests of those who may be sharing a home, particularly where their needs and interests are not uniform. While some Australian jurisdictions already prohibit installation of surveillance devices in a home without the informed and voluntary consent of all adults whose private activities may be filmed, this is not consistent.[126] The Australian Law Reform Commission has recommended national uniformity through Commonwealth legislation.[127] Douglas and Burdon argue for the importance of recognising differences between the use of surveillance devices by perpetrators and victim-survivors.[128] They suggest this might be done through judicial interpretation of the existing 'lawful interests' exception that allows for recording where this is necessary to protect the lawful interests of the recording party.[129] In particular, they propose that judicial interpretation proceed on the basis of an understanding of 'a broader jurisprudential understanding of privacy as protector and facilitator of individual autonomy'.[130] In our view, legislative reform is a firmer path to distinguish between the use of surveillance devices by perpetrators for purposes such as coercive control and victim-survivors for the purposes of safety and evidence. As explained above, New Zealand draws a distinction in the context of domestic surveillance based on whether the collection of information, including through recording, is 'highly offensive' to a reasonable person. However, this requires similar judicial nuance in interpretation as the Australian concept of 'lawful interests'. It would be preferable in both jurisdictions for relevant statutes to provide clearer rules that can be easily interpreted by non-lawyers to provide guidance on the circumstances in which domestic surveillance is permitted. The suggestion of the Law Commission in New Zealand provides a useful way forward. They propose permitting surveillance by a person who believes on reasonable grounds that it is necessary 'for the protection for the health or safety of any person' or 'to provide evidence that an offence has been or was being committed or planned', provided the surveillance is no more than reasonably necessary for such purposes.[131] One narrowing we would propose is to limit the offences that would justify surveillance.

Integrated service provision requires information sharing to coordinate practice and ensure safety. However, information sharing protocols and rules are often different in the domains of DFV and child protection, despite the practical overlap between the two scenarios. These rules should be harmonised, using similar language and concepts, with any differences in the two clearly explained in legislation and justified in related explanatory memoranda. Greater alignment between the two sets of rules will simplify compliance and training for staff in the field and reduce confusion in the many cases that cut across both contexts. Greater consideration is also required to develop policies about sharing information collected from victim-survivors of DFV with agencies with power to remove children from parental care. There is a risk that oversharing (or belief in oversharing) will

[125] For example, Australian Government, "Strengthening Australia's Cyber Security Regulations and Incentives"; Attorney-General's Department, "Review of the Privacy Act 1988 (Cth)."
[126] WESNET, "Women's Legal Guides on Tech-based Abuse."
[127] ALRC, Serious Invasions of Privacy in the Digital Era, recommendation 14–1.
[128] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 159.
[129] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 184.
[130] Douglas, "Legal Responses to Non-Consensual Smartphone Recordings," 184.
[131] Law Commission Te Aka Matua O Te Ture, "Invasion of Privacy."

reduce reporting rates of DFV, particularly in Indigenous communities.[132] At the same time, it is important to identify and protect children at risk of harm. Our research does not provide answers to this delicate balance, but it does identify its importance.

One aspect of broader privacy reforms that is particularly relevant in the context of DFV is mandatory data breach notification requirements. There remain some jurisdictions that have yet to enact such laws. The drafting of such laws should also recognise that most organisations *will not know* whether those affected by a data breach are at increased risk of violence as a result. For example, the current standard in the *Privacy Act 1988* (Cth) is that a data breach is 'eligible' where 'a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates'.[133] Similar language appears in the definition of notifiable privacy breach in New Zealand's legislation.[134] However, given the general lack of knowledge of organisations of the circumstances of those about whom they hold data, this should be rewritten to require disclosure *except* in cases where a reasonable person would conclude that the access or disclosure is *unlikely* to result in serious harm. The difference between the current law and the proposed reform relates to whether an individual is notified when the organisation does not know the personal circumstances of that individual. In most of the situations discussed in *Complexity of Practice*, the organisation was unaware that the individual affected by their conduct was a victim of DFV. Indeed, this will be the most common scenario. In that context, the default should be to ensure that individuals are notified and, thus, can manage any increased risks of serious harm themselves. The only circumstance in which notification would not be required is where, perhaps because of the nature of the data involved in the breach, a reasonable person would conclude that the access or disclosure is unlikely to result in serious harm. Guidance from the regulator to organisations should specifically reference the possibility of information being used by perpetrators of DFV violence as a factor for organisations to consider in the assessment.

Changes in Process

There are some standard business processes (in the context of both government and the private sector) that should be modified to take account of the needs of victim-survivors. These relate to disaggregation of joint accounts, processes around information sharing, transparency about information sharing and taking account of DFV scenarios in relevant security policies.

There are a variety of contexts in which domestic partners or families share an account or have linked accounts, either with business service providers (such as utilities and financial institutions) or with government (e.g., for certain welfare payments). All organisations that allow for this need to also allow for rapid account disaggregation or delinking on request and, if necessary, temporarily suspending communications containing sensitive personal information until forms and identity verification processes can be completed. This is particularly crucial for accounts that include location or address information, such as telecommunications services accounts.

Processes for information sharing (where legally permitted) should be designed to ensure that security is paramount, both in the course of information access or transfer and through general information management. Ensuring that information sharing does not undermine the privacy of those whose information is being shared is critical in protecting their personal security and safety.

Where information sharing does occur, it is important to maintain trust with those whose information is shared, particularly where they are at risk. Everyone, but particularly victim-survivors, should be kept informed about how and with whom their data may be shared (e.g., electronically, in case conferences or in high-risk inter-agency meetings). Information should also be made available about whether such sharing is secure and, at a high level, the kinds of arrangements in place to protect their privacy.

Cyber security and information security need to be designed with the needs of victim-survivors in mind. Agencies should specifically analyse the threat that perpetrators pose, particularly given they often have intimate knowledge of victim-survivors personal information and circumstances.

It will be important to include information sharing and privacy within the context of DFV in future government policies related to DFV.

[132] Langton, Improving Family Violence Legal and Support Services, 21.
[133] *Privacy Act 1988* (Cth) s 26WE(2).
[134] *Privacy Act 2020* (NZ) s 112.

Improvements in Training

Expertise in DFV and privacy rarely overlap, yet it is crucial that those providing services to victim-survivors are aware of both sets of issues and how these relate to the role they are performing. Training on information sharing legal frameworks and related security arrangements is essential. Frontline staff should be given specific training to reduce the risk of accidental disclosure to perpetrators, particularly in the context of domestic relationships where a perpetrator will know enough to answer standard 'security questions'. Training is also required specifically on safety and privacy issues associated with technology—both in contexts where perpetrators exploit technology (e.g., spyware) and where it claims to protect victim-survivors.

Further Research

Our final recommendations relate to future research. As explained at the outset, this was a preliminary study considering TFDFV through a pluralist privacy approach, limited primarily to doctrinal and legislative analysis. Given the importance of the issue, we believe that further research is required to confirm our findings in the jurisdictions analysed and to identify similar issues in other jurisdictions. Further evidence is required on the effectiveness of technology tools that claim to protect victim-survivors and to establish best practice in the delivery and implementation of technological tools that increase the safety of victim-survivors or monitor perpetrators as part of an ongoing research and policy agenda on TFDFV. This research should address specific important empirical questions, such as whether it is better to notify perpetrators that their partner is using a duress alarm or CCTV camera or whether such notifications antagonise perpetrators and increase the likelihood of violence. It would also be worth exploring the possibility of partnerships between technology companies and DFV service providers to explore ways to improve the design of applications and platforms in ways that reduce the risks of TFDFV and related loss of privacy.

Acknowledgement
This research was pursuant to a grant from the International Association of Privacy Professionals (Australia and New Zealand).

Bibliography

Allen, Anita. *Unpopular Privacy: What Must We Hide? Studies in Feminist Philosophy*. New York, NY: Oxford University Press, 2011.

ALRC. *Family Violence—A National Legal Response* (Report 114). Sydney, NSW: ALRC, 2010.

———. *Serious Invasions of Privacy in the Digital Era* (Report 123). Sydney, NSW: ALRC, 2013.

Arief, Budi, Kovila P. L. Coopamootoo, Martin Emms and Aad van Moorsel. "Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse." In *Proceedings of the 13th Workshop on Privacy in the Electronic Society—WPES '14*, 201–4. Scottsdale, AZ: ACM Press, 2014. https://doi.org/10.1145/2665943.2665965

Attorney-General's Department. "Review of the Privacy Act 1988 (Cth)—Issues Paper," 30 October 2020. https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

Australian Bureau of Statistics (ABS). *Personal Safety, Australia, 2016.* Canberra, ACT: ABS, 2017.

Australian Government. "Strengthening Australia's Cyber Security Regulations and Incentives," 2021. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf

Bailey, Jane. "Towards an Equality-Enhancing Conception of Privacy." *Dalhousie Law Journal* 31, no 2 (2008): 267–310.

Bailey, Kimberly D. "It's Complicated: Privacy and Domestic Violence." *American Criminal Law Review* 49, no 4 (2012): 1777–1814.

Blumberg, Andrew and Peter Eckersley. "On Locational Privacy, and How to Avoid Losing It Forever." *Electronic Frontier Foundation: Defending Freedom in the Digital World*, 2009.

Bowles, Nellie. "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse." *The New York Times*, 23 June 2018, sec. Technology. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Breckenridge, Jan, Inara Walden and Gabrielle Flax. *Staying Home Leaving Violence Evaluation: Final Report*. Sydney, NSW: Gendered Violence Research Network, 2014.

Cavoukian, Ann. "Privacy by Design: Leadership, Methods, and Results." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, 175–202. Dordrecht: Springer Netherlands, 2013. https://doi.org/10.1007/978-94-007-5170-5_8

Clapham, Andrew. *Balancing Rights—Free Speech and Privacy. Human Rights: A Very Short Introduction*. New York, NY: Oxford University Press, 2015.
Clarke, Roger. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms." Xamax Consultancy Pty Ltd, 1997. http://www.rogerclarke.com/DV/Intro.html
———. "The Resistible Rise of the National Personal Data System Focus on Australia." *Software Law Journal* 5, no 1 (1992): 29–60.
Cohen, Julie E. "Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20, no 1 (2019): 1–31. https://doi.org/10.1515/til-2019-0002.
———. "What Privacy is For." *Harvard Law Review* 126, no 7 (2013): 1904–1933.
Commonwealth of Australia. *National Plan to Reduce Violence against Women and their Children 2010–2022*. Canberra, ACT: Commonwealth of Australia, 2010.
Commonwealth of Australia. *Fourth Action Plan: National Plan to Reduce Violence against Women and their Children 2010–2022*. Canberra, ACT: Commonwealth of Australia, 2019.
Cripps, Kyllie and Megan Davis. *Communities Working to Reduce Indigenous Family Violence*. Canberra, ACT: Indigenous Justice Clearinghouse, 2012.
Department of Communities Tasmania. *Safe Homes, Families, Communities: Tasmania's Action Plan for Family and Sexual Violence 2019–2022*. Hobart, TAS: Department of Communities Tasmania, 2019.
Douglas, Heather and Mark Burdon. "Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence." *University of New South Wales Law Journal*, no 1 (2018): 157–184.
Douglas, Heather, Bridget A. Harris and Molly Dragiewicz. "Technology-Facilitated Domestic and Family Violence: Women's Experiences." *The British Journal of Criminology* 59, no 3 (9 April 2019): 551–570. https://doi.org/10.1093/bjc/azy068
Dragiewicz, Molly, Bridget Harris, Delanie Woodlock, Michael Salter, Helen Easton, Angela Lynch, Helen Campbell, Jhan Leach and Lulu Milne. "Domestic Violence and Communication Technology." *QUT* (2019): 1–52.
Ducich, Stefan. "These Walls Can Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment." *Duke Law & Technology Review* 16, no 1 (2018): 278–299.
Eitkan, Ilker, Saluamain Abubakar Musa and Rukayya Sunusi Alkassim. "Comparison and Convenience Sampling and Purposive Sampling." *American Journal of Theoretical and Applied Statistics* 5, no 1 (2016): 1–4.
e-Safety Commissioner. "What is Technology-Facilitated Abuse?" n.d. https://www.esafety.gov.au/key-issues/domestic-family-violence/technology-facilitated-abuse
Essert, Cassandra. "Addressing Imperfect Solutions to Technology-Facilitated Domestic Violence Notes." *Women's Rights Law Reporter* 41, no 3–4 (2019–2020): 117–143.
Everson, Eric. "Privacy by Design: Taking Ctrl of Big Data." *Cleveland State Law Review* 65, no 1 (2017): 27–44.
Fanslow, Janet, Ladan Hashemi, Zarintaj Malihi, Pauline Gulliver and Tracey McIntosh. "Change in Prevalence Rates of Physical and Sexual Intimate Partner Violence Against Women: Data from Two Cross-Sectional Studies in New Zealand, 2003 and 2019." *BMJ Open* 11, no 3 (2021): 1–14. http://dx.doi.org/10.1136/bmjopen-2020-044907
Finn, Rachel L., David Wright and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet, 3–32. Dordrecht, Netherlands: Springer Netherlands, 2013.
Fried, Charles. "Privacy." *Yale Law Journal* 77, no 3 (1968): 475–493.
Froomkin, Michael. "The Death of Privacy?" *Stanford Law Review* 52, no 5 (2000): 1461–1544.
Froomkin, Michael and Zak Colangelo. "Privacy as Safety." *Washington Law Review* 95, no 1 (2020): 141–204.
Gendera, Sandra, Paula Jops, Timothy Broady, Kylie Valentine and Jan Breckenridge. *Evaluation of the Technology Trial (Keeping Women Safe in Their Homes)*. Sydney, NSW: Social Policy Research Centre UNSW, 2019.
Goldfarb, Sally F. "Violence against Women and the Persistence of Privacy." *Ohio State Law Journal* 61, no 1 (2000): 1–88.
Gordon, Sue, Kay Hallahan and Darrell Henry. *Putting the Picture Together: Inquiry into Response by Government Agencies to Complaints of Family Violence and Child Abuse in Aboriginal Communities*. Perth, WA: State Law Publisher, 2002.
Gotell, Lise. "When Privacy is Not Enough: Sexual Assault Complainants, Sexual History Evidence and the Disclosure of Personal Records Special Issue: Privacy Law." *Alberta Law Review* 43, no 3 (2006): 743–778.
Harris, Bridget. "Spacelessness, Spatiality and Intimate Partner Violence: Technology-Facilitated Abuse, Stalking and Justice." In *Intimate Partner Violence, Risk and Security: Securing Women's Lives in a Global World* (Routledge Studies in Crime, Security and Justice), edited by J. Maher, S. Walklate, J. McCulloch and K. Fitz-Gibbon, 52–70. United Kingdom: Routledge, 2018.
Harris, Bridget A. and Delanie Woodlock. "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies." *The British Journal of Criminology* 59, no 3 (9 April 2019): 530–550. https://doi.org/10.1093/bjc/azy052.
Harris, Bridget. "Technology, Domestic and Family Violence: Perpetration, Experiences and Responses." *QUT Centre for Justice*, no. 4 (April 2020): 5.

Henry, Nicola and Anastasia Powell. "Beyond the Sext: Technology-Facilitated Sexual Violence and Harassment against Adult Women." *Australian and New Zealand Journal of Criminology* 48, no 1 (2015): 104–118.

——— "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research." *Trauma, Violence, & Abuse* 19, no 2 (1 April 2018): 195–208. https://doi.org/10.1177/1524838016650189

Jones, Meg Leta. "Privacy Without Screens & the Internet of Other People's Things." *Idaho Law Review* 51, no 3 (2015): 639–660.

Kelly, Kristin Anne. *Domestic Violence and the Politics of Privacy*. New York, NY: Cornell University Press, 2003.

Kilgore, Olivia. "Your Head is in the Cloud: The Application of Outdated Privacy Law to Rapidly Changing Technologies." *Drake Law Review Discourse* 67 (2018): 101–122.

Koops, Bert-Jaap, Bryce Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski and Maša Galič. "A Typology of Privacy." *University of Pennsylvania Journal of International Law* 38, no 2 (2017): 483–575. https://doi.org/10.1177%2F0004865814524218

Langton, Marcia, Kristen Smith, Tahlia Eastman, Lily O'Neill, Emily Cheesman and Meribah Rose. *Improving Family Violence Legal and Support Services for Aboriginal and Torres Strait Islander Women*. Sydney, NSW: ANROWS, 2020.

Law Commission Te Aka Matua O Te Ture. "Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3." January 2010. https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R113.pdf

Levy, Karen E. C. "Intimate Surveillance." *Idaho Law Review* 51, no 3 (2015): 679–694.

Logar, Rosa and Johanna Niemi. *Emergency Barring Orders in Situations of Domestic Violence: Article 52 of the Istanbul Convention*. Strasbourg, France: Council of Europe, 2017

Massey, Aaron. "Getting to October: Why Understanding Technology Is Essential for Privacy Law." *Idaho Law Review* 51, no 3 (2015): 695–710.

Mele, Christopher. "Data Breaches Keep Happening. So Why Don't You Do Something?" *The New York Times*, 1 August 2018, sec. Technology. https://www.nytimes.com/2018/08/01/technology/data-breaches.html

Moore, Adam D. *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Penn State University Press, 2010.

Nancarrow, Heather and Tanya Modini. *Electronic Monitoring in the Context of Domestic and Family Violence: Report for the Queensland Department of Justice and Attorney-General*. Sydney, NSW: ANROWS, 2018.

Naughton, Liam and Herbert Daly. "Augmented Humanity: Data, Privacy and Security." In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, edited by Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran and Jaime Ibarra, 73–93. Advanced Sciences and Technologies for Security Applications. Cham, Switzerland: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-35746-7_5

Netsafe. "Netsafe Quarterly Report April–June 2020." 2020. https://www.netsafe.org.nz/the-kit/fy20q4/

New Zealand Government. *Pasefika Proud: Pathways for Change 2019–2023*. Wellington, New Zealand: New Zealand Government, 2019.

New Zealand Government. *Family Violence Risk Assessment and Management Framework: A Common Approach to Screening, Assessing and Managing Risk*. Wellington, New Zealand: New Zealand Government, 2017.

New Zealand Government. *Family Violence, Sexual Violence and Violence within Whānau: Workforce Capability Framework*. Wellington, New Zealand: New Zealand Government, 2017.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2009.

Northern Territory Government. *Domestic, Family and Sexual Violence Reduction Framework 2018–2028*. Darwin, NT: Northern Territory Government, 2018.

Office of the Australian Information Consumer (OAIC), *Chapter C: Permitted General Situations*. Sydney, NSW: OAIC, 2019.

Pacheco, Edgar, Neil Melhuish and Jandy Fiske. *Image-based Sexual Abuse: A Snapshot of New Zealand Adults' Experiences*. Wellington, New Zealand: Netsafe, 2019.

Parton, Chloe. *Attitudes Towards Violence Against Women and Gender Equality Among People in NSW: Summary of Findings from the 2017 National Community Attitudes Towards Violence Against Women Survey (NCAS)*. Sydney, NSW: ANROWS, 2019.

Patton, Michael. *Qualitative Research and Evaluation Methods*. Thousand Oaks, CA: SAGE Publications, 2002.

Peppet, Scott R. "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent." *Texas Law Review* 93, no 1 (2015): 85–178.

Powell, Anastasia, Nicole Henry, Asher Flynn and Adrian Scott. "Image-based Sexual Abuse: The Extent, Nature and Predictors of Perpetration in a Community Sample of Australian Residents." *Computers in Human Behaviour* 92 (2019): 393–402. https://doi.org/10.1016/j.chb.2018.11.009

Powell, A. and N. Henry. "Technology-Facilitated Sexual Violence Victimization Results from an Online Survey of Australian Adults." *Journal of Interpersonal Violence* 34, no 17 (2019): 3637–3665. https://doi.org/10.1177%2F0886260516672055

Privacy International. "What is Privacy?" 2017. http://privacyinternational.org/explainer/56/what-privacy
Richards, Neil M. "The Dangers of Surveillance Symposium: Privacy and Technology." *Harvard Law Review* 126, no 7 (2013): 1934–1965.
Robertson, Boni. *The Aboriginal and Torres Strait Islander Women's Taskforce on Violence Report*. Brisbane, QLD: Queensland Government, 1999.
Safetynet. "Covid-19 QR Code Scanners—Advice for Survivors." *TechSafety* (blog). Accessed 31 August 2021. https://techsafety.org.au/resources/resources-women/covid-19-qr-code-scanners-advice-for-survivors/
Schneider, Elizabeth M. "The Violence of Privacy." *Connecticut Law Review* 23, no 4 (1991): 973–1000.
Selvadurai, Niloufer. "Protecting Online Information Privacy in a Converged Digital Environment—The Merits of the New Australian Privacy Principles." *Information & Communications Technology Law* 22, no 3 (2013): 299–314. https://doi.org/10.1080/13600834.2013.856125
Sentencing Advisory Council. *Sentencing Image-Based Sexual Abuse Offences in Victoria*. Melbourne, VIC: Sentencing Advisory Council, 2020.
Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154, no 3 (2006): 477–564. https://doi.org/10.2307/40041279
———. "Introduction: Privacy Self-Management and the Consent Dilemma Symposium: Privacy and Technology." *Harvard Law Review* 126, no 7 (2013): 1880–1903.
———. "The Myth of the Privacy Paradox." *George Washington Law Review* 89, no 1 (2021): 1–51.
———. *Understanding Privacy*. Michigan: Harvard University Press, 2008.
Stark, Evan. *Coercive Control: How Men Entrap Women in Personal Life*. New York, NY: Oxford University Press, 2007.
Suk, Jeannie. *At Home in the Law: How the Domestic Violence Revolution is Transforming Privacy*. Michigan: Yale University Press, 2009.
Valentine, Kylie and Jan Breckenridge. "Responses to Family and Domestic Violence: Supporting Women?" *Griffith Law Review* 25, no 1 (2016): 30–44.
Victoria State Government. *Ending Family Violence: Victoria's Plan for Change*. Melbourne, VIC: Victoria State Government, 2016.
Warren, Samuel D. and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no 5 (1890): 193–220. https://doi.org/10.2307/1321160
WESNET. "Women's Legal Guides on Tech-based Abuse." Accessed 27 May 2021. https://techsafety.org.au/resources/legal-guides/
Westin, Alan Furman. *Privacy and Freedom*. London, England: The Bodley Head, 1967.
Wild, Rex and Patricia Anderson. *Ampe Akelyernemane Meke Mekarle 'Little Children are Sacred': Report of the Northern Territory Board of Inquiry into the Protection of Aboriginal Children from Sexual Abuse*. Darwin, NT: Northern Territory Government, 2007.
Woodlock, Delanie, Karen Bentley, Darcee Schulze, Natasha Mahoney, Donna Chung and Amy Pracilio. *Second National Survey of Technology Abuse and Domestic Violence in Australia*. Canberra, ACT: WESNET, 2020.
Woodlock, Delanie, Mandy McKenzie, Deborah Western and Bridget Harris. "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control." *Australian Social Work* 73, no 3 (2 July 2020): 368–380. https://doi.org/10.1080/0312407X.2019.1607510

Primary Materials

Legislation

Australia

Charter of Human Rights and Responsibilities Act 2006 (Vic)
Crimes (Domestic and Personal Violence) Act 2007 (NSW)
Criminal Code Act 1995 (Cth)
Domestic and Family Violence Act 2007 (NT)
Domestic and Family Violence Protection Act 2012 (Qld)
Domestic Violence Agencies Act 1986 (ACT)
Enhancing Online Safety Act 2015 (Cth)
Family Violence Act 2004 (Tas)
Family Violence Protection Act 2008 (Vic)
Human Rights Act 2004 (ACT)
Human Rights Act 2019 (Qld)

Intervention Orders (Prevention of Abuse) Act 2009 (SA)
Invasion of Privacy Act 1971 (Qld)
Listening Devices Act 1991 (Tas)
Listening Devices Act 1992 (ACT)
Online Safety Act 2021 (Cth)
Privacy Act 1988 (Cth)
Privacy Code of Practice (General) 2003
Telecommunications (Interception and Access) Act 1979 (Cth)
Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
Restraining Orders Act 1997 (WA)
Surveillance Devices Act 1998 (WA)
Surveillance Devices Act 1999 (Vic)
Surveillance Devices Act 2007 (NSW)
Surveillance Devices Act 2016 (SA)

New Zealand
Bill of Rights Act 1990 (NZ)
Crimes Act 1961 (NZ)
Family Violence Act 2018 (NZ)
Harmful Digital Communications Act 2015 (NZ)
Privacy Act 2020 (NZ)
Telecommunications Industry Privacy Code 2020

European Union
General Data Protection Regulation 2018

Case Law

Australia
Complainant B v Statutory Entity [2003] VPrivCmr 2
'ST' and Chief Executive Officer of Services Australia (Privacy) [2020] AICmr 30
WZ and CEO of Services Australia (Privacy) [2021] AICmr 12

New Zealand
Case Note Annual Report 2001/02 (settlement) [2002] NZPrivCmr 15
Case Note Annual Report 2004/05 (disclosure) [2005] NZPrivCmr 7
Case Note 300915 [2020] NZPrivCmr 2
Hosking v Runting [2004] NZCA 34