Queensland University of Technology

accan
Australian Communications Consumer Action Network

Domestic violence and communication technology

Survivor experiences of intrusion, surveillance, and identity crime

Molly Dragiewicz, Bridget Harris, Delanie Woodlock, Michael Salter, Helen Easton, Angela Lynch, Helen Campbell, Jhan Leach, Lulu Milne

11 July 2019

Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime

Authored by Molly Dragiewicz, Bridget Harris, Delanie Woodlock, Michael Salter, Helen Easton, Angela Lynch, Helen Campbell, Jhan Leach, Lulu Milne

Published in 2019

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.

Queensland University of Technology
Website: https://www.qut.edu.au/
Email: m.dragiewicz@griffith.edu.au
Telephone: +61 7 3138 4000

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au.

ISBN: 978-1-921974-59-5
Cover image: Anthony Rees 2019

This work can be cited as: 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, Australian Communications Consumer Action Network, Sydney.

This research was made possible by a grant from ACCAN and supported by previous work undertaken by Dragiewicz and Harris at QUT. The authors note our commitment to academic freedom and research integrity. No third party exerted any influence over the research design or analysis.

Contents

Acknowledgements

The authors would like to express our deep appreciation to the survivors who participated in the interviews in Queensland and New South Wales. Sharing your knowledge allows telecommunications companies, platforms, services, justice systems, government, and academics to better understand the nature and dynamics of domestic violence. This information can contribute to improved policy and practice for intervention and prevention. Although the experiences you described are difficult to hear, we are always inspired by the wisdom, strength, resiliency, and humour of the survivors we have the privilege of interviewing.

We also thank the specialised domestic violence services and staff who participated in the online focus groups. Your insight gleaned from years of work with survivors and communities has greatly informed this study. Special thanks are due to our community partners, Women's Legal Service Queensland, Women's Legal Service New South Wales, and Blacktown Women and Girls Health Centre. Your assistance with recruitment helped to ensure that we identified participants safely and in the context of support for services and referrals. We would also like to thank our universities. Support from Queensland University of Technology has been invaluable, especially that provided by Maxine Brown, Gail Fellows, and Vanessa Stott. Western Sydney University and The University of New South Wales have also assisted with research administration. Thanks to Tanya Karliychuk, Narelle Clark, and Kit Catterson for guidance throughout the project. We would like to express our appreciation to the Australian Communications Consumer Action Network which made this study possible via their research grants scheme.

Executive Summary

Domestic violence has significant social and economic costs each year in Australia. Information and communications technologies (ICTs) play an increasingly important role in this abuse. ICT security and privacy are essential to domestic violence victims, but are often compromised.

Digital technologies play an increasingly important role in everyday life. The ubiquity of these technologies, combined with factors like with GPS tracking, cloud-based storage, and platform integration, present significant challenges to personal security and privacy. This is particularly true for domestic violence survivors. The control and fear that characterise experiences of domestic violence have an expanding technological dimension as perpetrators weave technology into patterns of abuse. ICTs offer domestic violence survivors vital opportunities for communication, help-seeking and support. Domestic violence victims are a uniquely vulnerable population of consumers who face risks including loss of access to and control of their telecommunications accounts, privacy rights, personal security, and physical safety when technology is abused.

This study extends the emerging research on technology-facilitated coercive control (TFCC) to gather deeply contextualised qualitative evidence from survivors. We conducted interviews with domestic violence survivors in Queensland and New South Wales who had experienced technology-facilitated abuse, supplementing the interviews via focus groups with practitioners who work with domestic violence survivors in rural, regional, and remote areas in Queensland and New South Wales. The data provided by this study comprise a preliminary evidence base to guide future research, policy, and practice in an area of growing concern.

This study documented Australian domestic violence survivors' experiences of technology-facilitated abuse; discovered what resources and tactics survivors and practitioners use to deal with technology-facilitated coercive control; and compiled survivor and practitioner recommendations about how to improve responses to this form of abuse. The findings allow us to better understand technology use in the context of domestic violence, the resources currently available, and how to improve responses to this type of abuse.

Our findings indicate that domestic violence creates an intimate threat model requiring innovative cybersecurity responses. This exploratory study elicited four key recommendations for future policy and practice.

More training and education about technology-facilitated coercive control and tools to combat it

- Increase recognition of TFCC as a serious part of domestic violence.
- Mandate workplace training about TFCC for telecommunication companies, police, and courts
- Provide required courses on domestic violence with content on TFCC in university programs such as psychology, criminology, social work, and law
- More in-person training for workers who come into contact with domestic violence
- Empowering consumer decision making by providing directly comparable information about resources for domestic violence survivors, 1300 call charges, and policies for charging for phones destroyed in a crime
- Improved consumer safeguards to protect privacy and facilitate release from contracts and family plans when domestic violence is an issue

Enhanced affordability of telecommunication devices and service for domestic violence survivors

- Eliminate charges for changing and un-listing phone numbers due to TFCC
- Release survivors from charges for phones that abusers have taken or destroyed
- Offer financial hardship plans for domestic violence survivors unable to pay for phone contracts and plans
- Recognising and responding to the digital divide

Expansion of existing resources

- The Women's Services Network (WESNET) and Telstra SafeConnections program: making phones and credit available for survivors
- More in-person training, including in rural, regional, and remote areas, updated and repeated periodically
- Hands-on security checks for domestic violence services and survivors

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 movements 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 action taken in response to complaints and establishing an appeal process

Introduction

This report advances ongoing conversations about technology and abuse in Australia.

The discussion so far has largely been centred on kids and "sexting," (Kids Helpline 2017; Salter, Crofts & Lee, 2013); image-based sexual abuse (Hayes & Dragiewicz, 2018; Powell, Henry, & Flynn, 2018); harassment and abuse of women online (Filipovic, 2007; The Futures Company, 2017; Salter 2018), and legal responses (Australian Law Reform Commission, 2014; Henry, Flynn & Powell, 2018). This report is the first publication based on an ACCAN funded study of the misuse of technology in domestic violence[1] in Australia and survivor and practitioner recommendations for improving responses to this abuse. We conducted interviews with domestic violence survivors in Queensland and New South Wales who had experienced technology-facilitated abuse. We supplemented the interviews via focus groups with staff from organisations that work with domestic violence survivors in rural, regional, and remote areas in Queensland and New South Wales, in order to learn about the resources and training they know about and identify the challenges they face responding to TFCC. The data provided by this study provide a preliminary evidence base to guide future research, policy, and practice in an area of growing concern. The findings allow us to better understand technology use in the context of domestic violence, the resources currently available, and how to improve responses to this type of abuse.

This study had three primary objectives

1 **Document Australian domestic violence survivor experiences of technology-facilitated abuse;**

2 **Discover what resources and tactics survivors and practitioners use to deal with technology-facilitated coercive control;**

3 **Compile survivor and practitioner recommendations about how to improve responses to this form of abuse.**

Although the study questions were focused on help seeking and responses by information and communication technology companies, most participants also spoke about police and court responses to technology-facilitated abuse. We will discuss those findings in greater detail in future publications.

1 In some Australian jurisdictions, the term domestic and family violence is used as an alternative, but we have not used it here as this term incorporates violence enacted by family members other than partners. Where other terms have been used in this report, it is in reference to research which has adopted another term but retained a focus on intimate partners.

Key terms

We acknowledge that a variety of terms are used to identify domestic violence depending on the focus of the discussion. Each term has its own benefits and drawbacks (see Dragiewicz et al., 2018, p. 610). For the purposes of this study, we use the term domestic violence due to its widespread recognition beyond academia in anti-violence practice and in the community. Domestic violence is a pattern of violent, coercive, or controlling behaviour perpetrated by one current or former intimate partner against another. Domestic violence encompasses multiple forms of manipulation and abuse, often backed up by actual or threatened physical or sexual violence. Domestic violence frequently continues following separation and divorce. It may include dating couples who do not live together as well as those in cohabiting relationships. Domestic violence often extends outside the home to affect survivors' social and professional networks and interactions with systems (Sharp-Jeffs, Kelly, & Klein, 2018). The dynamics, distribution, and outcomes of this abuse are shaped by structural inequalities such as sexism, racism, xenophobia, and homophobia (DeKeseredy, Dragiewicz, & Schwartz, 2017; Stark & Hester, 2019). Scholars and practitioners recommend the adoption of a broad definition of domestic violence, incorporating sexual, verbal, financial, and psychological abuse as well as the more commonly recognized physical forms of violence. This is because the dynamics of domestic violence include multiple abusive tactics concurrently and over time.

This study is focused on the form of domestic violence we refer to as technology-facilitated coercive control (TFCC). TFCC is violence and abuse by current or former intimate partners, facilitated by information and communication technologies (ICTs) or digital media,[2] acknowledging technological aspects of abuse in the context of coercive and controlling intimate relationships (Dragiewicz et al., 2018; Harris 2018; Harris & Woodlock, 2018). TFCC includes behaviours such as monitoring via social media, stalking using GPS, video and audio recording, making threats via email, phone or other technological medium, surveillance of partners' email, accessing accounts without permission, impersonation, and publishing private information or images without consent (Dragiewicz et al., 2018; Harris & Woodlock, 2018; Southworth, Finn, Dawson, Fraser, & Tucker, 2007; Woodlock, 2017). These behaviours may be overt or clandestine. Unauthorised access may be achieved using force, coercion, deception, or stealth. TFCC affects survivors' mental health and causes or contributes to trauma, manifesting in psychological and physical symptoms.

Domestic violence survivors comprise a large group of vulnerable telecommunications consumers whose rights, privacy, and security are compromised when telecommunication services and Internet connected devices are misused (Chatterjee et al., 2018; Douglas, Harris, & Dragiewicz, 2019; Dragiewicz et al., 2018; Dragiewicz, Woodlock, Harris, & Reid, 2019; Freed et al., 2017, 2018; Harris & Woodlock, 2018; Suzor et al., 2019; Woodlock, 2017). Access to safe and secure information and communication technologies are essential for survivors' civic and social engagement, access to information, and help-seeking (Dimond, Fiesler, & Bruckman, 2011; Hand, Chung, & Peters, 2009; Harris, 2018).

Cybersecurity is most often understood to refer to corporate rather than personal security in the use and application of ICTs (Wall, 2013). However, at a time when mass technological platforms and devices gather tremendous amounts of personal data about individuals, the specific dynamics of domestic violence present a unique yet prevalent type of threat to personal cybersecurity. Goode's analysis of identity theft cases reported to IDCARE in Australia in 2016 found that 20% of 268 incidents where victims identified the perpetrator involved an ex-partner, partner, or associate of an ex-partner (2017, p. 29). However little is known in Australia about the dynamics and impact of TFCC or the challenges involved in responding to it.

This study fills this gap in knowledge, identifying directions for future research, practice, and policy to improve outcomes for those experiencing domestic violence. Although this study focused on the particular dynamics of TFCC against women, our findings can be used to inform future studies designed to empirically document the characteristics of abuse in other contexts. Addressing survivors' concerns can potentially benefit

2 Information and communications technologies include the "devices, networking components, applications and systems that combined allow people and organizations (i.e., businesses, nonprofit agencies, governments and criminal enterprises) to interact in the digital world" (Pratt, 2005).

all consumers by drawing attention to a widespread intimate threat model that receives little attention from cybersecurity bodies, police, or the courts. This project extends the emerging research on technology-facilitated domestic violence into areas that have yet to be investigated in Australia or elsewhere in the world.

This study moves beyond efforts to create typologies of technology-facilitated abuse and document its prevalence to investigate the ways that intrusion, surveillance, and identity crime affect the privacy and security of domestic violence survivors, ultimately abrogating their rights. Advocates and survivors report that the abuse of technology is a common part of survivors' overall experience of domestic violence, with profound and lasting implications. Our findings indicate that current responses to these threats are inadequate, exacerbating risks to a vulnerable population. They also point to gaps in cybersecurity design and policy more generally.

This report is structured as follows. In the first section, we define key terms used in this report and present basic facts about domestic violence as a social problem. Then, we discuss the growing role of digital technologies in everyday life. Next, we review the small body of research on technology-facilitated domestic violence in Australia. In the second section, we present the research methods used in this study, discuss study limitations, and provide information about the participants. In the third section, we present our key findings. This section outlines essential contexts for understanding the dynamics of technology-facilitated abuse and discusses the abuse reported by the survivors and domestic violence workers. This section also includes information about the impact of technology-facilitated abuse on survivors. Next, we discuss survivors' efforts to get help dealing with the abuse and their outcomes. After that, we present recommendations from survivors and service-providers about what would be useful to manage and respond to technology-facilitated abuse. Finally, the conclusion reviews key findings of our study and makes recommendations for future research, policy, and practice to strengthen responses to technology-facilitated abuse.

Context

Domestic violence is one of Australia's most pressing social problems, with extensive economic and human costs. The financial cost of violence against women and children in Australia from 2015–2016 was estimated at $22 billion (Australian Institute of Health and Welfare, 2018, p. xi).[3] Intimate partner violence against women cost an estimated $12.6 billion from 2014-2015 in Australia (Pricewaterhouse Coopers, OurWatch & Vichealth, 2015, p. 11). Domestic violence crimes comprise one of the largest categories of police activity. According to the Royal Commission into Family Violence report, approximately 40 to 60 percent of front-line policing activities are related to family violence (Royal Commission into Family Violence, 2016, p. 56).

Domestic violence is highly gendered, meaning it disproportionately harms women due to persistent and pervasive gender norms and structural inequality between women and men (Dragiewicz, 2009; World Health Organization, 2009). For this reason, this report is focused on domestic violence against women. The gendered nature of domestic violence is starkly illustrated by the distribution of domestic homicide. Of the 487 homicide incidents in Australia from 1 July 2012 to 30 June 2014, 26 percent were committed by current or former intimate partners (Bryant & Bricknell, 2017, p.1). Seventy-nine percent of the victims in these incidents were female (Bryant & Bricknell, 2017, p. 37).[4] Abusive and obsessive contact and stalking via technology have been identified as emerging trends across intimate partner homicide and filicide cases (Domestic and Family Violence Death Review and Advisory Board, 2017; Dwyer & Miller, 2014).

3 However, the true cost is likely to be up to $4 billion higher as certain groups such as Aboriginal and Torres Strait Islander women, pregnant women, women with a disability, and women experiencing homelessness are underrepresented in this calculation (Australian Institute of Health and Welfare, 2018, p. xi).

4 Deaths in these incidents also include male and female children, deaths of the primary targets' new intimate partners, and other collateral killings. These deaths can make sex differences in the distribution of intimate partner homicides look smaller than they actually are.

Technology in Everyday Life

ICTs play an enormous role in our everyday lives. Technological changes associated with ubiquitous mobile devices, increased Internet access and speed, cloud-based storage, GPS technology, platform convergence, consolidation of media ownership, and the Internet of Things have major social, cultural, and economic implications (Baym, 2015). Access to the Internet and digital media are no longer luxuries. Access to and use of ICTs have been described as critical infrastructure concerns and even human rights issues due to the importance of ICTs in contemporary life (Suzor et al., 2018). However, the pace and extent of technological development has persistently outstripped legislation and regulatory frameworks that aim to diminish criminal harm and promote public safety. The Internet has been compared to a virtual "wild west" or digital frontier in which consumers interact in a semi-lawless environment in the absence of effective policing by government agencies or administration by technology industries (Phillips, 2015).

The Internet and smartphones play a growing role in intimate relationships. While most Internet users (74 percent) report that technology has a positive effect on their relationships, 24 percent report the impact is mixed or mostly negative (Lenhart, Duggan & Smith, 2014, p. 15), and this segment is growing. The intimate relationship context creates unique technological security and privacy risks. A Pew study in the United States found that 67 percent of Internet users in a marriage or committed relationship reported they had shared the password to one or more of their online accounts with their partner (Lenhart, Duggan & Smith, 2014). In addition, 27 percent shared an email account, 11 percent shared an online calendar, and 11 percent shared a social media profile. Older couples were more likely to share an email account (Lenhart, Duggan & Smith, 2014, p. 7), and parents were more likely to share account passwords (71 percent) (Lenhart, Duggan & Smith, 2014, p. 10). It is important to note that identical technologies and behaviours can be innocuous or positive in a healthy relationship and toxic or dangerous in the context of abuse.

The intimate threat model includes:

- risks created by intentional sharing;
- intimate knowledge that can facilitate guessing of passwords or answering security questions; and
- physical access to passwords, networks, and devices.

Technology-facilitated abuse poses real threats to the privacy, dignity, and freedom of targets of abuse and can constrain their ability to participate in everyday life (Citron, 2014). As discussed below, many of the survivors in this study had partners who provided and set up their technology before they knew their partner was abusive. The reach, storage capacity, and replicability of digital media (Baym, 2015) create a context where the text and images used by abusers can remain visible to a broad audience and may be connected to the victim's identity in ways that affect their personal and professional lives over the long term. The same technologies that we enjoy everyday for their convenience and capabilities can create serious vulnerabilities when they are misused (Dragiewicz et al., 2018; Ybarra, Price-Feeney, Lenhart, & Zickuhr, 2017).

Research on Technology and Domestic Violence

ICTs are now a prominent feature in the abuse and control strategies of domestic violence perpetrators (Dragiewicz et al., 2018; Lopez-Neira, Patel, Parkin, Danezis, & Tanczer, 2019; Suzor et al., 2019). The Council of Australian Governments Summit on Reducing Violence against Women and their Children (COAG, 2016) and Australia's Third Action Plan to Reduce Violence Against Women and Their Children (Australian Government & Department of Social Services, 2016) identify technology-facilitated abuse as a growing concern in need of evidence to guide practice. ICT security and privacy are essential to domestic violence survivors, yet they are often compromised. Kelly (1988) argued that different types of violence and abuse can be conceptualised on a continuum, from those widely recognised as criminal to those that are so common they are normalised. Exposure to abuse across contexts, from home to work and leisure activities, can contribute to what survivors experience as "spaceless violence" (Harris, 2018) or "climates of unsafety" (Stanko, 1990). The continuum of unsafety is an apt characterisation of TFCC. As ICTs are incorporated into mundane tasks and everyday activities, abusers have taken advantage of the opportunities to extend and intensify coercive, controlling, and abusive behaviours across time and space in ways that were not previously possible (George and Harris, 2014; Woodlock, 2017).

To date, research on technology-facilitated abuse is mostly focused on the United States. These studies have mostly relied on convenience samples of university students (Reed, Tolman & Ward, 2016). They frequently conflate aggression and abuse, rendering findings of limited use for understanding domestic violence or coercive control (for a discussion of measures, see Brown and Hegarty, 2018). One nationally representative survey of 2,810 Americans 15 and older who had ever been in an intimate relationship found that "12% of respondents who have ever been in a romantic relationship have experienced intimate partner digital abuse" (Ybarra et al., 2017, p. 3). Ybarra et al. found that those who were targeted by romantic partners were more likely to take action in response to abuse than those who were targeted by other perpetrators online, with 77 percent of victims of intimate partner digital abuse using at least one protective strategy.

Key findings about actions taken in response to intimate partner digital abuse include:

- Forty-one percent had changed their email address or phone number.
- Thirty-four percent had reported or flagged content that was posted without their permission.
- Twenty-five percent had created a new social media profile.
- Twenty-five percent had stopped using social media.
- Sixteen percent had gotten a restraining order or protection order.
- Sixteen percent had stopped going online.
- Nine percent had gotten help from a domestic violence center, hotline, or website (Ybarra et al., 2017, p. 23).

While these findings are not disaggregated by sex or sexuality, Ybarra et al. (2017, p.24) report that three times more women than men got a restraining order.

Our knowledge of technology-facilitated domestic violence in Australia is primarily derived from anecdotal information from practitioners and incidental findings from studies on other issues. Australian scholars have studied image-based sexual abuse, using surveys to produce prevalence estimates for a broad array of online behaviours (e.g. Henry, Powell & Flynn 2017). However, these emerging studies provide little information about the context in which acts take place and aggregate a range of dissimilar behaviours. As a result, their applicability to domestic violence is unclear.

The studies designed to investigate technology-facilitated domestic violence in Australia so far have mostly relied on surveys of professional and practitioner respondents (e.g. Woodlock, 2017). Preliminary studies on TFCC indicate that it has profound implications for survivor security and well-being (Dragiewicz et al., 2019; Harris, 2016; Woodlock, 2017). In Australia, two studies conducted by community organisations found that the use of technology by perpetrators of domestic violence is an emerging issue for both practitioners and survivors (Woodlock, 2017; Woodlock, McKenzie, Western & Harris, 2019). In 2014, Victoria Legal Aid funded the Domestic Violence Resource Centre Victoria (DVRCV) to conduct a scoping study in Victoria on the ways that perpetrators were using technology and how the law was responding to this abuse. One hundred and fifty-two practitioners and 52 survivors in Victoria completed the survey (Woodlock, 2017). The findings showed that practitioners felt that technology was being used by perpetrators as part of their abuse tactics, creating a sense for victims that the perpetrator was omnipresent. Survivors described the abuse they had experienced via technology, with many sharing that the relentlessness of the abuse had an impact on their mental health and well-being. Both survivors and practitioners felt that the use of technology by perpetrators was not taken seriously as a form of domestic violence by police or the legal system (Woodlock, 2013).

DVRCV, along with Women's Legal Service New South Wales and The Women's Services Network (WESNET), conducted a national survey in 2015, building on the previous research in Victoria. This study, funded by ACCAN, surveyed 546 domestic violence practitioners about their perceptions of how perpetrators use technology and the effects of this abuse on women and children. The findings showed that the most commonly used technology to abuse was text messaging, as well as social media such as Facebook (Woodlock, McKenzie, Western & Harris, 2019). Practitioners reported that they observed women being impersonated by perpetrators, such as sending emails from women's accounts, with 41 percent seeing this "sometimes" and 21 percent observing it "often" (Woodlock, 2015). Practitioners reported that survivors were frequently given simplistic and unhelpful advice to turn off or withdraw from technology and blamed for the abuse if they did not comply (Woodlock, McKenzie, Western & Harris, 2019).

To date, there has been scant investigation of the ways domestic violence perpetrators use technology to interfere in survivors' lives via intrusion, surveillance, and identity crime (The Futures Company, 2014; Harris & Woodlock, 2018; Kim, 2015; Littwin, 2012). Littwin (2012) observed abusers acquiring debt under victims' names, such as by using credit cards obtained without the victim's knowledge. Kim argues that "[r]esearch has only recently begun to fully comprehend the consumer and credit dimensions of domestic violence" (2015, p. 283). In their study of domestic violence in rural, regional, and remote areas, George and Harris (2014) documented abusers logging into survivor accounts and changing information such as authorised user names and passwords. Women in their sample reported extensive challenges when seeking assistance from telcos and institutions. Women also reported receiving phone calls from persons impersonating police officers who "attempted to intimidate women and dissuade them from pursuing formal responses to family violence" (George and Harris, 2014, p. 157-158). Ultimately, women in these cases experienced additional trauma and invested considerable time and effort to regain control of their devices and accounts, but were usually unable to achieve satisfactory resolution of these issues. This study builds on these foundational efforts to expand the evidence base on women's experiences of TFCC.

Methodology

This exploratory study used qualitative methods to gather deeply contextualized, rich data directly from survivors of technology-facilitated coercive control. The study also collected qualitative data from domestic violence practitioners who work in rural, regional, and remote areas in order to learn about the challenges involved in responding to this abuse.

We used a convenience sampling approach in both arms of the study. Data collection occurred during late 2018 and early 2019. Because most of the extant Australian data on TFCC is quantitative, we used a combination of semi-structured interviews and focus groups to gather new information. Both parts of the study had ethical approval via QUT's Office of Research Ethics and Integrity. A secondary External Ethics Approval was granted by Western Sydney University.[5] Throughout this report, pseudonyms are used to identify the survivor participants. Service provider feedback was aggregated because of the potential identifiability of individual services in rural, regional, and remote areas of Queensland and New South Wales and concerns about working relationships with local police and other organisations.

The research team conducted interviews with twenty participants who are survivors of technology-facilitated abuse, ten in Queensland and ten in New South Wales. We asked survivors about:

- Demographics;
- experiences of technology-facilitated abuse;
- help-seeking strategies;
- recommendations for improving responses to technology-facilitated coercive control; and
- perspectives on participating in the research.

We recruited our survivor participants with the assistance of local women's legal support programs and health services which have well-established relationships and long histories working with domestic violence survivors. We elected to conduct recruitment via service intermediaries because of the risks to participants inherent in online and telephone communication with survivors of domestic violence who have experienced TFCC. The specialised services were an essential component of this study. They were able to identify potential participants and reach out to them, sharing the study recruitment documents and explaining about the study. They also provided tremendous assistance by scheduling the interviews and providing space in which to conduct them. The practitioners were experienced at working with domestic violence, using established, survivor-centred organisational practices to assess whether contact was safe and the survivor participants felt comfortable participating in an interview. The interviews were conducted on-site at the specialist service offices or on the phone for a few women for whom a telephone interview was more convenient. All interviews were recorded for later transcription and coding. Survivor participants received a $50 gift card from a major supermarket chain as a token of appreciation for their time and to help offset the costs of time spent on the interview. One woman, Jade, was abused by a sibling rather than an intimate partner.[6] Since that abuse had different dynamics to the coercive and controlling partner abuse we set out to study but involved some of the same technological issues, we include examples from her experience below.

5 QUT Ethics Approval numbers 1900000218 and 1800000562. Western Sydney University External Ethics Approval Recognition number H12987.
6 This interview was with the one participant in the study who identified as Aboriginal. The family and domestic violence described in her interview highlights the need for additional research led by Indigenous scholars and advocates and family violence scholars on the complex dynamics of abuse across sibling and other family relationships.

In addition to the interviews, we conducted three online focus groups with ten rural, regional, and remote service providers who work with domestic violence survivors.

Practitioners were asked about:

- types of intrusion, identity theft or surveillance they hear about most often in their work,
- common platforms for abuse;efforts to seek assistance from telcos or platforms;challenges of responding to technology-facilitated coercive control;resources they use; and
- what would be helpful for assisting survivors who are experiencing these types of abuse.

We conducted these focus groups online using the conferencing software Zoom to ensure that staff from rural, regional, and remote areas could easily participate and we could record the focus groups for transcription. It was important to gather perspectives from rural, regional, and remote domestic violence service providers because of the concentration of domestic violence services in a handful of cities and regions in Australia and the fact that our interviews were held in cities. Prior research on domestic violence has identified unique issues for survivors in rural, regional and remote areas, such as women's increased reliance on ICTs for information and support and black spots where mobile service is unavailable (George and Harris, 2014; Harris 2016). Speaking to service providers allowed us to gather information about rural, regional, and remote challenges and gain a different perspective from the survivors. The practitioners provided excellent information about TFCC resources and training and other needs, as well as reinforcing many of the points survivors made.

Participant Profile

We interviewed twenty survivors for this study. Nineteen of them were abused by current or former intimate partners. Ten of the women were in Queensland and ten were in New South Wales. Participants ranged from 21 to 65, with an average age of 39. Half of the women were in their forties, five were in their thirties, three were in their twenties, and one was 65. When asked about their backgrounds, half of the women identified as Australian (9) or Aboriginal (1) and half identified as from overseas, including Canada, China (2 women), India (2 women), Italy, Japan, New Zealand, Northern Ireland, and South Africa.

In addition, we held three online focus groups with domestic violence service provider staff working in rural, regional and remote Queensland and New South Wales. The domestic violence workers were from refuges, other specialised domestic violence services, women's health services and women's legal services. Despite the small number of participants in the focus groups, we quickly reached saturation, with practitioners reporting very similar issues and experiences across locations.

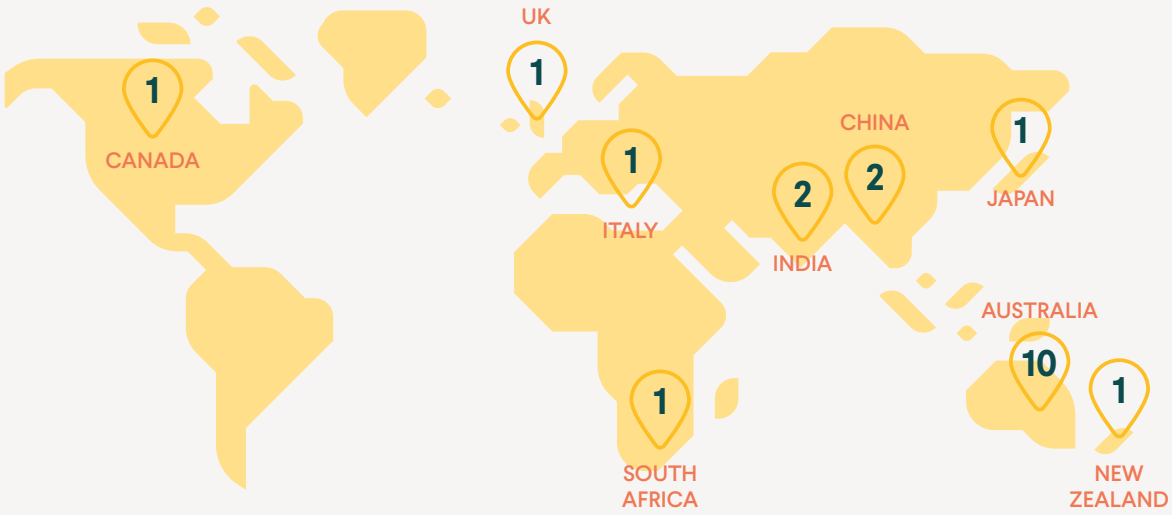
All interviews and focus groups were recorded for later transcription and transcribed by a professional transcription service. The research team coded the transcripts using the computer assisted qualitative data analysis software NVIVO and extracted key themes. In this report, we focus on the findings relevant to ACCAN's communications related priorities. However, we mention concerns about police and courts due to their prevalence in the participant comments.

Limitations

Since this is a qualitative study involving a relatively small total number of participants in two states, the findings are not intended to be representative of TFCC in general. Although we present some information about the number of survivors in this study who discussed specific issues, readers should not regard these as informative about the distribution or dynamics of abuse in the general population. Instead, this information is provided to allow readers to understand the intensity with which certain themes emerged in our convenience sample.

Because we recruited survivors who are women, we want to be very clear that readers should not assume that the dynamics described here would be reflected in relationships with male victims of partner abuse. Although we did not specifically recruit heterosexual women, all of the survivors in this study reported that their abusers were men. However, our findings can and should inform future research in other locations, with larger samples, and with additional cohorts of diverse survivors.

Participant background



Findings

This study identified a range of coercive and controlling uses of technology in the context of domestic violence. In line with previous studies, survivors most commonly described repetitive texting, emailing, and stalking and harassment via Facebook. In our sample, many survivors also reported abusers using cloud-based storage, especially iCloud and Google, and GPS data and devices in the abuse. Some of the TFCC was overt, with abusers ostentatiously demonstrating their surveillance and control. Other forms of abuse were more clandestine, intended to uncover imagined affairs, control communication with survivors' social networks, and prevent them from leaving.

Most survivors described abusers exploiting commonly-held knowledge, devices, and apps. These approaches do not require special skills, knowledge, or tools, although they may require access to a physical device or unlocked or shared accounts. Unauthorised access may be possible when perpetrators are able to guess their partners' passwords or know the necessary details to access devices or accounts. In our sample, attempts to prevent or control women's access to technology included the destruction, theft, and hiding of devices. Survivors also described abusers using pressure, violence, threats of violence to force compliance with demands to access to devices. Some survivors in our sample said that their abusers had greater than average tech skills due to professional IT experience and qualifications. These survivors expressed greater doubts about their ability to escape the TFCC.

In this section, we first describe key contexts for understanding the dynamics of TFCC. Then, we describe common types of TFCC including intrusion, surveillance, and identity crime.

Key Contexts for Understanding Technology-Facilitated Coercive Control

This study reinforces findings from previous research on TFCC and provides new information. Key contexts for understanding TFCC emerged from participant stories. These contexts are essential for understanding the characteristics that distinguish TFCC from other forms of online or technology-facilitated abuse, cybercrime, and bullying. Given our recruitment strategy involving specialised domestic violence and legal services, these findings reflect serious domestic violence necessitating help-seeking. As a result, our sample is substantively different from those accessed in previous population or panel-based surveys of people who have ever experienced a range of negative technology-facilitated behaviours. This group of survivors is also broader than survivors in refuge settings, a common cohort for research specifically designed to collect data on domestic violence or coercive control. Key contexts for understanding the dynamics of TFCC include: the coercive and controlling relationship, pre- and post-separation abuse, co-parenting with abusers, the high cost of ICTs for consumers, and survivors' safety work.

Tech abuse increases at separation

100% of survivors abused by an intimate partner reported tech abuse began or escalated at separation.

The coercive and controlling relationship

One of the challenges for understanding and dealing with TFCC is that some of the behaviours and technologies used by abusers can be innocuous in the context of a non-abusive relationship. In other words, identical behaviours, from frequently texting your partner to checking their location, can be harmless or abusive depending on the overall context of the relationship. Like many aspects of domestic violence and coercive control, TFCC describes relational dynamics involving an interplay of behaviour and reactions against a shifting backdrop of control and fear. The overall history of the relationship, behaviour patterns, and the meaning of the behaviours to the parties involved are key to understanding TFCC. A behavioural focus that does not account for the context and patterning of behaviour can trivialise the seriousness of TFCC and fail to accurately identify the primary aggressor in an abusive relationship.

Pre- and post-separation abuse

Copious research indicates that domestic violence does not end when the relationship ends. Instead, perpetrators often escalate and extend their abuse to other family members, friends, new partners, and collateral victims at separation (DeKeseredy, Dragiewicz & Schwartz, 2017). This study confirms these findings. Twelve of our survivor participants were aware of TFCC during the relationship. All of these women reported that it increased at separation. The remaining seven survivors reported their partner began using TFCC at separation. None of our participants reported that TFCC decreased or ended at separation.

Echoing survivors consulted in other research (George & Harris 2014; Harris & Woodlock 2018; Woodlock 2017), women in this study emphasised that TFCC was part of their overall experience of domestic violence. Like more "traditional" domestic violence, our study found that abusers often established control in ways that appeared benevolent at first. As ICTs blur boundaries between public and private life (Salter, 2016), abusers can exploit the ambiguity around privacy and intimacy norms in relationships. For example, Nicole "didn't really find it to be inappropriate" that her husband would access her Facebook and Instagram accounts "because I thought, oh well, we're married and that's what you do."

Sarah's account demonstrates how the intimate threat model unfolds in a relationship setting. She recalled that on their first date, her ex showed her all of his devices and offered to let her log in with her own profile on his computer. He watched her enter all of the information. Sarah said he was "right there, and I remembered feeling awkward about it, but I wasn't very IT savvy." She continued,

> **he watched me because I put the password in, I just kind of felt - because I had always protected my password and I thought [maybe this wasn't okay], but he's put me on his computer, so I guess we're sharing these things, but that was right from the beginning.**

Pre-separation, abusers were able to garner information about women's activities, communication, and movements where they shared accounts or devices. Family plans and devices connected to the same cloud or wi-fi network also aided surveillance practices. In a number of cases, abusers gifted or offered shared phones, tablets, or computers or connected profiles. For example, as their relationship continued, Sarah's ex gave her his old Apple devices and bought Apple products for her and her mother. As she was previously a Microsoft user, he "set up our accounts." He characterised his actions as ensuring they were "all a part of the family," and said, "Don't worry about it if you can't [use the device], I'll do it for you." She explained that his actions "look helpful" but facilitated surveillance because "he could see the communication between us."

Perpetrators' privacy violations and demands to access women's ICTs escalated as relationships progressed and abuse became more visible. Mirroring patterns reported by other survivors in this study, Sarah's ex gradually "took control of everything, so he controlled all of the passwords... [and was] wanting to share [financial and ICT] accounts and share everything." Sarah's abuser objected to her use of other profiles and software, such as her non-Apple email, "because it's password protected." He tried to persuade her to stop using it on the basis that it was technologically inferior to the account he had provided. Sarah reported that he wanted to control and monitor her use of technology in general, for example objecting when she deleted her Internet browsing history. Like Sarah, other survivors in this study began to recognise their partners' use of ICTs for purposes of surveillance, intrusion, harassment, and threats as abusive relationship dynamics emerged over time.

As Dimond, Fiesler and Bruckman observed, TFCC can "pose not only a greater danger, but also provides a deterrent for some women who are leaving" (2011, p. 413-414). Survivors in our sample reported that TFCC made leaving even more frightening and difficult. For example, Michelle knew that her abuser was monitoring her devices, apps, and browsing history. She was concerned that he would be able to find out information she had downloaded on her phone while at work to assist her in leaving. Michelle described her terror when "[h]e got hold of my phone that day and was going to go through it." He was unable to access it because of her password and she said "[i]t was God looking over me because if he had found that, I would have been toast."

Separation did not stop TFCC for our participants. For example, Isabella reported that her former partner shifted from more private forms of TFCC such as text messaging to public harassment post-separation, posting negative messages on social media "every couple of days," including after an apprehended violence order was issued against him. Perpetrators also continued taking advantage of information provided via shared accounts and devices post-separation, particularly where women didn't know how to restrict access to data or devices. Jia discarded her phone, but said that "the one thing I ignored when we separated" was that her account was connected to the same cloud as her abuser, so "everything, like passwords" was all still available "all automatically, and for him it's easy [to see everything]." In sum, abusers often established surveillance and control of survivors' ICTs during the relationship, before they realised the partner was abusive. They were able to use this information to continue abuse post-separation.

Post-separation parenting

13 of 14 survivors with children reported technology-facilitated abuse during post- separation parenting.

Co-parenting with an abuser

Our findings indicate that post-separation parenting is a key context for TFCC. Fourteen of our survivor participants had children. Thirteen of these reported TFCC in the context of post-separation co-parenting. Voluntary or court-ordered contact between abusers and their children provided opportunities for them to continue abuse against mothers and children. Abusers often used children as a source of information post-separation, asking them about phone numbers, location, and account information. For example, Julia's ex pressured her son to provide him with a streaming entertainment service password, through which he could gain access to further information about Julia. Nicole noted the challenges involved in ongoing communication between her abuser and their children:

> **My tactic is generally to block [my ex on social media] but it's made it very difficult because we have two children together and they want to contact their father and speak to him, so at some stage I have to unblock him and then the kids will want to talk to him. They like to FaceTime him and he will just then ask them, "Where's mum? What's mum doing?"**

Jessica's ex used different kinds of technology to contact her, "trying to side-step" the no-contact agreement, for example saying "'Well, I didn't write.... It doesn't say anywhere that I can't send voice recordings."

Survivors and practitioners described the extensive ongoing labour required to search for tracking devices and check settings in children's toys, prams, phones, tablets, smart watches, computers, and fitness devices on return to their mothers' residence. This was particularly stressful for survivors in refuge or who had relocated to a new address their abuser didn't know. Domestic violence workers noted that apps could be used for good or evil, with abusers using apps developed for child safety to track their partners.

High cost of information and communication technologies

Participants in our study indicated that ICTs were both indispensable and prohibitively expensive. Survivors reported that the cost of mobile devices and services were a challenge for them as they sought to extricate themselves from abusive relationships. As a result, some survivors in our sample had to continue using mobile phones and services tied to their abusive partner post-separation. This created security risks as it enabled some abusers continued access to information about the communication activities and whereabouts of their former partners. It also offered opportunities for abusers to change password information and interfere with access to services. Some survivors struggled to get telco or platform assistance to regain control of accounts. Additionally, the cost of setting up new accounts or purchasing new phones, tablets, or computers was too high for some of the women. Yume emphasised that "[s]ince we separated I don't have a lot of money. I have hardly any money." "Everyone tells me to get a new phone," she noted, "but I don't have money to do that." As a result, Yume's abuser was able to use the cloud to detect her location and activities. Many participants in our study also described abusers smashing their phones. In some cases, women were forced to continue paying for devices which had been destroyed by their abusers.

These results support campaigns for affordable telephone and broadband service based on the disproportionate burden of ICT for low income households and the trend to move public services online (ACCAN, 2019). Mobile broadband offers communication opportunities beyond telephone service such as via messaging apps like WeChat, What'sApp, and Facebook Messenger. However, many domestic violence survivors access multiple services in their efforts to protect themselves and their families from abuse which may require telephone service. While 1800 numbers are now free when accessed via mobile phone in Australia, telcos have stopped short of making 1300 and 13 numbers toll free from mobiles. Instead, they have made available "1300 friendly" plans (ACMA, 2014). Accordingly, our findings add another dimension to calls for affordable Internet and telephone services: the safety and security needs of domestic violence survivors. The widespread misuse of ICTs by domestic violence perpetrators could be minimised by industry and/or government policy to protect ICT consumers experiencing domestic violence.

Survivor safety work

Drawing on Kelly's concept of "safety work" (Kelly in Vera-Gray 2016: xi), previous studies on the use of technology in domestic violence have highlighted the burden that is often placed on survivors to keep themselves, and their children, safe from abuse (Harris & Woodlock, 2018). Survivors' efforts to enhance their online security and privacy at a time of acute crisis placed them under further emotional strain. Survivors described frequently checking whether their phones, tablets, apps, profiles, or accounts had been accessed. For example, Michelle believed that her abuser continued to access to her email and social media accounts post-separation. Seeking to detect his access to these accounts, she described her process of checking login attempts, noting she had to review "all of those... [and] check that I had done them all [logged in at all those times and places]." She also demonstrated high-level awareness of location settings in apps and devices, which she carefully reviewed and turned off. Michelle reported that she "felt like a sleuth."

When survivors are unable to access effective service or systems responses to technology-facilitated abuse, they may elect or be pressured to disengage from using ICTs. However, this form of safety work exacerbates the isolation created by domestic violence. Given the extensive role ICTs play in everyday life, disengagement from technology limits opportunities for building supportive networks, accessing education, and professional engagement.

Significantly, many participants in this study reported that disengagement from technology escalated rather than alleviating the abuse, since offenders may react to survivors' disengagement in aggressive and intrusive ways. As a result, some survivors strategically used ICTs as part of the safety work they did to protect themselves and their families. Indeed, in the absence of meaningful relief from threats of further violence, including femicide and familicide, several of our participants reported enduring ongoing electronic monitoring and communication as part of their attempts to assess and manage threats posed by their abusers. For example, Sarah said,

> **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; like for example, our daughter's school, I can't give them - so I have a whole new phone, I own a Samsung, so a completely Android, and he doesn't have that number, but I have to have a number that he knows about because otherwise he will go looking for me elsewhere.**

Many survivors in our sample reported that the abuse escalated when abusers were not able to contact or monitor women using ICTs. Rebecca explained that, "If I didn't answer the phone or I didn't reply to his text messages within 30 seconds or anything like that, the abuse would double." If Rebecca's ex was unable to reach her, "he would just come home early just to make sure that I was at home," which "eventually led to me not being able to leave the house, not even to do grocery shopping … I was like a prisoner in my own home." Her abuser's efforts to control her online life extended further and further into her offline life.

Perpetrator behaviour also escalated in response to women's efforts to manage their security or restrict access to ICTs. Nicole "used to receive bombardment of text messages and if I would ignore them then it would just get more and more and if I blocked them then I'd get emails." Jia said her attempts to avoid TFCC "makes him even angrier. More angry… he feels, hmmm. It's like one thing has been blocked, so he tries to use other ways to access me." This reinforces previous research which found perpetrators sometimes engaged in additional abuse such as physical assaults or in-person stalking when they were unable to contact survivors using ICTs (George & Harris 2014; Harris 2016).

These patterns are important to highlight because survivors who disclose abuse to their personal networks, police, and services continue to be advised to disengage from technology as if this were a solution for TFCC. For example, Charlotte sought to stop her former partner harassing her and her family via ICTs. She received advice from a serving police officer - a family member - on how to informally instruct her ex to cease contact. However, this request did not curb the harassment. Her mother, cousin, and stepfather began receiving spam emails and threatening letters in hard copy and electronic form. Amidst a barrage of abusive texts, he threatened to contact her entire social network if she did not meet him in person one last time. Similarly, when Catalina blocked her ex from calling or texting her mobile, he began contacting her mother, attempted to contact her brother, and did not cease attempts to contact her. His in-person stalking spiked: "He started to show up at my work and then decided to come to my house." Accordingly, it should be emphasised that recommendations for survivors to disengage from technology are not only impractical, they can create or escalate risks to survivors and their loved ones.

Mirza describes the process of enduring and managing abuse as "compliant agency" (2018, p. 45). Mirza's research with 11 Pakistani Muslim women in the UK was focused on their decisions about whether to stay in abusive relationships or not. She argued that, "women's agency is best understood as a decisional balance of weighing the pros and cons of 'choices', where the benefit of ending the relationship are weighed against the cons of internal and external constraints" (2018, p. 45). The concept of compliant agency, wherein women choose from the options available to them based not just on abuse, but also the on personal, cultural, material, and structural factors that characterise their situation, can be also applied to TFCC. The women in our sample made choices that weighed the risks and benefits of enduring some forms of abuse in the context of their current personal resources; ineffective legal responses to domestic violence, especially when they had children with an abuser; and lack of government support to meet basic needs, including access to telecommunications services.

The key contexts described in this section provide essential background considerations for readers seeking to understand TFCC. The meaning, types, and outcomes of TFCC are shaped by survivors' location across these and other contexts. Consequently, remedies for TFCC should take the broader social ecology of domestic violence into account when considering how to best address the abuse. In the next section, we discuss survivor experiences of different forms of abuse and their effects on survivors.

Survivor Experiences of Technology-Facilitated Coercive Control

This study documented a wide variety of technology-facilitated coercive control. Below, we discuss three primary categories of TFCC: intrusion, surveillance, and identity crime. Intrusion includes behaviours such as repetitive texting and calling via mobile phone; contacting survivors' social networks; and networked abuse. Surveillance includes monitoring and stalking behaviours. Identity crime includes impersonation, identity theft, and unauthorised account access. This is not an exhaustive list of types of TFCC reported by participants. However, these categories represent commonly reported forms of abuse.

Intrusion

Intrusion is an under-studied aspect of domestic violence that is widely acknowledged by survivors and specialist domestic violence services. Constant demands and interruptions are a key part of TFCC. Intrusion allows abusers to harass, humiliate, and pressure their partners. Many abusers use intrusion during the relationship to coerce and control their partners. At separation, ICTs allow abusers to continue intruding into their targets' lives when they may have reduced physical access to partners. In this study, we most often heard about repetitive texting and calling; contacting survivors' social networks; and using ICTs to arrange "real world" contact by willing confederates or unknowing dupes.

Repetitive texting and calling

All of the survivors in our study described repeated texting and calling to mobile phones by their abusers. Many survivors also reported abusers using other messaging and social media apps to send numerous messages. This type of abuse had different dynamics pre-and post-separation. Pre-separation, many abusers sent high volumes of messages and voice calls in efforts to control and monitor partners. During the relationship, Amahle felt like she had "no reprieve from this constant availability that I had because of my mobile phone." Her partner "wouldn't let me get off the phone with him… he'd just be refusing to, and [if] I hung up he'd call back." "[T]here was no way to de-escalate it," she lamented. "[I]f he wanted to speak to me I felt like I had to speak until he was ready to stop speaking." Isabella's abuser believed she was cheating and sent "text messages, [made] phone calls" and would use Facebook, Instagram and WhatsApp, "[b]asically, any form of app you could get he was messaging me on" to constantly contact her. Julia described having "Seventy-two missed calls and threatening messages" from her abuser. Josie received "hundreds and hundreds and thousands" of abusive text messages throughout their relationship.

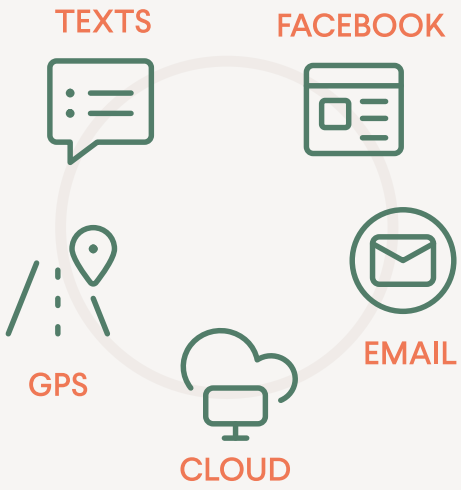
Often, abusers demanded that their texts and phone calls receive an immediate reply. For example, Nicole's abuser wanted her to have read receipts (a function that tells the sender when their text messages have been read by the receiver) active on her text messages at all times. Many abusers required survivors to have their phones charged, with them, and turned on at all times. They expected that women would answer the phone within a set number of rings, call or text back immediately, or send photos to document their location and activities.

Failure to immediately reply typically resulted in an increase in the number of times abusers made contact and escalation of their aggression. Jessica noted that when "I just stopped responding to his calls and texts … it just amplified it. It went mental. I've probably got, you know, 50 to 70 texts a day, sometimes 20 to 30 missed calls." Threats of violence or humiliation were used to reinforce demands for an immediate reply. Julia's former partner would send messages or leave voicemails saying "Oh, you'd want to effing answer your phone… threatening [me] - trying to intimidate and make me feel scared."

Women were also sent messages that contained defamatory, degrading, and offensive content. These might include attacks on women's behaviour, appearance, or parenting. Alternatively, they might reference prior sexual assaults or threaten distribution of sexualised images. Many abusers deliberately used veiled references and avoided explicit threats, which made it difficult for women to provide clear evidence of the abuse they were experiencing to police, courts, and telecommunications companies.

Common types of abuse

Repetitive texting, emailing, GPS, cloud and Facebook monitoring were the most common types of abuse.



This abuse did not end at separation. Most of the survivors and domestic violence support workers we consulted indicated that repetitive texting and calling increased exponentially at separation. Many women experienced it as overwhelming, "constant," and extremely stressful. The morning she spoke with researchers for this study, Rebecca noted she had received "13 missed calls within, say, 20 minutes .... He will just constantly ring until I answer the phone." Julia told researchers she had received 73 calls in one day. Although her abuser had had other relationships and remarried, "he's never actually stopped throughout all these years of being separated, of trying to be in control." Nicole described receiving "[b]ombardments of text messages," around 20 or 30 a day. She described these as "abusive messages - or just multiple messages about the same thing - and if I don't answer them, there would be another message and another message if I didn't answer within what he feels that was a reasonable time frame."

Text and social media messages and phone calls often rapidly cycled between verbal abuse, threats of violence and self-harm, and threats of punishment for not responding. Catalina's former partner "kept calling me and calling me." When she entered another relationship, "the abusive message would come and be like, 'if you think you're going to be happy, you've got [another] thing coming; both of you are dead. I'll make sure of it, I'm going to kill him before I ever see you with him.'" Elizabeth's ex (who had an array of weapons at his house) sent "[a picture of] 'the knife I'm going to slit my wrists with,'" then "pictures of needles [saying] 'I'm going to kill myself.'" Ajinder's former partner also sent emails with "some horrifying images, like he cut his wrist and wrote, 'I miss you'" in efforts to pressure her to respond to him and reconcile.

Some survivors in our study described what has been called the cycle of abuse, wherein abusers alternate abuse and expressions of love or contrition. Elizabeth's ex sent "a whole lot of text messaging trying to make up" alongside abuse and threats to harm her and himself. Michelle explained that "'it was pretty much that domestic violence cycle of they blow up and then they'd love you." In this vein, during the dissolution of their relationship, Anaya's ex oscillated between sending emails saying "You are a bad crazy woman. You are a bad woman," and "I love you. I have done something wrong to you. I was [acting] in anger... I can be for you forever... I can't live without you and I love you so please call me back." Likewise, Isabella's former partner "was just so full on with the [abusive] messages or he'd go off at me via text message for no reason and then he'd be like, 'I'm so sorry, can I take you to dinner', and then it's just - it seems like it just starts all over again."

Contacting survivors' social networks

Survivors reported that abusers contacted, or threatened to contact, their family, friends, and co-workers using ICTs. This approach was used to enlist survivors' social networks in pushing for contact. Yume's daughter refused to respond to ICT requests from her abuser, so the abuser had his son send messages on behalf of her father, pressuring her to talk to him. Abusers also sought to intimidate, harass, and humiliate women or challenge womens' accounts of abuse via their networks. Jia's ex "mentioned that he had all - like, most of my friends" contact information. She worried that her abuser would "say bad things to my friends about me, to my friends" or impersonate her online if she refused demands to meet with him. Similarly, post-separation, Charlotte felt she had to "engage in reputational management" after her abuser reached out to various family members and sent several text messages to her warning that he would tell everyone his version of the story. Josie's former partner stole her phone and wrote to all her Facebook friends to inform them she had left him, adding "I don't know what happened to her. She's not mentally okay."

Networked abuse

Some survivors reported that their abusers had recruited other people to participate in TFCC. Many perpetrators used their friends' and family members' devices and accounts to contact survivors. While women sometimes blocked their abusers' number or account or had orders prohibiting communication, it was not possible for survivors to block all possible contacts in their abusers' networks. For example, after Michelle obtained a domestic violence order prohibiting contact, her abuser was "trying to keep [the TFCC] going" by drawing on his closest associates, "and it was really hard." He "got his daughter to text me, he got his mother to text me, his sister to text me because he wasn't allowed to. So they all said quite nasty things as well." In Anaya's case, her abuser's family used technology in ways she found distressing and believed constituted invasions of her privacy. Her former partner's family pressured her to reconcile with him via email and phone.

Surveillance

Abusers used numerous techniques and technologies to monitor women's actions, communication, movement, and location. Sometimes this monitoring went undetected for long periods. Amahle didn't know that her abuser had been tracking her until after they separated. Elizabeth noticed her abuser's phone in her car one occasion, and later "discovered that he was tracking different places that I'd go to [using his phone]." Several survivors reported that they realised after they separated that their partners' surveillance was greater than they had realised during the relationship. Sarah's former partner had a video camera in their car. She learned he had installed cameras throughout their house via legal documents related to their separation. She reflected that she was "always stalked, always controlled, [during the relationship and he] had [captured] all of our communication." Indeed, the practitioners in the focus groups suggested that the majority of women underestimate the degree to which perpetrators used technology to stalk.

In many cases, however, abusers were overt in their stalking. Michelle was aware that her abuser would "continually go through my phone, my iPad" reviewing her Internet browser history, apps, and text messages. Rebecca knew her ex "had my location tracked, logging into my iCloud - yeah, logging into my Facebook. Had my Facebook linked to his phone so he could monitor all my messages, went through my phone, my text messages, my location, everything." Rebecca's abuser used apps and enabled settings on her smartphone so he could track her location and had installed a camera in their house to watch her. She noted that her abuser would send abusive text messages and make repeated phone calls if his tracking efforts placed her in a location that didn't match where he thought she should be.

Women's knowledge or suspicion that they were under surveillance affected their experiences and responses to domestic violence. Michelle's ex had set up her devices and those belonging to her family members. All of these were connected to a cloud account that he controlled. She knew he was able to access their phones and tablets, see their communication, and was monitoring her online activities. In preparation for leaving, she asked friends not to send any text messages and endeavoured to clear her digital footprint, "deleting every email. Emptying my trash, all

of that," and devices "[e]very app that I had on the iPad I took off that." She then mainly used technology at her workplace instead of at home. When Michelle left the house they shared, she hoped he would not be able to find her. That evening "he was at the front door of my new home." She was not certain how he found her. Michelle reflected that he may have located her via ICT devices or features she had not disabled despite her rigorous security regime. She said, "he worked for the car company … we think he got somebody within a car company to track me via a GPS in the car."

As Dimond, Fiesler and Bruckman (2011, p. 420) caution, technologies "pose not only a greater danger, but also provide a deterrent for some women who are considering leaving." Seeking to intimidate and discourage her from ending the relationship, Jia's former partner told her and some of her friends that, "I know everything. So, whenever you hide, I can always find you." She became convinced that "it's an information age and it's the [age] of information technology, so he can always find me." Elizabeth became aware that her abuser had used his phone (and possibly other means) to track her location, which seemed to facilitate his in-person stalking post-separation. Similarly, Amahle's ex-husband used her mobile phone to track her over an extended period after the relationship ended. She said,

> **[My] mobile phone was used to somehow create a tracking device on my phone that then my ex used to track my movements for over a year … It emerged later that he knew every single place I went to … What initially happened was that he… sort of started telling me things that he knew I'd been doing. He said "Oh, you've been to this place and you've been here and there" … If I went somewhere unusual, he would go there and hang out outside and wait and watch and use that to actually, yeah, locate me, stalk me when he wanted to. So that was bad.**

Amahle revealed that her ex-husband had been sent a parcel which was inadvertently delivered to her address with a GPS tracking device enclosed. "It was tiny," she notes "and what is in my mind now is that those things can go in anything." Sarah worried about modes of surveillance her abuser might use, describing how she would check and wash her children's toys and clothes in an effort to find or disable devices.

Julia explained that "every time I'd change my phone number or whatnot, he seemed to get it … I don't know how." Suyin had changed the passwords of her compromised accounts (her email and government immigration account) but realised he was still able to access the accounts and was told by victim service workers that her email was not safe. She also discovered that her abuser was accessing her Facebook profile and Messenger by reviewing account login times and IP addresses. Jia found out that her ex was monitoring her email and the online profiles of her banking and educational institutions. She was not able to discern how he had done so.

These survivor narratives speak to the fear they experienced as well as ongoing pressure to locate and block further monitoring attempts. Women were often aware they were under surveillance, but not of the methods engaged by their abusers. This made prevention difficult or impossible.

Restricting access to technology

Some survivors reported that abusers restricted their access to technology in addition to surveillance. Amahle described how her abuser "just grabbed my phone out of my hand and drove off with it. Because it was open when I showed it to him, he just kept it open and jumped into all of my private messages, emails, photos, everything," which he later downloaded. The destruction of technology and restriction of access to technology is another form of TFCC. Julia noted that her former partner would "basically just smash the phone so you can't contact anyone." Josie's ex cancelled her phone plan and changed the number. Earlier research has noted that restricting access to technology can exacerbate existing vulnerabilities, such as for survivors with disabilities (George & Harris 2014; Harris 2016; Harris & Woodlock 2018). Some survivors reported that their former partners accessed their devices and accounts to delete data. Suyin's ex deleted many of her emails, including correspondence from her overseas support network and electronic documents she needed for the Department of Immigration.

Identity crime

As described above, survivors in our sample reported abusers engaged in unauthorised account access, impersonation, and identity theft. These categories often overlap.

Unauthorised account access

Survivors reported that abusers gained unauthorised control of various accounts and devices. In some cases, women felt that this was to monitor their communication or behaviour. As Julia put it, "[h]e still wants a little bit of control." Sarah found out that her abuser was trying to access her health care accounts, even trying to change her password while she was on the phone with the provider. She suspected he had attempted to add himself to and change login information on other accounts and received notifications indicating he had done so. She would have to "contact each and every one of them, show them it's me [on the phone] and that if it's changed its not me trying to change it, and please notify me of something," which was a lot of work. Jade realised her brother had accessed her father's email account because his abuse was based on private emails between her and her father. Some survivors also reported that their abusers used unauthorised account access to impersonate them.

Impersonation

Our participants indicated that abusers impersonated survivors and others online. Some reported that abusers had used their devices or logged into their social media accounts in order to impersonate them. This happened during relationships and post-separation. Amahle's abuser took her phone and messaged her friend, pretending to be her. Josie said,

> **He did pretend to be me … He will actually go on Facebook and pretend it was me and was writing. I can't believe it. One day I find … sweet Jesus, I didn't write this message. You know what I mean. So stuff like that which is not good. I don't know how he [found] me but I think I left it on, I don't know. Maybe it was my fault.**

Other women reported their abusers had created fake accounts in their name. Nicole discovered that her ex had both accessed her Instagram account and created fake accounts in her name. He had been communicating with people while impersonating her. She was concerned that "if [the interaction] went bad then the person thinks it's me." Isabella's former partner posted on social media that "my crazy ex is trying to add everyone on my Facebook." She suspected that he had created a fake social media profile in her name and sent friend requests to people in his network to prove his claim. Nicole reported that her ex created a PayPal account in her name but connected to his account. She worried that it would get her in trouble.

Nicole explained how difficult it was to try and respond to this problem. She searched on the Internet to learn what happened in these cases and was dismayed to see that, there's so many people saying that's what's happened to them. I thought "what the hell?" I'm not the only one that this has happened to. It's not hard [to take someone's identity to create an account and] … rack up a heap of debt in somebody's else's name.

Some survivors reported that abusers used fake social media profiles to contact them. During their relationship, Isabella's partner created fake social media profiles to monitor her interactions, convinced she was cheating on him. Post-separation, Georgia received messages from a barrage of different names that she attributed to her abuser. He would use these personas to "say all these horrible things about me and my family, and my now fiancé." Isabella also reported a high number of incoming texts all times of the day and night from random numbers. The seemingly endless supply of fabricated identities sending messages and the frequency of these messages combined with difficulties blocking senders to make survivors feel they were surrounded by vitriol. Abusers also impersonated others in communication with their own children. Yume's daughter stopped responding to her father's texts and video calls after she became frightened of him, so he created a fake Instagram account pretending to be the daughter's friend from her school in order to communicate with her.

Impersonation made it difficult for women to effectively block abusers. Isabella would block her former partner on social media, but he would "delete his whole account, not just deactivate, delete the whole account… so therefore that email address was no longer on the platform's system. Then he could go and make a new account and contact me again." Other survivors identified the ease with which perpetrators could manipulate loopholes in social media administration in order to create new accounts to harrass and abuse them. Jessica said:

> **I'm not sure how you can really stop stuff…. He's IT. He knows - he makes computer programs, so he's got probably, the knowledge to get around a lot of stuff… [and anyway] If I was to block one email, he can just as easily set up a new email address and start sending it that way. You can make 1000 of them, you know? So I don't see it as being productive.**

In addition to trouble with fake accounts, survivors reported concerns about abusers' unauthorised distribution of their real information and documents.

Doxing

Some survivors feared that their abuser would post their private information publicly in a practice known as doxing (Snyder, Doerfler, Kanich, & McCoy, 2017). Isabella's former partner said, "if you didn't have this AVO I would give [your private information] out on social media." Charlotte's partner used her name and personal details to conduct a campaign of harassment against her and her family. After they separated, Charlotte and her family members started receiving spam and commercial newsletters from a slew of companies. She and her family members received dozens of horoscopes and emails from mediums as well as notifications she had signed political petitions she hadn't signed. Some of the companies followed-up with personalised email and phone contact they believed she and her family members had requested. She heard from a weight management program, addiction clinic, budgeting service, and insurance company.

The combination of these many types of TFCC extend more traditional forms of domestic violence. In addition, ICTs allow new forms of abuse that are yet to be taken seriously by systems and often outpace existing laws, involving the manipulation of lax security features in social media and other online platforms. As a result, TFCC can multiply survivors' distress. Unprecedented reach, access, and resources mean that TFCC is not simply a nuisance or annoyance. Our participants reported extremely high levels of distress due to TFCC.

Impact of abuse

The survivors in our study reported serious, pervasive, and persistent negative outcomes of technology-facilitated abuse in their lives. Our findings make very clear that the use of technology by abusers has become interwoven within the pattern of domestic violence, comprised of numerous controlling, abusive, threatening, and violent activities. TFCC is inextricable from the overall dynamics of domestic violence.

Aoife said:

> **He's always demanding FaceTime with the youngest girl. When I was back home in the country I am from, I had to agree to FaceTime to keep that relationship open for her with him. We were in emergency accommodation and he would say things, even though he knew I was there, it didn't matter. Show me, where do you live now? Do you want to show me around your new house? Have you got a nice view from your window? Prompting her to go to the window and show him outside, it's just constant.**

The harms of TFCC include extending and exacerbating the trauma of domestic violence by rendering it "spaceless," unceasing, and inescapable (Harris, 2020). Our participants reported that this quality of the TFCC had catastrophic implications for their mental health. Suyin said:

> **I've even been to mental health hospital twice. I said, if it's physical. I can hide. I can escape, but for this, it's the same as anywhere. Anywhere.**

Increased fear due to the experience of constant danger of being tracked, surveilled, or contacted was a major concern. For Josie:

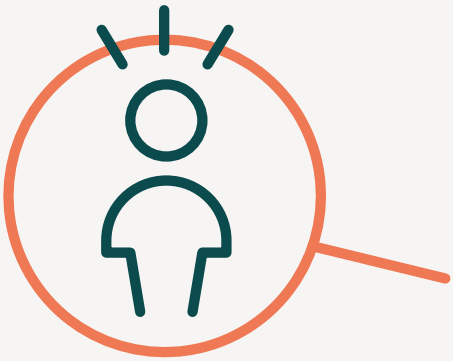
> **... I feel like I'm in a prison. Because I can't - going out I'm thinking, oh I'm not going to go there and I think I'm dead, I'm not going to go there. You know what I mean and you - I have to watch always at my back all the time. I feel really terrible.**

Amahle knew that the perpetrator had been ordering small GPS trackers online, prompting pervasive and understandable feelings of anxiety and insecurity.

> **Like every time he gives the children gifts now, the first thing I do is sit and feel them and take them apart to see if there's something in them. So it just creates this whole level of fear that you constantly have about being watched without your consent, and that there's so little you can do ... My kids have these toys and everytime I see the kids playing with it I can't help thinking that somehow those dolls are watching me. Even though I've taken them to the police to get them checked. So it just creates that level of like distrust around everything and how - and I think that the world is going to get worse with drones and things like that.**

Impact

Technology magnifies the harms of domestic violence and created new forms of abuse.



Jade explained that because her brother threatened her over the phone, it wasn't taken as seriously.

The privacy of communication via phone offers an opportunity for abusers to make direct threats without being observed by witnesses.

The climate of fear created by TFCC means that survivors such as Jade and Amahle are often seen as paranoid. As a result, their experiences may not be taken seriously by police and other authorities. Women also reported far-reaching implications of TFCC for their personal and professional social networks. As discussed above, it was common for abusers to identify and contact people in survivors' personal and professional networks using social media platforms like Facebook. In her efforts to escape persistent stalking and intrusion, Georgia's curtailed her online participation and modes of communication:

> **The stalking. The unwanted text messages. I had to get rid of most of my social media. My Facebook and Instagram and all that type of thing. I had to change my actual phone number nearly three or four times.**

Josie's ex-partner used social media extensively in order to contact her family and friends in an effort to track her. She said, "he was using all my contacts. Then everybody was [saying] oh, he rang me and he wants to know where you are."

Stereotypes about domestic violence characterise it as a "couple problem," and there are some couples who manage to keep most of the abuse out of public view. However, the reality is that abusers regularly extend their controlling and abusive behaviour to broader social networks. TFCC using social media makes this type of abuse visible in a way that it previously was not.

Many participants characterised the invasions of privacy and curtailment of communication as forms of violation that were damaging in and of themselves, infringing upon their basic dignity. Amahle observed that:

> **Nowadays our phones are so much [a part of] our entire identity, like everything is there. So to have your phone taken out of your hand and then read back to front is kind of like, it was just really violating. Yeah, I just felt like I had no - I just felt like he just had no care or respect, it was just really violating to be so revealed, really. Like every single private little message was sort of - so that was that. Then with the stalking, I mean it made me feel really scared, actually, just to have this device on you that you don't know how much, I don't even know if it was something that can turn on audio or not. Comments like this illustrate why well-intentioned advice that encourages survivors to stay off social media or the Internet to curtail TFCC is not only unreasonable and burdensome, but inadvertently colludes with the perpetrators' efforts to characterise their targets as deserving of less than the full complement of rights owed to others.**

Help-seeking

Participants in our study reported seeking help from multiple sources. Due to our recruitment strategy of partnering with women's legal and health services, all of our participants had sought assistance for dealing with the domestic violence they experienced. Fifteen of the twenty survivors discussed the ways they sought help for the technology-facilitated abuse. Survivors sought assistance from telecommunications companies, domestic violence services, friends and family, police, and courts. This is consistent with previous domestic violence research which has found survivors are active agents who use multiple strategies to manage their safety using the resources available at the time, given the cultural, material, and structural realities of their situation (Hayes, 2013; Kandiyoti, 1988; Mirza, 2018). Help-seeking is an important part of the process of escaping or surviving an abusive relationship. Many survivors who seek formal sources of assistance such as legal advice, police or court intervention, or specialised domestic violence services, discuss their situation with friends and family first (Meyer, 2010, 2011).

Telecommunications companies

Abuse and harassment via SMS, repeated calling, and monitoring using GPS on mobile phones were the most commonly reported types of TFCC in our study. Accordingly, many participants sought relief from their mobile phone and Internet service providers. The survivors in our sample requested assistance with many aspects of mobile service: getting released from friends and family plans held jointly with an abuser; changing phone numbers;making their phone number unlisted; regaining access to accounts after abusers changed passwords; getting a new phone; getting their phone or phone settings checked for security risks and/or spyware; and late fees and billing.

Participants noted the long wait-times on hold to speak to telecommunications companies when they needed help. Such delays may be irritating to all consumers, but they have additional safety implications for domestic violence survivors who may have a limited window to safely use the phone. Participants reported inconsistent results when seeking assistance from telecommunications companies, even over multiple contacts with the same provider. For example, Georgia needed to change her mobile number on her mobile plan due to the abuse. She said:

> **Well at first it was fine. Then the other times I had to pay money for it to get my phone number changed.**

In our convenience sample, Telstra was the telco most frequently identified as helpful. Optus and Vodafone were more often identified as less helpful or unhelpful.

Many of our survivor participants mentioned managing their own safety on Facebook by using blocking or privacy settings, pseudonyms, or limiting use of the platform. Few participants indicated they had used reporting functions or sought assistance directly from social media platforms like Facebook, Instagram, WeChat, or Snapchat. When asked why they hadn't sought help from these platforms following abuse, participants most often responded that they didn't think it would do any good. For example, Georgia noted that she used Facebook's block function. However, "everytime I did that he would just come up with another number. I just had to keep blocking every time."

Domestic violence services

Survivors sought and received a variety of types of assistance with TFCC from specialised domestic violence services. Overall, participants reported these services were supportive and encouraging. They provided a variety of types of assistance including:

- problem solving to figure out how security or privacy were being compromised,
- providing printed or online information about online safety and security,
- walking through ICT safety information alongside clients individually or in groups,
- hands-on checking of devices and items, and
- providing new phones and credit via the SafeConnections program.

Friends and family

The majority of our participants discussed the TFCC they experienced with friends and family at some point. Some of them were lucky enough to have friends who were knowledgeable enough about privacy and security settings to provide concrete help, such as Jia:

> **I have friends and they learn computer science. They are tech-savvy. So, I immediately, I just think of them. I ask them, how can I cut this? They ask me first to log out my iCloud and stop synchronising that … Then, they ask me to have another phone, like have a new phone. Still keep that one logged in and leave that one somewhere else. But I didn't do that, because I still need that phone. They also asked me to update my parents, their iCloud information, because my parents, they are using the same iCloud account, yeah. Because they don't know how to set up those, and so on. I decided - actually, they just use mine, and just sign in their iPhones. So, I did that.**

Others had family members or friends who were police officers, so they knew what police could and couldn't do. In some cases, these friends and family advocated for survivors with the police.

Police

The majority of our participants discussed their experiences seeking help for TFCC from police. While these issues are not the core concern of this report, the repetition of key issues requires discussion here. Participants reported mixed reactions from police when seeking assistance with TFCC. Many of our participants reported police saying there was nothing they could do about TFCC because they couldn't prove the identity of a caller or user. Others indicated that police recommended survivors screenshot texts and emails and save them for evidence.

Legal assistance

Survivors in our sample were recruited via women's legal services and provided accounts of seeking legal assistance for dealing with domestic violence. The survivors were very appreciative of the legal support they had received. Some of the challenges associated with legal responses to TFCC were: uncertainty about what evidence would be useful in court, how much evidence should be collected for use in court, and how to present it to the court in a way that would be useful.

Recommendations

Survivor Recommendations

This study sought recommendations from survivors and practitioners about how to improve responses to TFCC. Survivors were asked for their recommendations about how responses to TFCC could be improved and what would have been useful for them. Participants directed their recommendations in three main areas: the telecommunications industry, police, and courts.

In summary, survivors recommended several measures to improve responses to TFCC:

- improve recognition of TFCC as a serious part of domestic violence;
- educate and train police, courts, and telecommunication and technology companies about TFCC;
- eliminate charges for changing and un-listing phone numbers due to TFCC;
- offer financial hardship plans for domestic violence survivors unable to pay for phones, contracts, and plans;
- provide hands-on tech support for domestic violence survivors from law enforcement, phone companies and technology companies; and
- ensure that social media users and internet consumers experiencing domestic violence can contact the companies involved, and their needs and safety are prioritised.

Information and communication technologies

Participants felt there needed to be more awareness and understanding of TFCC within the telecommunication industry, in particular within phone companies. Several women had to pay to change their mobile number, which they felt was an unfair financial burden placed on survivors. Charlotte said:

> **I shouldn't have to pay to - because I'm never going to - I'm not going to get that money back; I shouldn't have to be paying them so that I stop getting harassed ... on their service. Yeah, I just, I don't know; they make me angry.**

Similarly, Georgia recommended that survivors not be charged for changing numbers, saying that the main area in which Optus could have improved their response to her was to have "not charged me for changing my number." Furthermore, Josie felt there should be more that phone companies can do for survivors rather than just suggest they change their number. She said:

> **I actually went there to Vodafone. I said, "Listen, is there any way that you can help me? I don't want to really change this number, I had this number for so long and why should I change it?" They're, "Oh the only option you have is to cancel it and we'll give you another number."**

Josie's experiences raise questions about the seriousness with which telecommunications companies are taking the misuse of their services by domestic violence perpetrators and the preparedness of staff to provide effective or tailored assistance. Her account also illustrates the wider effect that TFCC can have on survivors, wherein they are expected to modify and change their use of technology in order to minimise the abuse they are experiencing, amongst a range of forced accommodations across all aspects of their lives. Several women observed that phone company representatives evinced little understanding of the dynamics of domestic violence and were not helpful when women needed to break their contracts and phone plans. Nicole explained:

> **I keep my phone plan with them [Telstra] and I spoke to them about that and they just sort of like said "that's too bad." Because his phone and my phone are under the same plan and when I spoke to them about it, they were like, "you've just got to pay it out." It's like over $1000 I can't even afford to do that. So I'll have to suck it up and keep paying it.**

Rebecca felt that phone companies needed to offer hardship plans to women experiencing domestic violence, as she struggled to pay her phone bills after leaving her abusive partner. Rebecca said:

> **I had an argument with Vodafone. They were ringing me because my bill was overdue, but unfortunately, due to the financial abuse and the minimal payments that I was receiving from Centrelink, I was struggling to keep food on the table, and they were going to cancel my phone. I explained to them that I'm in a domestic violence situation. I'm trying to pack and get out of my house and I couldn't afford to make the payments just now, and they told me that that was just too bad. They were going to cancel my phone. I couldn't lose my phone number, because all the schools had the number, and it was school holidays, so my kids were at friends' houses and stuff like that. So it made it even more stressful that they were not willing to help in my situation, even just to put me on a minimal payment plan until I found my feet.**

Rebecca's experiences highlight the significant impact that a lack of understanding about domestic violence from phone companies like Vodafone can have on women and children's lives. Rebecca's suggestion of a hardship payment plan is a practical way that phone companies can support consumers who are experiencing domestic violence.

Survivors also had recommendations for the development of apps and services such as Gmail. As often advised for survivors of TFCC, Aoife has location services turned off on her phone, as well as cookies. However, this has meant that she is unable to use certain apps, such as banking apps. Aoife explains:

> **You see so many of these apps require your location services and require your cookies to be enabled, because I have a bank account back home and I've been trying to get access to it since I've come over here and I couldn't get access to it. I've disabled cookies, I've disabled everything. So, I know if I want access to that, I have to switch that on. Which is difficult to handle as well you know. Maybe the bank could have another way to confirm that it's you, without the cookies and the location, so that you can use the service without compromising your privacy.**

As Aoife's experiences highlight, when apps are not designed with the needs of consumer groups such as domestic violence survivors in mind, it can prevent them from utilising much needed services such as banking apps.

Jia noted that Gmail only keeps past activity on your account for 28 days, which made it difficult for her to obtain the evidence she needed to show that her ex-partner was accessing her account. When Jia tried to contact Gmail to ask for past information on her account she could only find an online form to contact them. However this did not give her the options she needed. Jia said:

> **I tried to figure out what their contact number is. It's not there. So, it's just the online one. It's like AI. They can help you, but it's not a real person. Because our case is very complicated. I cannot just use the online forum to ask them.**

Jia had a similar issue with WeChat. Jia felt that WeChat offered good privacy and security, and she was able to block her ex-partner from seeing some of her activity. However, because they have friends in common on WeChat, any posts or comments that she made to her friends accounts were visible to her ex-partner. When she tried to contact someone to explain her issues, she could not get through to talk to anyone. Jia felt that there needed to be clearer options for those experiencing abuse to be able to contact services such as Gmail and WeChat.

Police

A key recommendation from survivors was for increased education and awareness of TFCC amongst first responders such as police. Survivors reported that police usually did not offer to do basic checks of their devices for security threats, did not collect evidence of TFCC, and failed to offer helpful advice about how survivors could best collect such evidence themselves. Amahle explained that when she went to the police for assistance due to stalking, no one looked over her phone to see if she was being tracked via these means. Amahle said:

> **I came in there [to the police station] reporting that the guy quite clearly had been following me the night before. They looked at the messages from him on my phone to kind of like assess whether they could make an application for the temporary protection order. But no one at that point just checked my phone to see if there was a tracking device on it, which, having done it ourselves about two hours later, I just don't understand why. No one even checked that. Why aren't the police just having a really basic knowledge on like how to check a phone for tracking devices?**

Amahle indicated that even if the police did not have the technical knowledge to check for tracking on a device, that they should at least have explained the ways that a phone could be tracked:

> **It seems like a pretty basic thing that they could fix, like even if they only have a basic knowledge on how to check it. Or just provide me with that website to go over a quick rundown on my phone and check that.**

Likewise, Jia felt that the police did not offer her any guidance on how to best collect evidence of TFCC from her devices. Jia had a protection order but did not know how to show when the perpetrator was breaching the order. Jia explained:

> **I have this order, so I can go to the police and they can charge him but I think it's more like, how I can provide evidence. It's so difficult. Because I'm not, like, tech-savvy. I don't know how I can get at evidence. I say, okay, he probably monitors my iPad, but how can I prove it?**

Jia felt that the police did not take TFCC seriously, and that it was only through assistance from her friends that she was able to secure her device. Similarly, Sarah complained that police did not take the abusive text messages from her partner seriously and that they needed more education about TFCC. Sarah said:

> **And the police, they need education about it, because yeah, when you show them your phone, which I did, they just - I guess because we all have dramatic text messages, all of us, whether it's with friends or family, so there's no context of what that means.**

Sarah's ex-partner sent her text messages throughout the night, which was significant to her as she knew that if she didn't reply that he would "rock up [to the house] because you haven't answered at 2:00 am." However, Sarah reported that police minimised her experiences, and were unable to recognise that these messages were part of a pattern of abusive and controlling behaviour.

Courts

Several women said that there needed to be more education throughout the court system on the seriousness of TFCC. In Sarah's experience, TFCC was not considered a serious matter by the courts. If it was not physical abuse then it was not seen as "dangerous." She said:

> **There's just not enough education about what technology, how it can be used, because it's seen as safe, because they're not breaking your bones. When you're in the courts fighting for protection or fighting for orders, they just look at well are you physically harmed and if you're not physically harmed and they feel like they don't have that physical access to you, you're deemed safe, and technology is not deemed as dangerous.**

Similarly, Yume said that the forms that she had to fill out to get a protection order asked many questions about physical abuse, but did not give her the opportunity to describe the TFCC she had experienced:

> **On the form it mostly asks about physical violence, but it should also have on there about the phone. It is hard to explain when it is not physical what is going on. If they had it on the form, the technology abuse and the texting it would be easier to explain. That's one thing they could change.**

Aoife felt that this lack of understanding about TFCC, and the impact on survivors, meant that when court orders stipulated that contact regarding children be made via email there was no consideration of how this could be an avenue for further abuse. Aoife explained:

> **I would say that the legal system really needs to be careful in how they expect that [child contact] to happen and to still safeguard the women from further abuse, further psychological abuse through emails. I think sometimes they just assume that it's safe because it's not face-to-face, you know what I mean?**

Practitioner Recommendations

The practitioners from specialised domestic violence services, women's refuges, and women's legal services had multiple recommendations about which resources are valuable and should be expanded as well as what would be helpful to assist them in supporting domestic violence survivors in the future. Key recommendations include:

- recognising and responding to the digital divide;
- enhanced platform and telecommunication access and responsiveness;
- increased training and education;
- expansion of existing resources; and
- hands-on technology security checks.

Recognising and responding to the digital divide

Cost and connectivity challenges result in rural Australians experiencing a digital divide: that is, their access to the Internet and ICTs are significantly less than Australians in urban or regional areas (Curtin 2001-2002; George & Harris 2014; Rooksby, Weckert & Lucas 2007). Domestic violence workers reported that service gaps are a major problem in rural, regional, and remote areas in Australia. In some cases, service is only available in certain parts of town, dropping off quickly once you head out of the centre. Some communities have no mobile service. Workers noted that personal safety alarms and safe phones rely on networks, and as a result, they don't work in service black spots.

Consumers living in these areas would be well aware of the service gaps from experience. Service coverage maps intended to provide helpful information about where phones will work also tell consumers where service is unavailable. Abusers can use this information to carry out abuse where the survivor will not be able to call for help. As the example from Vodafone below illustrates, large areas are unable to access mobile phone and Internet service and there is significant variability in signal quality where coverage is available.

Figure 1. Snapshot of Vodafone Coverage Checker map

Source: https://www.vodafone.com.au/network/coverage-checker

Practitioners noted that while mobile phone and Internet access had improved in recent years, the cost of service was prohibitive for many vulnerable women. The workers pointed out that there are fewer employment and educational opportunities in non-urban areas, which can affect the financial status and security of rural survivors (see also George & Harris 2014; WESNET 2000). Better communication for poorly serviced areas and affordable communication are therefore essential to improving survivors' experiences as consumers and responses to TFCC.

Enhanced telecommunication and platform access and responsiveness

Advocates had numerous recommendations which would serve to empower consumers and improve consumer safeguards. In the course of assisting women in responding to TFCC, few of our practitioner participants contacted platforms or telecommunications companies for assistance. Some indicated they did not know what channels were available. Others described their past experiences seeking help from platforms or telecommunications companies as "unhelpful," "like banging your head against a wall… pointless." Consequently, they usually "don't bother [reaching out for assistance] now."

Workers noted that most of the women they served had tried to manage their own security using blocking and privacy settings before contacting domestic violence services. One worker joked that she did not believe it would be worth seeking assistance to take down abuse, harassment, or threatening messages on Facebook "unless someone is showing a nipple," which the workers suggested prompted a speedier response. Workers identified difficulties in accessing physical telecommunication store locations in non-metropolitan areas due to significant distances from services, refuges, or survivors' residences. Visiting telecommunication stores was almost impossible where women did not have a car or the abuser controlled access to the car. In many rural and regional areas, public transport networks are limited and private transport is expensive.

Advocates indicated that online forms were inadequate for women and workers to quickly contact platforms and telecommunication providers for assistance dealing with TFCC. Often, reports were submitted but no follow up communication was ever received, so the person reporting didn't know what action had been taken. Our practitioner participants requested clearer communication about what resources are available for survivors in regaining control of accounts, separating accounts, removing abusers from accounts, replacing phones, or accessing financial hardship allowances. Some advocates suggested a portal through which domestic violence services could inform telecommunication companies that a consumer was experiencing domestic violence, with the survivor's permission. Workers recommended that this notification could facilitate survivor access to assistance such as gathering login information and communication that could be used as evidence. Workers reported that women were not always aware of the ways perpetrators could use social media to attain information, such as via geotagging on images. Risks could be compounded by changes to standard settings and functions, such as when Snapchat launched their "find my friends" function with public location settings enabled. Practitioners thought telecommunication providers and platforms could take issues like domestic violence into consideration to improve overall service and safety.

Increased training and education

Across all focus groups conducted for this project, it was apparent that workers highly valued TFCC training and education. Practitioners recommended that education about domestic violence and TFCC should be incorporated into university curricula across programs like social work, criminology, law, and psychology. Most participants had completed the "brilliant" in-person training offered by WESNET. Some workers had also attended the in-person training offered by the Office of the eSafety Commissioner. Online resources and guides produced by WESNET, eSafety and Legal Aid New South Wales were also identified as helpful for advocates and survivors. They especially liked the checklists that were useful for completing safety audits.

While electronic resources were well regarded, in-person training was strongly preferred. The workers said trainers could help them walk through settings on their own devices, allowing them to ask questions in real time. Staff in regional, rural, and remote locations valued regional trainings, emphasising that it was difficult and expensive to travel to metropolitan locations for education programs. Although we had anticipated that services might prefer online trainings due to ease of access, participants reported that it was easier to commit to in-person sessions than online trainings which could always be deferred in the face of more urgent demands. They reported that in-person trainings could be run in different blocks so some staff could attend while others continued operation of the service.

Our participants reported that TFCC training is important because support workers perform the bulk of device and account checks. Workers noted that refuge staff had experienced increased workloads involving inspection of survivors' device settings and property to identify technology that could be used to identify locations or continue abuse. One worker suggested that "Ninety percent of women have no idea what [technology to facilitate stalking] is on there." Practitioners wanted ongoing training and frequently updated resources so they would be aware of evolving technology and risks. For example, one practitioner noted how a gaming console that was "always listening" had been used for surveillance purposes. Highlighting the critical role played by agencies offering training and resources, workers recommended that support and funding for these organisations and programs be increased.

Police training was also identified as essential for enhancing policy and practice. Mirroring findings in other research (George & Harris 2014), workers and survivors in our study had more positive perceptions of domestic violence specialist police officers than generalist officers. Specialist officers were said to have a better understanding the dynamics of domestic violence and TFCC. Workers noted that it was problematic when generalist officers did not offer guidance on or respond to abuse or harassment including breaches of intervention orders via ICTs. They reiterated that officers advising women to disengage from technology was inadequate and could increase their risk.

Advocates recommend that there be mandatory police training to aid the recognition, detection, and prevention of TFCC. Some workers described feeling as though they alone were responsible for managing women's safety via technology, wishing police were better able to advise survivors, refer them to other resources, and investigate TFCC crimes and breaches. Practitioners thought it was important that police be trained to understand how TFCC manifests in the context of domestic violence, its impact on survivors, and the heightened risks involved. They also recommended training to improve trauma-informed responses to abuse. For example, one worker explained that an understanding of trauma might help officers to understand how some technology-facilitated contact might seem innocuous to an outsider but be understood by a survivor as a serious threat.

Moreover, workers suggested that training could improve recognition of the dangers signalled by high volume contact and monitoring via technology. Workers suggested that such training would be beneficial for legal services and judicial officers, too. All of the workers reported ongoing confusion and a lack of consistency about what kinds of evidence are required by police and the courts and how best to provide it. Practitioners and survivors repeatedly stressed that officers would benefit from training about investigative strategies that can help police and courts to establish the sender of abusive communication. Almost all of our participants reported police refusing to follow up on abuse via ICTs, saying there was no way to know who had posted, texted, or called. However, basic investigative tactics exist to address this issue and they are regularly used to investigate other crimes.

Expansion of existing resources

All of the advocates reported growing awareness of training and other resources available to assist survivors with TFCC. As noted above, all of the practitioners had attended at least one of WESNET's trainings on domestic violence and technology or accessed the information and resources on their website. Although these were less familiar, perhaps because they are newer, several practitioners had also attended in-person trainings by the E-Safety Commission. All of the practitioners had also participated in or referred survivors to the SafeConnections program. The workers strongly recommend that the SafeConnections program administered by WESNET be continued and expanded. Under this scheme, Telstra provides safe smartphones, pre-paid credit, and information about safe use of devices to WESNET. WESNET distributes the resources to trained partner agencies across Australia who use them to assist survivors. Telstra also has a Pre-Paid Recharge Program, which provides pre-paid mobile recharge cards at no cost to agencies assisting survivors. Practitioners reported that these programs are an integral component of the safety and exit planning they facilitate with survivors. All of the practitioners said they would give out more of the SafeConnections phones and cards if they could.

Hands on technology safety checks

Practitioners indicated that they would love to have in-house staff who specialised in TFCC and could provide hands-on assistance to survivors individually or in groups. They indicated that this could be a partnership with IT organisations so that they could take on some of the work involved in responding to TFCC. One participant described a local auto mechanic that provided a technology safety check service. Some workers spoke about the potential of private agencies that could provide services such as checking devices for settings and spyware and sweeping vehicles and houses for recording and surveillance technologies. However, they emphasised that in practice, such services are paid for out of Victim Services stipends. They could be expensive, with one practitioner noting fees seemed to expand to match the funds awarded to crime victims. In addition, risks identified by private companies often required security solutions that were unaffordable. Given the impact of TFCC and difficulties in detecting covert surveillance, it is unsurprising that workers recommended more accessible and affordable support for technology safety checks. These would be beneficial in protecting and empowering survivors and lightening the load for specialised services with many other obligations.

Conclusion

Domestic violence is an important context for cybercrime and cybersecurity, requiring innovative responses. The threats to privacy, security, and safety recounted by our participants have different dynamics and patterns than those identified in Australian research on other forms of online crime and abuse. Accordingly, our findings point to different research and policy priorities.

Domestic violence abusers are insider threats who often gain access to accounts through intimate personal knowledge, sabotage, coercion, and physical force. Consequently, ordinary privacy and security measures are inadequate to ameliorate the threat. While most of the TFCC described in this study occurred post-separation, it often began before survivors knew their partner was abusive. As one practitioner put it, most women assume he "won't or can't do that and it is not until later when she realises he has been virtually standing beside her while she's been doing whatever she needed to do."

Significantly, survivor and practitioner participants stressed that cutting off ICT communication with abusers or getting off social media or the Internet can increase rather than decrease the risks to survivors and their loved ones. Many women who thwarted their abusers' communication or location tracking reported that these tactics resulted in the escalation of abuse, including widening the scope of harasment to include other family, friends, and co-workers.

In addition to learning about the types of abuse survivors experience, we documented key background factors that are essential for understanding the dynamics and risks of TFCC: the coercive and controlling relationship, pre- and post-separation abuse, co-parenting with abusers, the high cost of ICTs for consumers, and survivors' safety work.

Survivors in this study reported that, despite its non-physical nature, TFCC magnified and expanded the negative outcomes and trauma of domestic violence by rendering it ubiquitous and inescapable. Abusers' access via ICTs made it more difficult for survivors to leave and move on with their lives. TFCC is also frequently backed up by credible threats of violence and self-harm. Our participants stressed that TFCC increased their level of fear pre- and post-separation. In addition, they experienced the privacy invasions and interference in their ability to communicate using ICTs as rights violations and transgressions against their self-respect and dignity.

Despite the high visibility of domestic violence as a social problem in Australia, survivors and practitioners reported the persistence and prevalence of low levels of understanding of the dynamics and harms of coercive control. Survivors and practitioners observed that TFCC appeared to be minimised because of its non-physical nature. Practitioners and survivors thought that telecommunications staff, police, and courts could be better informed about the ways abusers might use ICTs in the context of domestic violence and the types of assistance survivors might need.

Based on this exploratory study, we make four recommendations for future action to address TFCC:

More training and education about technology-facilitated coercive control and tools to combat it

- Increase recognition of TFCC as a serious part of domestic violence.
- Mandate workplace training about TFCC for telecommunication companies, police, and courts.
- Provide required courses on domestic violence with content on TFCC in university programs such as psychology, criminology, social work, and law.
- More in-person training for workers who come into contact with domestic violence.
- Empowering consumer decision making by providing directly comparable information about resources for domestic violence survivors, 1300 call charges, policies for charging for phones destroyed in a crime.
- Improved consumer safeguards to protect privacy and facilitate release from contracts and family plans when domestic violence is an issue.

Enhanced affordability of telecommunication devices and service for domestic violence survivors

- Eliminate charges for changing and un-listing phone numbers due to TFCC.
- Release survivors from charges for phones that abusers have taken or destroyed.
- Offer financial hardship plans for domestic violence survivors unable to pay for phone contracts and plans.
- Recognising and responding to the digital divide.

Expansion of existing resources

- WESNET and Telstra SafeConnections program: making phones and credit available for survivors.
- More in-person training, including in rural, regional, and remote areas, updated and repeated periodically.
- Hands-on security checks for domestic violence services and survivors.

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 movements and activities and potential safety and privacy risks.
- Requiring telecommunications companies 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 action taken in response to complaints and establishing an appeal process.

These future actions could potentially improve responses to TFCC and help prevent future abuse. However, the reality is that safety and security risks will never be eliminated while abusers can force and coerce survivors to provide access to devices and accounts. The only way to ameliorate this risk is to alter the cultural and structural factors that engender domestic violence and entrap survivors in abusive relationships. An ecological approach targeting individuals, communities, corporations, culture, and governments is required to decrease risks due to domestic violence.

Survivors' efforts to manage TFCC using "compliant agency" by enduring certain forms of technological contact with abusers must be understood in the context of persistent and pervasive cultural norms minimising domestic violence and coercive control; structural factors that force women into ongoing contact with and financial dependency on abusers; and a more general failure to hold abusers accountable for abuse. As Mirza put it,

> **"Abused women employ a range of strategies throughout their marriages that reflect an awareness of their strengths, options, resources and limitations. These strategies show how women struggle to make the relationship non-violent and devise strategies to this end. Women react and reflect on the efficacy of these strategies, as well as the abusers' responses to them, and manoeuvre accordingly." (Mirza, 2018, p. 54)**

This means that improving responses to TFCC will require listening to women when they describe their experiences of abuse, resource and intervention needs, and safety and other concerns.

Future Research

This was the first qualitative study specifically designed to investigate women's experiences of technology-facilitated coercive control in Australia. Evidence about the role of technology is beginning to emerge as part of studies on domestic violence and technology-facilitated abuse in Australia. However, this study points to several directions where further research is required to better understand the problem and inform potential avenues for prevention and intervention. This exploratory study involved two states, Queensland and New South Wales. Approaches to domestic violence and resources available to survivors vary greatly across states and territories. National studies are needed to establish an evidence base to drive best practice around technology and abuse. These should include representative, quantitative studies and qualitative studies with survivors as well as key stakeholders in government, law, justice, social services, and essential infrastructure.

As in other areas of domestic and family violence research, more research is needed on TFCC in Indigenous communities. Research on cybersafety in remote Aboriginal communities indicates that factors such as living with extended family networks, limited mobile service, sharing devices and accounts, and unique cultural dynamics shape privacy and abuse risks (Rennie, Yunkaporta, & Holcombe-James, 2018). These may have implications for domestic and family violence. In addition, no research exists on technology-facilitated abuse in the Torres Strait Islands or Torres Strait Islander communities. Indigenous communities have the highest risks of harm due to domestic and family violence in Australia, yet knowledge in this area lags behind. Research led by Indigenous communities and researchers should be funded to begin to fill this gap.

Our research findings indicate that TFCC in the context of post-separation parenting was a particular problem for survivors. Most survivors who had voluntary or court-ordered contact with abusers reported having no meaningful way to stem TFCC. One participant noted her positive experience with a post-separation parenting communication app which saved all communication about the children. She reported that it helped control abusive communication. This example indicates that there can be technological solutions to TFCC. More research is needed about programs and apps that have been developed for or are potentially useful for domestic violence survivors.

Financial abuse is commonly recognised as an integral part of domestic violence. However, limited research has been conducted on it to date. Survivors and practitioners in this study mentioned forms of TFCC that are also likely financial abuse. They also noted the ways that TFCC can interfere with women's ability to earn a living if they have an online business. This is an area where much more research is needed.

While heterosexual men are disproportionately likely to be the perpetrators of domestic violence and women are disproportionately harmed by domestic violence, intimate partner abuse is not limited to heterosexual couples or female victims. Given the different risks of crime victimisation and patterns of differential access to resources for heterosexual and LGBTQ women and men, intimate partner abuse in same-sex couples and against men merits studies specifically designed to capture its unique dynamics. This is especially important given early survey research which indicates LGBT people face higher aggregated rates of online abuse. Future research on domestic violence in diverse couples would add to our knowledge about the lived experience and impact of the abuse in different contexts.

These findings can inform future research in other locations, with larger samples, and with additional cohorts of diverse survivors. It is the opinion of the authors that abuse in diverse relationships merits empirical research intentionally designed to uncover the dynamics of abuse in specific contexts. This research should be informed, as this study was, by empirical data on the particular dynamics and intersectional risk factors that shape abuse.

Recommendations

Recommendation 1:

More training and education about technology-facilitated coercive control and tools to combat it

- Increase recognition of TFCC as a serious part of domestic violence.
- Mandate workplace training about TFCC for telecommunication companies, police, and courts
- Provide required courses on domestic violence with content on TFCC in university programs such as psychology, criminology, social work, and law
- Enhanced platform and telco access and responsiveness
- More in-person training for workers who come into contact with domestic violence
- Empowering consumer decision making by providing directly comparable information about resources for domestic violence survivors, 1300 call charges, policies for charging for phones destroyed in a crime
- Improved consumer safeguards to protect privacy and facilitate release from contracts and family plans when domestic violence is an issue

Recommendation 2:

Enhanced affordability of telecommunication devices and service for domestic violence survivors

- Eliminate charges for changing and un-listing phone numbers due to TFCC
- Release survivors from charges for phones that abusers have taken or destroyed
- Offer financial hardship plans for domestic violence survivors unable to pay for phone contracts and plans
- Recognising and responding to the digital divide

Recommendation 3:

Expansion of existing resources

- WESNET and Telstra SafeConnections program: making phones and credit available for survivors
- More in-person training, including in rural, regional, and remote areas, updated and repeated periodically
- Hands-on security checks for domestic violence services and survivors

Recommendation 4:

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 movements and activities and potential safety and privacy risks
- Requiring telecommunications companies 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 action taken in response to complaints and establishing an appeal process

Authors

Helen Campbell

OAM is the Executive Officer of Women's Legal Service NSW. She is a lawyer with over 20 years' experience in the community and public sectors. In addition to her legal qualifications she is a Master of Women's Studies and holds a Diploma in Frontline Management. Previously Helen managed Redfern Legal Centre, and has also held a wide range of voluntary appointments including Community Legal Centres NSW, Rape and Domestic Violence Services Australia and the Women's Justice Network. In 2011 Helen was awarded a medal in the Order of Australia for services to the law and to the community of Redfern.

Molly Dragiewicz

is Associate Professor in the School of Justice, Faculty of Law at Queensland University of Technology in Brisbane, Australia. Dragiewicz is an internationally award-winning criminologist whose research focuses on violence and gender. She won the 2018 Domestic Violence Prevention Leadership Award from the Domestic Violence Prevention Centre Gold Coast; the 2017 Robert Jerin Book of the Year Award for ***Abusive endings: Separation and divorce violence against women*** from the American Society of Criminology Division on Victimology; the 2012 Critical Criminologist of the Year Award from the American Society of Criminology Division on Critical Criminology; the 2009 New Scholar Award from the American Society of Criminology Division on Women and Crime; and the QUT Vice Chancellor's Performance Award in 2016. Dragiewicz is author of Abusive endings: Separation and divorce violence against women (2017) with Walter DeKeseredy and Martin Schwartz; author of ***Equality with a vengeance: Men's rights groups, battered women, and antifeminist backlash(2011), editor of Global human trafficking: Critical issues and contexts (2015),*** editor of ***The Routledge handbook of critical criminology (2012, 2nd ed. 2018),*** and editor of ***The Routledge major works collection: Critical criminology (2014)*** with Walter DeKeseredy.

Helen Easton

Helen Easton is an independent researcher and consultant based in Sydney. She has recently returned to Australia after a period of 18 years in London as an academic, researcher and policy advisor in a range of roles, most recently as Senior Research Fellow and Senior Lecturer in Criminology at London South Bank University. In this role Helen conducted research for the Scottish Equality and Human Rights Commission on the experiences of people trafficked for the purposes of commercial sexual exploitation; for the Ministry of Justice, evaluating the pilot of conditional cautions for women offenders; for the Northern Ireland Office evaluating the Inspire Women's Project and for the Scottish Executive evaluating the work of the 218 Women's Project. Helen has also conducted research on a range of topics including the effectiveness of the Prolific and Priority Offender scheme, fear of crime, the outcomes of anti-social behaviour orders, and alcohol related violence and disorder. Helen's current research focus is violence against women and girls, women's desistence from offending and women exiting prostitution. Her book ***Exiting Prostitution (2014)*** has informed efforts to reform the legal frameworks relating to prostitution in England and Wales, Scotland and Northern Ireland. Since her return to Australia in 2018 Helen has worked with the NSW Law and Justice Foundation evaluating a pilot scheme to improve access to justice in remote, regional and rural communities in NSW. She is currently working with the Centre for Women's Justice in London on a project examining the operation of legal defences for women who kill violent men while completing her PhD in Law at Macquarie University.

Bridget Harris

is an early career researcher and member of the Crime, Justice and Social Democracy Research Centre; and, Law Lab in Technology, Regulation and Justice at Queensland University of Technology, as well as an Adjunct Lecturer in Criminology at the University of New England. She is currently completing the Criminology Research Grant (under the auspices of the AIC - the Australian Institute of Criminology) Spaceless Violence and Advocacy: Technology-facilitated Abuse, Stalking and Service Provision in Australia with Delanie Woodlock, Women's Legal Service New South Wales, and Professor Harry Blagg. Harris is the lead editor (with Woodlock) of ***Technology and Domestic Violence: Experiences, Perpetration and Responses***, to be published by Routledge in 2021. Her study (with George, in 2014) ***Landscapes of Violence: Women Surviving Family Violence in Regional and Rural Victoria*** was the first research, internationally, to explore the dynamics and impacts of and responses to TFCC in different geographic landscapes.

Jhan Leach

Is Executive Officer of Blacktown Women's and Girls Health Centre and the North Western Sydney Women's Domestic Violence Court Advocacy Service. She sits on the Board of Women's Health NSW and on the Blacktown City Council Women's Advisory Committee. She's a teacher with a Master of Art Education, a Diploma of Art Education and a Diploma of Fine Art. She is a survivor of domestic violence and sexual abuse who has empowered women and communities to 'break the silence of abuse'. She's lectured on 'art as therapy', at the University of NSW COFA and continues to share her skills and knowledge as an artist, survivor and educator with students on placement, from Western Sydney University. During her 30 year career, in the community welfare sector, she's enabled women and girls to come together and share an experience of healing using 'art as therapy' and has engaged broadly, both locally and nationally, through the media, to champion the rights of women and children victims and survivors of domestic violence and sexual abuse. She's collaborated and facilitated with the Royal Women's Hospital Randwick, Midwifery Department, facilitating 'art as therapy', support groups for Culturally and Linguistically Diverse Mothers, holding an exhibition of their artworks at the Royal Women's Hospital Randwick and presented the findings at conferences in Sydney and Melbourne. Facilitated the "Women's Art Expression and Empowerment Groups" using 'Art as Therapy', resulting in six exhibitions at the Bondi Pavilion, the Royal Hospital for Women at Paddington and the Mascot and Waverley Libraries. Jhan's passion about "breaking the silence of abuse," resulted in artworks from these group being donated to the State Library in Sydney. In 2016 she won "The Heart of the Community Award" and dedicated the award to her mother who was a survivor of domestic violence abuse from her father.

Authors

Angela Lynch

is the CEO of the Women's Legal Service (WLS) and across her 24 years with the service has made significant front-line contributions to the prevention of domestic and sexual violence. At a national level, Angela has been a board member of the Women's Legal Services Australia (WLSA) network for 12 years. During this time Angela was national law reform coordinator for two tenures, led the development of law reform submissions and represented WLSA before federal parliamentary committees. Angela's expertise has been recognised through her appointment to the Queensland Domestic and Family Violence Death Review and Advisory Board and the Queensland Government Sexual Violence Roundtable. Angela was awarded the 2017 Women's Agenda leadership in the legal sector award and the Lawyer's Weekly 2017 Not for Profit Lawyer of the Year and the Women in Law excellence award and a Member of the Order of Australia award this year.

Lulu Milne

is the Principal Social Worker at Women's Legal Service Qld, where she supervises a small team of social workers and provides holistic services to women who are experiencing domestic violence and engaging in the legal system. She has over 15 years experience in the domestic violence and homeless sectors.

Michael Salter

is a Scientia Fellow and Associate Professor of Criminology at the University of New South Wales. His research is focused on the criminological aspects of complex trauma, including violence against women, technologically-facilitated abuse and the sexual exploitation of children. His published work includes the books ***Organised Sexual Abuse*** (2013, Routledge) and ***Crime, Justice and Social Media*** (2017, Routledge). He sits on the Board of Directors of the International Society for the Study of Trauma and Dissociation, who awarded him the 2018 Morton Prince Award for Scientific Achievement. Current research projects include a study funded by the Australia's National Research Office for Women's Safety on women's experiences of complex trauma and existing service responses, and a study funded by the Australian Centre to Counter Child Exploitation that analyses the role of parents in producing child exploitation material of their children.

Delanie Woodlock

is an independent scholar and Adjunct Lecturer in Criminology, University of New England. She is a pioneering researcher who has studied technology-facilitated abuse and stalking under a previous ACCAN project and is currently involved in an AIC study on technology and domestic violence in rural and regional areas with Dr Harris. She has extensive networks in the domestic violence, legal and women's health sectors and has worked in community organisations in the areas of research, evaluation and policy.

References

ACCAN. (2019). No Australian left offline: Affordable broadband for all. Australians. Retrieved from http://accan.org.au/files/Affordability/No%20Australian%20Left%20Offline.pdf

ACMA. (2014). *Mobile calls to 13 numbers: Research report*. Retrieved from Australian Government, Australian Communications and Media Authority website: https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/ACMA-13-research-report_July-2014-pdf.pdf?la=en

Australian Institute of Health and Welfare. (2018). *Family, domestic and sexual violence in Australia*. Canberra: Australian Government.

Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era: Final report*. Sydney, NSW.

Australian Government, & Department of Social Services. (2016). *Third Action Plan 2016-2019 of the National Plan to Reduce Violence Against Women and their Children 2010-2022*. Canberra: Department of Social Services, Commonwealth of Australia.

Baym, N. K. (2015). *Personal connections in the digital age* (2nd ed.). Malden, MA: Polity.

Brown, C., & Hegarty, K. (2018). Digital dating abuse measures: A critical review. *Aggression and Violent Behavior*, *40*, 44–59. https://doi.org/10.1016/j.avb.2018.03.003

Bryant, W., & Bricknell, S. (2017). *Homicide in Australia 2012–13 to 2013–14: National homicide monitoring program report (No. 2)*. Canberra: Australian Institute of Criminology.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N. McCoy, Damon, Ristenpart, T. (2018). The spyware used in intimate partner violence. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 1–18). San Francisco: IEEE.

Citron, D.K. 2014. *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press.

Council of Australian Governments (COAG). (2016). *COAG 2016 national summit on reducing violence against women and their children: Outcomes and reflections*. Canberra: COAG.

Curtin, J. (2001-2002). A digital divide in rural and regional Australia. *Current Issues Brief 1.* Retrived from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/cib0102/02CIB01

Domestic and Family Violence Death Review and Advisory Board. (2017). *Domestic and Family Violence Death Review and Advisory Board*. Brisbane: Domestic and Family Violence Death Review and Advisory Board.

DeKeseredy, W. S., Dragiewicz, M., & Schwartz, M. D. (2017). *Abusive endings: Separation and divorce violence against women*. Oakland, CA: Univ 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. https://doi.org/10.1016/j.intcom.2011.04.006

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, *Online first*, 1–20.

Dragiewicz, M. (2009). Why sex and gender matter in domestic violence research and advocacy. In E. Stark & E. Buzawa (Eds.), *Violence against women in families and relationships: Vol. 3 Criminal justice and the law* (pp. 201–215). Santa Barbara, CA: Praeger.

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. https://doi.org/10.1080/14680777.2018.1447341

References

Dragiewicz, M., Woodlock, D., Harris, B. A., & Reid, C. (2019). Technology-facilitated coercive control. In W. S. DeKeseredy, C. M. Rennison, & A. K. Hall-Sanchez (Eds.), *The Routledge international handbook of violence studies* (pp. 244–253). New York: Routledge.

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

Filipovic, J. (2007). Blogging while female: How Internet misogyny parallels real-world harassment. *Yale Journal of Law and Feminism*, *19*, 295–304.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders. In *Proceedings ACM Human-Computer Interaction* (Vol. 1, pp. 46:1-46:22). https://doi.org/10.1145/3134681

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). A stalker's paradise: How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (pp. 1–13). Montreal QC, Canada: ACM Press. https://doi.org/10.1145/3173574.3174241

The Futures Company. (2014). *2014 Teen Internet safety survey*. Cox Communications. https://www.cox.com/content/dam/cox/aboutus/documents/tween-internet-safety-survey.pdf.

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

Goode, S. (2017). *Identity theft and Australian telecommunications: Case analysis*. Sydney: Australian Communications Consumer Action Network.

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.

Harris, B.A. (forthcoming, 2020). Technology, spatiality and violence against women. In S. Walklate, K. Fitzgibbon, J. McCulloch & J.M. Maher (Eds.), *Emerald handbook on feminism, criminology and social change.* Great Britain: Emerald.

Harris, B. (2018). Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice. In K. Fitz-Gibbon, S. Walklate, J. McCullough, & J. Maher (Eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52–70). London: Routledge.

Harris, B. (2016). Violent landscapes: A spatial study of family violence. In A. Harkness, B. Harris & D. Baker (Eds.), *Locating crime in context and place: Perspectives on regional, rural and remote Australia* (pp. 70-84). Sydney: The Federation Press.

Harris, B. A., & Woodlock, D. (2018). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, *Online first*, 1–21. https://doi.org/doi:10.1093/bjc/azy052

Hayes, B. E. (2013). Women's resistance strategies in abusive relationships: An alternative framework. *SAGE Open*, *3*(3). https://doi.org/10.1177/2158244013501154

Hayes, R. M., & Dragiewicz, M. (2018). Unsolicited dick pics: Erotica, exhibitionism or entitlement? *Women's Studies International Forum*, *71*, 114–120. https://doi.org/10.1016/j.wsif.2018.07.001

Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, *19*(6), 565–581. https://doi.org/10.1080/15614263.2018.1507892

Henry, N., Powell, A., & Flynn, A. (2017). Not just 'revenge pornography': Australians' experiences of image-based abuse, a summary report. Melbourne: RMIT University.

Kandiyoti, D. (1988). Bargaining with patriarchy. *Gender & Society*, *2*(3), 274–290. https://doi.org/10.1177/089124388002003004

Kelly, L. 1988. *Surviving sexual violence*. Oxford: Polity Press.

Kids Helpline. (2017). Sexting. Retrieved April 28, 2019. Retrieved from https://kidshelpline.com.au/teens/issues/sexting

Kim, C. (2015). Credit cards: Weapons for domestic violence. *Duke Journal of Gender Law & Policy*, *22*, 281–309.

Lenhart, A., Duggan, M. & Smith, A. (2014). Couples, the Internet and social media: How American couples use digital technology to manage life, logistics, and emotional intimacy within their relationships. Retrieved from http://pewinternet.org/Reports/2014/Couples-and-the-internet.aspx

Littwin, A. (2012). Coerced debt: The role of consumer credit in domestic violence. *California Law Review*, *100*(4), 951–1026.

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter. *Safe: The Domestic Abuse Quarterly*, *63*, 22–26. https://doi.org/10.2139/ssrn.3350615

Meyer, S. (2010). *Responding to intimate partner violence victimisation: Effective options for help-seeking* (No. 389; pp. 1–6). Canberra: Australian Institute of Criminology.

Meyer, S. (2011). Seeking help for intimate partner violence victims' experiences when approaching the criminal justice system for IPV-related support and protection in an Australian jurisdiction. *Feminist Criminology*, *6*(4), 268–290. https://doi.org/10.1177/1557085111414860

Mirza, N. (2018). Reframing agency in abusive contexts: Beyond "free choice" and "open resistance." *Journal of Gender-Based Violence*, *2*(1), 41–56. https://doi.org/10.1332/239868017X15127297709475

Phillips, W. (2015). This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture. Cambridge, MA & London: MIT Press.

Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In W. S. DeKeseredy & M. Dragiewicz (Eds.), *The Routledge handbook of critical criminology* (2nd ed., pp. 305–315). London, UK: Routledge.

Pratt, M. K. (2005). What is ICT (information and communications technology, or technologies)? Retrieved from https://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies

PricewaterhouseCoopers, OurWatch & VicHealth. (2015). *A high price to pay: The economic case for preventing violence against women*. Victoria: PricewaterhouseCoopers, OurWatch, VicHealth.

Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). Snooping and sexting: Digital media as a context for dating aggression and abuse among college students. *Violence Against Women*, *22*(13), 1556–1576.

Rennie, E., Yunkaporta, T., & Holcombe-James, I. (2018). *Cyber safety in remote Aboriginal communities: Final report*. Retrieved from Digital Ethnography Research Centre, RMIT University website: http://apo.org.au/node/172076

Rooksby, E., Weckert, J., & Lucas, R. (2007). The digital divide in Australia: Is rural Australia losing out? In E. Rooksby & J. Weckert (Eds.), *Information technology and social justice* (pp. 240-261). Hershey: Information Science Publishing.

Royal Commission into Family Violence. (2016). *Royal Commission into Family Violence: Summary and recommendations.* Victoria: Royal Commission into Family Violence.

Salter, M. (2016). Privates in the online public: Sex(ting) and reputation on social media. *New Media & Society*, 18(11), 2723-2739.

Salter, M. (2018). From geek masculinity to Gamergate: the technological rationality of online abuse. *Crime, Media, Culture*, 14(2), 247-264.

Salter, M., Crofts, T., & Lee, M. (2013). Beyond criminalisation and responsibilisation: Sexting, gender and young people. *Current Issues in Criminal Justice*, 24(3), 301–316.

Sharp-Jeffs, N., Kelly, L., & Klein, R. (2018). Long journeys toward freedom: The relationship between coercive control and space for action—measurement and emerging evidence. *Violence Against Women*, *24*(2), 163–185. https://doi.org/10.1177/1077801216686199

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). *Fifteen minutes of unwanted fame: Detecting and characterizing doxing*. 432–444. https://doi.org/10.1145/3131365.3131385

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence Against Women*, *13*(8), 842–856. https://doi.org/10.1177/1077801207302045

References

Stanko, E. (1990). ***Everyday violence: How women and men experience sexual and physical danger***. London: Pandora.

Stark, E., & Hester, M. (2019). Coercive control: Update and review. ***Violence Against Women***, ***25***(1), 81–104. https://doi.org/10.1177/1077801218816191

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. https://doi.org/10.1002/poi3.185

Vera-Gray, F. (2016), ***Men's intrusion, women's embodiment: A critical analysis of street harassment***. London: Routledge.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. ***Security Journal***, ***26***(2), 107–124. https://doi.org/10.1057/sj.2012.1

WESNET. (2000). ***Domestic violence in regional Australia: A literature review***. Australia: WESNET.

World Health Organization. (2009). Promoting gender equality to prevent violence against women. Retrieved from: https://www.parliament.vic.gov.au/file_uploads/3_RFV_320ppA4_ReportRecommendations_VolumeIII.WEB_9F6w0Y9c.pdf

Woodlock, D., McKenzie, M., Western, D., & Harris, B.A. (forthcoming, 2019). Technology as a weapon in domestic violence: Responding to digital coercive control. ***Australian Social Work.***

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

Woodlock, D. (2015). ***ReCharge***. Unpublished raw data.

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

Ybarra, M. L., Price-Feeney, M., Lenhart, A., & Zickuhr, K. (2017). ***Intimate partner digital abuse***. New York, NY: Data & Society Research Institute, Center for Innovative Public Health Research.

Domestic violence and communication technology

Survivor experiences of intrusion, surveillance, and identity crime

Queensland University of Technology

Australian Communications Consumer Action Network