Original Research Article

Violence Against Women
1–23
© The Author(s) 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/10778012221088310
journals.sagepub.com/home/vaw
SAGE

Technology-Based Responses to Technology-Facilitated Domestic and Family Violence: An Overview of the Limits and Possibilities of Tech-Based "Solutions"

Diarmaid Harkin[1] and Robert Merkel[2]

Abstract

It is increasingly common for domestic and family violence to have an element of technology-facilitated abuse (TFA). As a result, technology-based responses have emerged to address TFA. Using observations from several empirical research projects into TFA, it will be shown that technology-based responses are necessary without being sufficient, and that they have persistent limitations that need to be recognized. Relatedly, it will be argued that there should be an ongoing emphasis on the development of human resources as a support for those experiencing TFA, particularly the use of professional DV support workers.

Keywords

domestic and family violence, intimate partner abuse, technology-facilitated abuse, technology-facilitated responses to abuse, safety by design, support workers

Introduction

Survey data with Australian domestic and family violence (DFV) organizations suggest that 99.3% of frontline support workers have clients who experience some form of technology-facilitated abuse (TFA) (see Woodlock et al., 2020). It

[1]Faculty of Arts and Education, Deakin University, Waurn Ponds, Victoria, Australia
[2]Independent Researcher

Corresponding Author:
Diarmaid Harkin, Faculty of Arts and Education, Deakin University, 75 Pigdons Road, Waurn Ponds, Victoria 3216, Australia.
Email: diarmaid.harkin@deakin.edu.au

is increasingly clear that many circumstances of DFV have a technological component and, as outlined by Eterovic-Soric et al. (2017), abusers utilize a wide variety of technology to track, harass, stalk, intimidate, manipulate, and "gaslight" their targets. This can include using GPS trackers, hidden cameras, social media, spyware, nonconsensual image-based abuse, and a range of other niche technology-facilitated attacks such as harnessing Bluetooth capabilities to "AirDrop" unwanted files and images (Eterovic-Soric et al., 2017, p. 282). Moreover, the types of technology-facilitated abuse are expanding and diversifying as new technological developments offer new opportunities. The growth of consumer "IoT" (the internet of things) is a particular area of concern for intimate partner abuse (Lopez-Neira et al., 2019; Tanczer et al., 2018). New opportunities for abuse are constantly emerging while existing tools and services such as "ip stressors," item-trackers, or "remote access management tools" are easily adapted for hostile purposes, while other developments such as the rise of "deep-fakes" are similarly worrisome (Dodge & Johnstone, 2019).

The full range of potential technological threats are becoming harder to exhaustively track and TFA is causing considerable problems for victim-survivors of DFV including psychological harm (Mandau, 2020; Stevens et al., 2020), while also facilitating physical abuse and homicide (Citron, 2015, Todd et al., 2021). Criminal justice responses to TFA are not progressing adequately, with an Australian study suggesting that some victim-survivors of TFA are still "not taken seriously" by police (Harris & Woodlock, 2019, p. 531). Furthermore, support workers in DFV advocacy organizations around the world are similarly struggling to respond to TFA (Freed et al., 2017; Lopez-Neira et al., 2019; Tanczer et al., 2021). TFA can often outstrip the technical knowledge of those who work in the DFV advocacy sector, with many in the sector not having the skills or abilities to diagnose and suitably respond to various forms of TFA.

Although a variety of responses to TFA are facing challenges, this article is focused on the specific development of technology-based responses to TFA. A number of authors have discussed the potential of using technology as a means of "fighting fire with fire" (Al-Alosi, 2020) or "stalking the stalkers" (Eterovic-Soric et al., 2017). It is emphasized how "innovative uses of technology" (Al-Alosi, 2020, p. 1) can help protect victim-survivors and there is a "need for technologies which empower victims" (Eterovic-Soric et al., 2017, p. 284). Technology in this regard is discussed as offering a range of potential solutions, responses, aids, "fixes," or opportunities for combatting TFA and supporting the needs of victim-survivors. This article explores this idea further. Although this article does not intend to dispute or undermine the potential of using technology for these purposes, it also wishes to highlight limitations and persistent shortcomings of the capacities and strategic value of technology-based responses.

There has been a range of technology-based responses to TFA that have been implemented, trialed, or explored by a variety of actors in recent years. For instance, there is a growing set of online websites aimed at providing specific advice and information about TFA; this includes examples such as the NGO

"Chayn" providing "DIY Online Safety" (Chayn, 2021a), or the Office of the eSafety Commissioner in Australia providing a range of resources aimed at educating women about "online safety planning" and various tech-based threats (eSafety, 2021a). The Office of the eSafety Commissioner also provides an online portal for reporting image-based abuse to assist with takedown efforts (eSafety, 2021b). Other technology-facilitated responses include the development of Kaspersky's "TinyCheck," a spyware-detection tool (Ruiz, 2021), and there is the promotion of "technology design principles" to combat domestic abuse (IBM, 2020). "Bug detectors" are also used to attempt to find tracking devices (see Harkin, 2020). These and many other examples represent efforts to harness technology to respond to TFA.

With technology-based responses gathering momentum, it is an opportune moment to reflect and take stock of the strategic value of this type of approach. These approaches have emerged to supplement and operate alongside existing support provision from the criminal justice system and DFV support organizations, and it is useful to consider how they should be embedded within and work alongside established forms of support. As will be argued in this article, due to the many limitations of technology-based responses, there is a need for a sustained and ongoing commitment to providing human resources to respond to TFA-related DFV, particularly the use of DFV support workers and organizations. There are a number of distinct advantages to investing in well-skilled professional support workers when compared against "tech" related responses.

To prosecute this argument, this article will proceed through several steps. First, it will be outlined how the observations, conclusions, and reflections featured in this article have emerged from several original and empirical studies into TFA. Second, the article will organize a range of technology-based responses into categories to enable discussion of shared limitations and strategic issues. These categories are (a) *tech-supported information provision*, which includes developments such as the emergence of sizable online "digital safety" guides; (b) *efforts to "design out" abuse*, which includes efforts to implement "safety/privacy by design" of different technological devices or platforms; (c) *developing and applying tailored, circumstantial tech solutions*, which includes a miscellaneous range of efforts to provide responses such as purposefully designed spyware detection tools and the use of "bug detector" scanners; and (d) *tech-supported reporting or connecting with services* which include a number of apps developed to allow victim-survivors to take notes or connect with support services.

Third, after reflecting on the various shortcomings and persistent limitations of addressing TFA through the various categories of technology-based responses, a number of "meta-reflections" will be provided regarding the wisdom of using technology-based responses to the issue of TFA. Ultimately, an argument will be made that the use of human resources and support services will continue to be a vital and persistent backbone for best serving the interests of DFV victim-survivors regardless of the ongoing development of new technological threats or new technology-based response tactics.

A Note on Methods

The findings, observations, and original data presented in this article come from empirical projects the authors have been involved with over the past few years. Each of these projects focused on TFA in the context of DFV with an emphasis on the technological aspects of the abuse. The authors have separately and collaboratively worked on projects that variously scrutinized the technical elements of TFA and how these can be addressed and undermined, and how the needs of victim-survivors may best be served. This has included a project into the consumer spyware industry, research into private security companies working with victims of domestic violence, a collaborative project funded by the *Office of the eSafety Commissioner* into Australia's responses to TFA, and a project examining the security standards of apps deployed by DFV organizations throughout Australia. The arguments from this article have emerged from reflections extracted from each of these projects. Further methodological detail for each of these studies will now be provided:

Private Security Companies Working with Victims of Domestic Violence

As principally outlined in Harkin (2020), private security companies are being contracted by certain DFV organizations (and government funders) to provide services for victim-survivors in Australia. A common aspect of this response involves "technical solutions" to issues of tracking, surveillance, stalking, and other forms of TFA. For instance, certain companies provide "bug-sweeping" services to search for GPS trackers, hidden cameras, and other malicious "bugs" (see Harkin, 2020, pp. 77–80). This is in addition to the provision of advice on spyware detection and other forms of cyber-security advice from private security companies (p. 80). Security companies also may encourage the deployment of CCTV or person duress alarms as tech-based responses to DFV (pp. 65–77). That research spoke with 90 key stakeholders in Australia including 15 victim-survivors, and a variety of representatives from government, DFV organizations, private security companies, and police. The research inquiry was primarily focused on the risks and benefits of private security companies working with victim-survivors, but also gathered pertinent data on the issue of technology-based responses deployed by private security companies and the positive and negative impacts they created (pp. 63–96).

Consumer Spyware Industry

Molnar and Harkin (2019) outline an investigation into the threats of consumer spyware. It explored the industry developing products that aid DFV perpetrators instalking and "spying" (see also Harkin & Molnar, 2020; Harkin et al., 2019). The research targeted nine different spyware products and subjected them to both "user analysis," whereby the researchers purchased and deployed the spyware on Android and iOS phones for the purposes of viewing how the spyware operates from the perspective of the abuser and the "target," and also to "technical analysis" that was sub contracted to the cyber-security consultancy group *HackLabs* (Australia). This research provided unique insights into the types of spyware being sold on the consumer market, the pathways it relies on to get into smartphones, and the comparable vulnerabilities of Android devices compared with iOS (Harkin & Molnar, 2020). The research also produced advice materials for combatting spyware for the Women's Services Network (WESNET) that was hosted on their website.

Australian Responses to TFA (Funded by the Office of the eSafety Commissioner)

In 2020, the authors undertook research for the Office of the eSafety Commissioner, alongside a number of collaborators, to produce two reports (not currently published). The first report examined the content of the *eSafety Women's* online safety guidance around TFA, and the second report explored a range of TFA-based threats and the potential strategic and policy responses to improving responses to TFA in Australia. Relevant aspects of that project to this article included exhaustively reviewing the range and detail of advice provided by *eSafety Women's* online digital safety guidance. The team also undertook original empirical research, including a hands-on assessment of 13 consumer IoT devices. Aimed at sampling a range of consumer IoT available at common high street technology stores, the team purchased a number of devices and scrutinized their functioning with attention to how the devices could create vulnerabilities for victim-survivors or allow abusers to leverage abuse (see Harkin et al., 2020a).

This project also offered a chance to further explore the credentials of "debugging equipment." One of the authors had previous experience with exploring the viability of using "debugging equipment" to uncover hidden forms of surveillance (see Harkin et al., 2018). Further efforts were taken to test the type of equipment often used by private security companies to "debug" property. A number of professional-grade "bug detectors" were purchased to then assess their ability to detect the radio emissions of a sample of items that could potentially be used for surreptitious surveillance of an intimate partner. This included testing the ability to detect a variety of IoT devices such as doorbells and home digital surveillance cameras, a selection of "hidden camera" devices purchased from surveillance equipment vendors, and an item-tracking device.

Similarly, this project engaged in some preliminary analysis of the *IPV Spyware Discovery Tool* (ISDi) developed by the "IPV Tech Research" team at Cornell Tech, Cornell University, and New York Univerity. The analysis focused primarily on whether the tool in its present form could be usefully deployed by frontline DV organizations. The process of installing ISDi on a variety of desktop computers was explored and scans were run on Android and iOS phones (with consumer spyware installed on some of the phones).

Testing Apps Deployed by Domestic Violence Advocacy Organizations

In 2020, Merkel participated in research to review mobile apps specifically designed for survivors of DFV (WESNET, 2020). The primary goal of the research was to provide consumer-facing reviews to assist survivors and frontline workers in choosing apps that best meet their needs. In addition to examining the apps' privacy policies and user-visible behavior, "reverse engineering" techniques (Chikofsky & Cross, 1990) were used by Merkel to determine how and where the apps stored and transferred information. The primary outputs from this project were consumer-facing reviews; however, security concerns about several apps were identified and raised directly with sponsoring organizations and developers.

This article thus offers cumulative observations from the above-mentioned studies. Each of these studies attempted to explore, identify, develop, or improve tech-facilitated solutions to TFA and therefore offer a unique perspective on the overall prospects of tech-based responses to TFA. The authors have been able to identify common shortcomings and limitations, but also the potential benefits of developing further tech-based responses. The following sections unpack the perspectives that have emerged from these multiple projects by attempting to categorize various tech-based responses and explore their respective challenges.

Technology-Based Response A: Tech-Supported Information Provision

The first type of technology-based response that is worth exploring is the rise of mechanisms to provide information about TFA using detailed websites or online resources. As mentioned earlier, a number of websites now provide information aimed at a combination of victim-survivors of TFA, those who work in the domestic and family violence advocacy sector, and general audiences of women who may be concerned about digital safety. Prime examples include the *Office of the eSafety Commissioner's* "eSafety Women" website (eSafety, 2021a) and the "DIY Online Safety" guide provided by the UK-registered NGO *Chayn* (Chayn, 2021a). These online repositories of information aim to provide detailed practical advice on a range of capabilities including how to protect privacy online, how to secure your devices, how to secure online accounts, and how to detect whether an abusive party has compromised an account or a device. A growing number of resources can be found online specifically tailored for TFA that provide detailed defensive instructions including other examples such as the "how-to guides" produced by the Cornell Tech-affiliated *Clinic to End Tech Abuse* (CETA, 2021a), WESNET's *Women's Technology Safety and Privacy Toolkit* (WESNET, 2021), and the National Network to End Domestic Violence's *Technology Safety and Privacy: A Toolkit for Survivors* (NNEDV, 2021).

These guides are characterized by attempts to provide readers with tips, strategies, details, or advice about specific threats and how to respond to them. They aim to cover a wide range of possible risks, accounting for a diverse range of platforms, devices, and accounts. On many occasions, these guides go into great detail about how to change settings on a device or an online account. Examples of this include the step-by-step guidance on how to check if an unwanted party may have accessed the iCloud account of an iPhone/Apple user (CETA, 2021b), how to change privacy settings on Instagram (eSafety, 2021c), or how to setup auto-recording of voice calls on an

Android phone (Chayn, 2021b). The presumed goal of each of these guides is that a victim-survivor will encounter this guide online and thus implement a partial “DIY” solution to a potential digital threat, or someone who is working to support a victim-survivor can utilize the information on their behalf (a worker in a DFV advocacy organization, for example).

Although these efforts to directly up-skill and inform victim-survivors (or support workers) of digital threats and how to respond to them are admirable and have potential use-value for certain individuals in particular circumstances, they also have a number of limitations that need to be recognized. There are some obvious challenges with this approach, such as keeping the details up-to-date as the respective platforms, applications, and devices make changes to menus, interfaces, and the functioning of their products. It takes a lot of labor and commitment to continually renew online text or video guides that are aiming to be sufficiently detailed to offer a practical impact. This type of information expires relatively quickly and could only be addressed through an ongoing effort to ensure all guidance is updated and accurate over a long period of time. The effort to conduct such a task should not be underestimated and it’s unlikely that any single organization or group, whether it is government-funded, an NGO, or an academic endeavor, would make the continued investment required to perform such a role over the long term.

Furthermore, information resources must not only account for new details or product updates but also account for the ever-expanding risks of TFA from new technological developments, services, or platforms. Taking the offerings of the eSafety Women website as an example, the authors conducted an audit in early 2020 of the range of issues of TFA that the online guidance addresses and identified a number of gaps. Although the eSafety Women website covered a wide range of potential TFA threats and has a substantial, detailed library of “how to” videos, checklists, quizzes, and information on TFA, it still could not account for the full variety of technology-facilitated forms of abuse that are possible or have been observed in the field. Specific gaps included a lack of mention of consumer “internet of things” devices that are a growing vector of abuse (Lopez-Neira et al., 2019; Tanczer et al., 2018), including incidents where abusers have used “smart” features in modern cars to track victim-survivors (see e.g., Bevin, 2019). Some other gaps included issues relating to tracking with item-finder devices such as “Tile,” the rise of “deep-fakes” as an instrument of abuse (Scott, 2020), malicious online services-for-hire such as “IP Stressors,” family monitoring software that often comes packaged within anti-virus software suites such as Norton Family, and use of drones (see Harkin et al., 2020b). This is not to undermine or criticize the considerable efforts of organizations such as the *Office of the eSafety Commissioner*, but to highlight that the in-the-field circumstances of TFA are evolving and expanding at a rate that makes it practically impossible for online information guides to address all the possible threats that exist for victim-survivors. In other words, the technological ecosystem in which victim-survivors are living is becoming more complicated and at a rate that outstrips the ability of organizations to adequately catalog and prepare “how to” guides as a response.

Additionally, when engaging with much of the detail provided in the "how to" guides, a new dilemma presents itself. On any given issue—for example, when instructing someone on the threats of spyware—many of the guides did not provide adequate detail on the full range of different spyware threats and how to address each of them. But if an organization was to attempt to provide the full articulated guidance of how to diagnose whether or not spyware is present on a device, it would inevitably provide too much information to the point that it is unlikely to be consumable by its intended audiences. As it stands, some of the online guides have such a volume of material and content that it is unlikely that victim-survivors (or advocates who work with victim-survivors) could reasonably be expected to digest all the information, and yet, on many of the issues discussed, more information and more detail is needed. Therefore, there is an irresolvable tension between the need to provide more detail to practically address the problems of TFA, and the need for these online repositories to be readable by victim-survivors who are facing imminent threats or trauma (or likewise, to be consumed by their advocates within the professional DFV sector).

Consequently, it is argued here that this particular technology-based response of attempting to provide information directly to victim-survivors and support workers via online guides and instructions is reaching the limits of its use-value. There will always be a need for instructional resources to help orient victim-survivors and support workers, but there are clear practical limitations on the ability to maintain up-to-date instructional guides that speak to the full diversity of new and emerging TFA threats. Furthermore, there exist strategic limitations on the ability to deliver useful, reliable information to its intended audiences that will create notable impacts upon safety and security. Ultimately, it is unlikely that online information libraries with associated detailed "how to" guides will ever adequately cover the range of threats to be factored, and there are clear trade-offs between overwhelming readers with excessive detail while also maintaining readability. As will be explored later, this is a major reason that ongoing human-based support is necessary to provide the best policy response for the needs of victim-survivors.

Technology-Based Response B: Efforts to "Design Out" Abuse

Another technology-based response to forms of TFA is attempting to "design out" abuse. This refers to instances where abusive possibilities are closed off and abusive "affordances" created by technology are addressed (Quayle, 2021). Technology creates various opportunities to harass, stalk, surveil, intimidate, and abuse individuals from remote vantage points, and unfortunately, new technologies are persistently utilized by perpetrators of intimate partner violence as new opportunities for hostile behavior (Eterovic-Soric et al., 2017). Consumer IoT is a recent prominent example of technological development that has given way to new opportunities for abuse. "Consumer IoT" refers to the rapidly expanding world of internet-connected domestic devices that exist in our everyday lives. It includes doorbells, fridges, TVs, toys, fitness trackers, pet-food dispensaries, thermostats, home surveillance cameras, "smart home" hubs, and a range of other conventional household items that increasingly feature internet-connected capabilities. It has already been noted by those within the DFV advocacy sector that these new consumer items are being used as weapons of intimate partner abuse (see e.g., Bowles, 2018). Moreover, the designers of consumer IoT hardware and software are unlikely to have factored the possibility of intimate partner abuse into their design (Harkin et al., 2021), thus inadvertently creating multiple opportunities for hostile exploitation.

As a result, there have been calls for technology companies to reflect upon their design choices. Harkin et al. (2021) make an argument that government authorities should increasingly recognize that intimate partner abuse is a major cyber-security issue that should inform the regulation of the safety standards of consumer IoT. Suzor et al. (2019) have similarly argued that social media companies have an obligation to consider the gender-based violence implications of their product designs. Parkin et al. (2019) explored the user interfaces of Amazon Echo and Google Home and how the design of access control systems can allow notable power imbalances for different users, having significant impacts on the threat of intimate partner abuse. And IBM (2020) has already declared a commitment to *Five Technology Design Principles to Combat Domestic Abuse.* There is a growing recognition that design choices made by software and hardware developers have downstream implications for the risks experienced by victims of intimate partner abuse (see also Harkin & Molnar, 2020).

Therefore, there is a clear need to put consistent pressure on technology companies to consider and factor implications for victim-survivors of abuse into their design choices and also proactively react to abusive use leveraged by their products. A high-profile example of companies placed under such pressure are major social media companies such as Facebook, Twitter, Instagram, and Tik Tok, who variously have instituted abusive-use policies, and some have specific mechanisms for victim-survivors to notify or report abuse. Technology companies providing other services have also been pressured to respond to abuse, including internet-based companies or services such as cloud-host providers that may unintentionally support spyware companies (see Molnar & Harkin, 2019), or controversial outlets such as PornHub who have been associated with various forms of abusive use (Kristof, 2020). But this pressure needs to extend to a wider range of IoT manufacturers, video game console developers, car manufacturers (particularly those with "smart" capabilities), smartphone developers, home surveillance system vendors, manufacturers of disability assistance tools, telecommunication companies, and ultimately, anyone offering domestic internet-connected products or internet-based services such as online banking or online government services. Providers of internet-based services or internet-connected products have an obligation to ensure they do not become easily exploited for abusive purposes.

However, while there is an ongoing need to demand further action from technology companies to "design out" or close-off abusive channels, there should also be a strategic recognition that it's an overwhelming task to attempt to shepherd hundreds of companies across a number of industries and jurisdictions to take concerted action. On many occasions, there may be simple adjustments that could be made to a product at a low-cost and the respective company may be willing to respond. For example, Parkin et al. (2019) advocate for IoT devices and manufacturers to consider who can set the major configuration settings for the device and how this can interact with the dynamics of abuse. Likewise, Apple launched an item-tracking device in 2021 that they suggested "has also been designed to discourage unwanted tracking" (Apple, 2021), indicating that some level of awareness of intimate partner abuse is being recognized and addressed by major tech companies.

Nevertheless, it should be noted that while these types of adjustments or changes may foreclose certain opportunities for abuse, they do not make the technology exploitation-free, even when the manufacturer actively attempts to mitigate TFA risks. In the Apple example, a report by the *Washington Post* found that the item still had significant stealthy tracking capabilities irrespective of Apple's efforts to "design out" this possibility (Fowler, 2021). As suggested by Fowler (2021), "even Apple, a company known for emphasizing security and privacy, can struggle to understand all the risks involved in creating tech that puts everyday things online." This points to a number of important limitations to this model of technology-based response: (a) it is very difficult to make technologies in a manner that they could not be exploited by a motivated malicious user; (b) even when a company is factoring issues of intimate partner abuse into their design, they may struggle to make the best choices in the interests of victims; and (c) ultimately, perpetrators are likely to discover more exploitable opportunities faster than they can be discovered and patched, in addition to the significant logistical challenges of identifying necessary re-designs and then lobbying multiple companies to address the design issues. The IoT industry currently has a reputation for a number of considerable technical security concerns (Newman, 2019; Schneier, 2014; Walsh, 2017) but is also made up of a diverse range of companies of varying degrees of production pedigree, scale of operations, jurisdictions, and willingness to be security conscious about their products, therefby putting clear practical limits on the ability to logistically and effectively coordinate necessary steps to "design out" abuse.

To be clear, the argument here is not to discourage important efforts to pressure various technology companies to consider the implications of their design choices for victims of intimate partner abuse. This is an important plank and an ongoing necessity in strategic actions necessary to combat TFA. Technology companies should be variously pressured to factor this issue into their production decisions and encouraged to act in the interests of victims. The key point to be considered here is that in addition to the strategy of attempting to "design out" TFA through safety-by-design, privacy-by-design, and other associated actions, technology companies should also be cognizant of the fact that this approach will not necessarily always meet the needs of victim-survivors or that this approach will be logistically successful (i.e., attempting to manage and coordinate an expanding industry of companies with an expanding array of products). Considering these limitations further supports the need for ongoing human-based resources to support victim-survivors over the long term.

Technology-Based Response C: Developing and Applying Tailored, Circumstantial Tech Solutions

There are also a series of miscellaneous efforts to develop or apply technology-based responses to specific problems. These are cases in which a defined issue has been identified and there is a bespoke attempt to create a unique solution using technology. Two major examples of this are the development of spyware detection tools and the use of "bug detectors" by private security companies. Both examples represent a useful additional tool to combat technology-facilitated abuse but also underline technical, practical, and strategic limitations of this type of technology-based response.

Spyware in the context of intimate partner abuse has received a significant amount of media and activist attention (see e.g., Bhargava, 2020; Dell et al., 2018; Greenberg, 2019). This attention has translated into a number of efforts to create technical responses to spyware including efforts led by Kaspersky as part of the *Coalition Against Stalkerware*, and researchers associated with the *Clinic to End Tech Abuse* creating their own forms of spyware discovery tools. The tool hosted by the *Clinic to End Tech Abuse* (Havron et al., 2019) works as a program that scans a phone looking for apps that are on a "blacklist" of known spyware (see Github, 2021). "TinyCheck" from Kaspersky works by acting as a WiFi-access point that examines the phone's internet traffic looking for data going to servers associated with spyware (Ruiz, 2021).

Both efforts represent useful developments that address the issue of trying to identify whether a given phone is likely to contain spyware or not. It has been noted that victims of intimate partner abuse are increasingly concerned about the possibility of spyware being on their devices (Freed et al., 2018), and there is a clear pressing need for domestic and family violence advocacy services to have options to determine whether or not spyware is present on a phone (to a reasonable degree of confidence). Although these tools could conceivably be utilized by advocates within the domestic and family violence sector (or even law enforcement), they also have notable limitations. These limitations can be technical; for example, both solutions depend on the respective "blacklists" of servers and apps to be up-to-date while also adequately reflecting the full range of possible spyware operating in the wild. It would be a major challenge for any team to exhaustively catalog all apps or servers that are deserving of being "black-listed," thus only ever "catching" a subgroup of spyware (even if that "subgroup" may be large).

Similarly, these tools provide a number of practical and strategic limitations. Ideally, this type of tool would be widely distributed to domestic and family violence support workers (and perhaps law enforcement) to allow many victim-survivors across multiple jurisdictions to have access to viable "spyware detection." They would need to be user-friendly enough that they do not rely on a small cohort of highly skilled workers to deploy and implement, but they should be sufficiently easy to use such that the larger cohort of advocates within DFV organizations could realistically operate the tools without requiring significant burdensome training or up-skilling. As yet, however, it is unclear whether there are realistic prospects of these types of tools having wide uptake from users in the DFV sector, who are already struggling with the technical skills needed to understand and respond to TFA in general (Freed et al., 2017; Tanczer et al., 2021). In principle, work could be done to improve the usability of these tools with a significant investment of resources and, similarly, a cohort of professionals within the DFV sector could be adequately skilled to deploy them; however it remains to be seen whether these tools could be deployed at the wide-scale at which they are needed. Likewise, interpreting results produced by these tools requires a degree of expertise to distinguish between legitimate applications and spyware, particularly when these can have overlapping features or processes.

The point to be made here is that considering their technical limitations in combination with the unlikely prospect that this type of solution could be scaled out for use among a wide variety of DFV services, this type of technology-based response option has limits. In practice, victim-survivors who are concerned that spyware is on their phone are best served with receiving human support where possible, individuals who can make contextual determinations about the likelihood of spyware being present and provide the rounded support that also recognizes that TFA is unlikely to be a stand-alone form of abuse. Options to deploy spyware detection tools could be useful from time to time but are more effective when embedded within well-resourced and knowledgeable human-based responses.

Another example of this type of partially supportive technology-based response that has technical and strategic limitations is the use of radio frequency detectors, often referred to as "bug detectors." As shown in Harkin (2020), the use of "bug detectors" as a means of diagnosing whether a perpetrator has deployed hidden cameras, GPS trackers, a malicious WiFi router, or any other hostile electronic surveillance equipment is often used by private security workers when they have been contracted to provide a "security audit" of a victim-survivor's home. Perpetrators have been known to deploy such devices and security workers have attested to making positive discoveries as a result of "bug detection" (p. 79). Furthermore, the "sweeping" of a home by a security worker has produced some positive psychological effects for victim-survivors who can take confidence from feeling their home has been declared to be surveillance-free: "It made you feel—once they'd gone through the house and everything like that … swept your cars for bugs and did all that sort of stuff, you could actually function again" (quoted in Harkin, 2021).

"Bug detectors," therefore, may have a useful role to play as a technology-based response to TFA, but similar to "spyware detection," there are technical and strategic limitations that must be recognized. Although there is some published work supporting the viability of electronic counter-surveillance (see Gold, 2013), the reliability of radio frequency detectors to confidently detect hidden surveillance is not established in the literature. Technical questions remain about the effectiveness of "bug detection" and, on closer inspection, there are a number of variables that need to be considered when making declarations that a property is surveillance-free based on "bug detection" (see Harkin et al., 2020a).

A small-scale, "hands-on" test with a professional-grade radio frequency detector was performed as part of an unpublished report for the Office of the eSafety Commissioner (see Harkin et al., 2020a). A number of devices, including internet-connected security cameras, “hidden cameras” purchased from online “spying” websites, and several consumer “Internet of Things” devices such as a “smart” doorbell, were tested using a professional-grade “bug detector” to explore whether it could “discover” a device capable of capturing video. The experiments revealed a number of variables that render “bug detectors” ineffective in certain circumstances. For instance, the success of detecting a hidden device depends on whether the device is “live” or “active” in the moments it is being “swept for;” that is, some devices are only detectable when they are broadcasting radio frequency signals and these broadcasts can be intermittent or dormant for significant periods of time. This undermines the capacity of a “sweep” to conclusively find hidden devices. Similarly, the angle at which a device broadcasts its radio frequency signal is also important, and there are circumstances where a radio frequency detector can be very close to the device (less than 20 cm) and not detect anything if it is approaching from the wrong direction. Furthermore, some devices sold on “spying” websites do not broadcast any radio frequency signals and thus are not detectable by “bug detectors.” Bluetooth devices posed notable challenges for detection. These variables add a number of complications and undermine confidence in declaring an environment as “surveillance-free” after “sweeping for bugs.”

Similar to “spyware detection” tools, radio frequency detectors (aka “bug detectors”) can be useful tools for making positive discoveries of malicious surveillance, but they also have caveats and a number of circumstantial variables to consider that diminish the level of confidence in making claims around their capacity to detect hostile surveillance equipment. As a technology-based response, these tools have specific limits that should be recognized, but the value of their contribution to combating TFA is enhanced within a context where there are skilled, well-informed, and well-equipped human forms of support for victim-survivors. This is not a method that can stand in isolation or be deployed by unskilled workers, but it can provide a useful option in the context of well-resourced human support services that can contextualize the merits of the tactic and provide holistic, bespoke support to the victim-survivor.

Technology-Based Response D: Tech-Supported Reporting or Connecting with Services

Finally, there is a range of other technology-based responses to TFA that aim to facilitate reporting or connect victim-survivors with services. This includes chatbots such as “Hello Cass,” apps that are designed for victim-survivors that typically provide facilities perceived as useful for them (including emergency alarm options, note-taking, evidence diaries, or general advice and contact details of support services), or the Office the eSafety Commissioner’s reporting portal for those experiencing forms of image-based abuse. Like the other technology-based responses, these can offer particular benefits and value for victim-survivors, but they also have a number of limitations that should be recognized. It should be reiterated at this stage that some of the examples of technology-based responses discussed in this section are not solely aimed at addressing TFA specifically and often have other primary purposes.

These technologies can in certain circumstances improve the ease of reporting and connect victims with support services more efficiently, but they also have their own limitations or can create new and unexpected dilemmas. For instance, when considering apps designed for victim-survivors, a significant level of skill, effort, and care is required to build, design, and operate apps with suitable security standards that are appropriate for deployment with victims of DFV (WESNET, 2020). The resources required to meet these standards are considerable, and if they are not met, they can expose victim-survivors to additional risks. As an example, one note-taking app used a password to protect the user's notes, but the password could be recovered from the phone's associated cloud account (WESNET, 2020). Although this particular app was withdrawn from distribution by its sponsoring organization, it is likely that other apps in this area will have similar or more serious flaws. Given that expert security design and expert security reviews are a considerable ongoing expense, it is likely that apps deployed with victim-survivors will have notable vulnerabilities now and into the future.

The example of apps being deployed with victim-survivors underlines many of the arguments being made in this article. To be effectively and securely deployed requires a commitment of resources over the long term that is unlikely to materialize, and in the meantime, noble efforts to provide victim-survivors with support can inadvertently create other risks related to the security standards of the app and its operating infrastructure. Furthermore, apps can provide welcome support but not a sufficient level of support, and their use needs to be carefully incorporated into a broader safety plan, with such plans being best put together in collaboration with frontline DFV support workers. Chatbots face similar limitations in that they are also resource-intensive to develop and maintain with up-to-date adequate advice information. Likewise, the Office of the eSafety's image-based abuse portal in Australia has clear use-value but also is limited to the willingness of certain platforms and technology companies to cooperate with takedown requests, and is unlikely to account for image-based abuse shared over end-to-end encrypted messaging apps such as iMessage, WhatsApp, or Signal (as examples). To reiterate, identifying these limitations is not to discourage or unnecessarily criticize impressive efforts to improve the lives of victim-survivors using technological resources, but to underline the ongoing complexity of responding to victim-survivors' needs and how human-based support services are critical to this task.

Discussion

The purpose of outlining various technology-based responses to TFA and underlining their practical, technical, and strategic limitations is not to undermine, deter, or argue against the creation and support of technology-based responses. Many of these ideas and resources should be sustained, supported, developed, and invested in. The purpose here, however, is to discuss how in the case of TFA these types of technological resources are not sufficient in and of themselves and should be *in addition* to strong support from human-based resources. The optimal ecosystem for supporting victim-survivors of TFA is one where there is a well-resourced and well-skilled professional DFV advocacy support sector (in addition to knowledgeable and skilled law enforcement). Having extensive human-based support should be the central plank of any national strategy to provide for victim-survivors of TFA, and technology-based responses should be embedded within such an ecosystem as much as possible (rather than being parallel, independent of, or separate from it).

As illustrated above, there are a number of limitations to technology-based responses and there are many ways in which human-based resources—particularly professional DFV advocacy and support workers—have distinct advantages over technology-focused responses. This is particularly true when thinking of long-term approaches and strategies for addressing TFA. As discussed in multiple examples, circumstances of TFA are too technically and situationally varied, involving multiple platforms, devices, functionalities, and products, and this complexity is only expanding, thus creating an ever-evolving and ever-expanding threat profile for victim-survivors. It is necessary, therefore, for the responses to be as versatile as possible to account for the full range of threats that are present today and the multiplying threats that will emerge in the future. It is more likely that skilled human resources can provide the suitable flexibility of responses when compared with attempting to develop and maintain up-to-date checklists, spyware detection tools, apps, or chatbot content (as examples). A suitably trained and sufficiently resourced human support base of professional DFV workers could provide a stronger over-arching and holistic assessment of the potential threats faced by victim-survivors, factoring the circumstantial variables that define their TFA victimization, both technical and personal.

Likewise, as outlined by Harris and Woodlock (2019), TFA interacts with other forms of abuse and has a "spacelessness" that transcends simple "online" or "offline" distinctions (see also Harris, 2020). Considering the complexity of the circumstances facing victim-survivors when experiencing forms of TFA, professional support workers are best placed to recognize and address how their TFA is unlikely to be happening in isolation, but rather is likely to be a component of wider abuse, threats, and danger. For example, consider that instances of TFA may interact or be dependent on associated problems of housing, migration status, employment, parental responsibilities, or other "structural inequalities" (Harris, 2020, p. 2), rather than an "isolated" problem that can be addressed on its own. In these situations, support workers are much more likely to be in-tune with the specific needs of victim-survivors and capable of addressing the graver contextual problems of which the TFA is a part. Overall, therefore, when considering the lived experiences and "in-the-field" realities of TFA for victim-survivors (see Douglas et al., 2019), it is better for victim-survivors to have access to qualified human support workers than piecemeal technology-based responses.

Technology-based responses to TFA also represent a form of "techno-solutionism" that should not come to pre-occupy responses to TFA. Evgeny Morozov (2014) is credited with coining the term "techno-solutionism" to refer to a 21st-century trend for social, political, and moral problems to be addressed using technological innovation and mechanisms. Attempting to harness "smart" technology, internet-connected devices, apps, "big data" analytics, digital tracking, and other newly emerged technological possibilities can create their own unintended consequences and unanticipated problems, and may ultimately distract from other essential policy questions or resource mobilization (Morozov, 2014). Similar dynamics can be seen when it comes to technology-based responses to TFA. Political decision-makers and those with the power to dictate policy responses are often eager to explore a "technological" fix that can often prove inadequate and overly costly, or that creates additional policy dilemmas (see Haven & Boyd, 2020; Krahulcova, 2021; Larson, 2020). A relevant Australian example was when the NSW Police Commissioner floated the idea of using an app to register "consent" as a method of addressing whether or not a sexual assault has taken place (Nguyen & Cockburn, 2021). The proposal was criticized as naive, overly optimistic about the possibility of technology addressing this issue, and showing a lack of understanding or inability to account for the multiple circumstances of sexual assault (Krahulcova, 2021; Nguyen & Cockburn, 2021).

In the area of domestic and family violence, there is increased attention to potential "technological" solutions that in Australia have included "technology trials" as part of the Women's Safety Package funded by the Commonwealth Government, which committed resources to "GPS trackers for perpetrators, safe phones and safety devices for homes" (DSS, 2020). The relevant minister also announced funding to research and develop "a tool that could sweep a victim's devices or physical environment to establish whether technology has been compromised by malicious software or covertly-installed hardware" (Fletcher, 2019). Such an investment of resources is welcome but will likely encounter many of the difficulties outlined above facing spyware detection tools, in addition to the noted limitations on "bug detection." These efforts may be regarded as their own form of "techno-solutionism," and while they may produce some valuable outcomes, their notable limits should also be acknowledged.

Ultimately, funding and the associated efforts needed to combat TFA are limited resources, and trade-offs are usually encountered when deciding in which resources to invest, either human or technological. As outlined, one of the temptations of "techno-solutionism" is that it may appear more efficient, and it can often have a superficial political appeal of being "innovative" or "cutting edge." But as outlined above, such solutions can have distinct shortcomings on issues of their technical capability and their capacity to deliver practical impacts—at scale—for victim-survivors who need immediate and multifaceted support. As argued by Schneier (2000), "security is a process, not a product" and specific technologies are unlikely to provide general solutions to quintessentially human problems. The purpose of this article, therefore, is to add a corrective to the impulse to over-invest in "techno-solutionism" and argue instead for the prioritization of human-based resources.

Specifically, this article supports investment in professional DFV support workers who are resourced to develop their understanding of TFA. Law enforcement also has a role to play in responding to TFA and can certainly improve upon its noted current shortcomings in this area (see Harris & Woodlock, 2019). However, professional DFV support workers are more likely to be best placed to provide impactful services for victim-survivors. There are long-standing issues with the relationship of victim-survivors of DFV and law enforcement agencies (see Douglas, 2021; Goodman-Delahunty & Crehan, 2016), and in many cases, the primary support for the needs of victim-survivors are best provided by professional, dedicated DFV support services.

It should be emphasized, however, that such support services are also currently struggling with a lack of resources, funding, knowledge, and skills to comprehensively address the needs of clients experiencing TFA (Freed et al., 2018; Lopez-Neira et al., 2019). The threat of TFA and the technical complications regarding the abuse experienced by their clients are currently beyond their skills and knowledge level, and even with many of the notable efforts to up-skill such workers documented here (such as the online safety guides and bespoke training provided by organizations such as WESNET), notable challenges still remain with preparing DFV support workers with the knowledge, funding, and resources they require to adequately provide for their clients. Furthermore, there are also issues with victim-survivors accessing support services, which was made more difficult throughout the pandemic (see Carrington et al., 2021; Pfitzner et al., 2020).

Despite such challenges facing the sector however, it is argued here that they ought to be the central pillar of a national strategy to combat TFA. Investing in the cohort of professional, specialist DFV support workers who work directly with victim-survivors is the ideal foundation for a strategy for dealing with the rapidly expanding nature of TFA facing victim-survivors and the complex, multifaceted nature of the abuse.

Ideally, the investment would primarily focus on two parallel and interrelated human resourcing requirements. First, the full breadth of DFV support workers must be targeted to raise the floor on their general awareness and skill level with TFA. Such training should be cognizant of the limitations of attempting to up-skill a large sector featuring thousands of individuals and instead adopt modest targets around its goals for learning. It is not required, for instance, that everyone who works in the sector develop high-level expertise on matters related to TFA, but should at least have some abilities to triage a technical problem and have access to colleagues who have considerably more technical knowledge and skills.

The second target of investment for better human resourcing in the DFV sector is in the creation and maintenance of a high-level “vanguard” of professional workers with particular expertise in TFA. It is more achievable and efficient to equip a smaller cohort with dedicated high-level skills, understanding, and the associated abilities to conduct more forensic analysis than to target the larger base of DFV support workers. Organizations such as WESNET or NNEDV already play such a role in Australia and the United States, respectively, but require ongoing, sustainable support and resourcing to adequately respond to the long-term ever-evolving dilemma of TFA. Providing frontline workers with access to a more tech-focused cohort that has the necessary skills, resources, and funding to provide support services at scale is imperative for addressing the full technical complexity of TFA now and into the future.

Ultimately, well supported and structured human resources are likely to be more impactful in the long term than any of the technology-based responses currently being trialed or implemented.

Conclusion

This article has aimed to draw out and articulate significant limitations of technology-based responses to TFA in the context of DFV. Many technology-based responses have promising merit and capacity to support certain victim-survivors of TFA, but as shown here, they can also have notable shortcomings and limitations, present new challenges or concerns, and often do not provide the type and scale of support necessary for assisting victim-survivors. The purpose of highlighting these limitations, therefore, is to help inform future-looking questions about the priorities of investment to combat TFA. From the perspective of national and international policy plans, technology-based responses should be treated as secondary to the primary priority of investing in human-based resources that can provide direct, holistic, multifaceted, and sustainable support for victim-survivors of TFA over the longer term. Human-based resources, and in particular professional DFV support workers, should be the core of a support ecosystem for victims of TFA, and technology-based responses ought to be supplementing that support, rather than potentially supplanting, replacing, or "crowding out" that support in terms of consuming limited funding, resources, or policy attention. Without a strong foundation in human-based support with an emphasis on skilled professional DFV support workers, responses to TFA will not be as effective as they could or should be.

Acknowledgments

The authors would like to acknowledge the support of multiple organizations and colleagues who have helped with or collaborated on various research projects that cumulatively resulted in this article. They include the support of the Office of the eSafety Commissioner (Australia), the Women's Services Network (WESNET), and the Australian Communications Consumer Action Network (ACCAN). The authors would also like to express thanks for the support and collaboration of a number of colleagues on these projects including Dr. Adam Molnar, Dr. Leonie Tanczer, Dr. Samer Hanoun, Prof. Marilyn McMahon, Ms. Andi Brown, and Ms. Karen Bentley and Ms. Susan Swain at WESNET.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Office of the eSafety Commissioner, Austalian Communications and Consumer Action Network. This article utilized findings and observations from multiple funded projects, including: (a) The *Office of the* *eSafety Commissioner* grant for “Provision of a scoping study exploring the availability of specialist technology support for those impacted by technology-facilitated abuse” awarded to Dr. Diarmaid Harkin, Dr. Robert Merkel, Dr. Samer Hanoun, Dr. Leonie Tanczer and Ms. Karen Bentley; (b) an *Australian Communication Consumer Action Network* (ACCAN) grant into “Risks, Impacts, and Accountability in the Consumer Spyware Industry,” awarded to Dr. Adam Molnar and Dr. Diarmaid Harkin; and (c) an *Australian Communication Consumer Action Network* (ACCAN) grant to fund “Staying Safe: Empowering Women to Navigate Privacy, Safety and Security Mobile Apps in the Australian Marketplace,” awarded to WESNET and Dr Robert Merkel.

ORCID iD

Diarmaid Harkin https://orcid.org/0000-0002-9928-719X

References

Al-Alosi, H. (2020). Fighting fire with fire: Exploring the potential of technology to help victims combat intimate partner violence. *Aggression and Violence Behaviour*, *52*, 1–10. https://doi.org/10.1016/j.avb.2020.101376

Apple (2021). *What to do if you find an AirTag or get an alert that an AirTag is with you*. https://support.apple.com/en-us/HT212227

Bevin, E. (2019). Man pleads guilty to stalking and controlling ex-girlfriend’s car with his computer. *ABC News*. https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980

Bhargava, A. (2020). Stalkerware: The growing hidden-software crisis. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2020/08/28/stalkerware-the-growing-hidden-software-crisis/?sh=4f44b7a26b00

Bowles, N. (2018, June 23). Thermostats, locks and lights: Digital tools of domestic abuse. *New York Times*. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Carrington, K., Morley, C., Warren, S., Ryan, V., Ball, M., Clarke, J., & Vitis, L. (2021). The impact of the COVID-19 pandemic on Australian domestic and family violence services and their clients. *Australia Journal of Social Issues*, *56*(4), 539–558. https://doi.org/10.1002/ajs4.183

Chayn (2021a). *Advanced DIY privacy for every woman*. https://chayn.gitbook.io/advanced-diy-privacy-for-every-woman/

Chayn (2021b). *Voice calls and keeping a diary*. https://chayn.gitbook.io/advanced-diy-privacy-for-every-woman/voice-calls-and-keeping-a-diary

Chikofsky, E. J., & Cross, J. H. (1990). Reverse engineering and design recovery: A taxonomy. *IEEE Software*, *7*(1), 13–17. https://doi.org/10.1109/52.43044

Citron, D. K. (2015). Spying Inc. *Washington and Lee Law Review*, *72*(3), 1243–1282.

Clinic to End Tech Abuse (2021a). Step-by-step how-to guides. *Cornell Tech*. https://www.ceta.tech.cornell.edu/aboutus

Clinic to End Tech Abuse (2021b). iCloud—Compromise Cleanup: Improving your security if you think someone else has gotten in. *Cornell Tech*. https://82beb9a6-b7db-490a-88be-9f149bafe221.filesusr.com/ugd/c4e6d5_773db8c792234c5c948fbc948fcd3990.pdf

Dell, N., Levy, K., McCoy, D., & Ristenpart, T. (2018). How domestic abusers use smartphones to spy on their partners. *Vox*. https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google

Department of Social Services (2020). *Women's safety package*. https://www.dss.gov.au/women-programs-services-reducing-violence/womens-safety-package

Dodge, A., & Johnstone, E. (2019). *Using fake video technology to perpetrate intimate partner abuse*. California Partnership to End Domestic Violence. https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf

Douglas, H. (2021). *Women, intimate partner violence, and the law*. Oxford University Press.

Douglas, H., Harris, B., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, *59*(3), 551–570. https://doi.org/10.1093/bjc/azy068

eSafety Commissioner (2021a). *Domestic and family violence*. https://www.esafety.gov.au/women/domestic-family-violence

eSafety Commissioner (2021b). *How to report image-based abuse*. https://www.esafety.gov.au/report/image-based-abuse

eSafety Commissioner (2021c). *Privacy settings in Instagram*. https://www.esafety.gov.au/media/privacy-settings-instagram

Eterovic-Soric, B., Choo, K. K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers—detecting and deterring stalking behaviours using technology: A review. *Computers and Security*, *70*, 278–289. https://doi.org/10.1016/j.cose.2017.06.008

Fletcher, P. (2019). Joint Media Release: Keeping Australians Safe—New investments to protect women and children. *Media Release of Federal Minister Paul Fletcher MP*. https://www.paulfletcher.com.au/media-releases/joint-media-release-keeping-australians-safe-new-investments-to-protect-women-and

Fowler, G. (2021, May 5). Apple's AirTag trackers made it frighteningly easy to "stalk" me in a test: Apple knows its tiny new lost-item gadgets could empower domestic abuse but doesn't do enough to stop it. *Washington Post*. https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/

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 of the ACM on human-computer interaction: Volume 1 issue CSCW*. https://www.ipvtechresearch.org/pubs/a046-freed.pdf

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A stalker's paradise": How intimate partner abusers exploit technology. In *ACM Conference on Human Factors in Computing Systems*. https://www.ipvtechresearch.org/pubs/stalkers-paradise-intimate.pdf

Github (2021). *stopipv/isdi*. https://github.com/stopipv/isdi

Gold, S. (2013). Electronic countersurveillance strategies. *Network Security*, *2*, 15–18.

Goodman-Delahunty, J., & Crehan, A. C. (2016). Enhancing police responses to domestic violence incidents: Reports from client advocates in New South Wales. *Violence Against Women*, *22*(8), 1007–1026. https://doi.org/10.1177/1077801215613854

Greenberg, A. (2019). Hacker Eva Galperin has a plan to eradicate stalkerware. *Wired*. https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

Harkin, D. (2020). *Private security and domestic violence: The risks and benefits of private security companies working with victims of domestic violence*. Routledge.

Harkin, D. (2021). The uncertain commodity of "security": Are private security companies "value for money" for domestic violence services? *Australian and New Zealand Journal of Criminology*, *54*(4), 521–538.

Harkin, D., Brown, A., & Tanzer, L. (2021). *Securing the "Internet of Things" (IoT) for victim-survivors of domestic and family violence (DFV): Recommendations for "Safety by Design*." Unpublished paper.

Harkin, D., Hanoun, S., & McMahon, M. (2018). Debugging hardware and family violence: A market, technical, and legal analysis. Technology-Facilitated Family Violence Research Group. https://blogs.deakin.edu.au/criminology/wp-content/uploads/sites/2/2019/02/Deakin-Debugging-Hardware-Project.pdf

Harkin, D., Hanoun, S., Merkel, R., Tanczer, L., Bentley, K., & Swain, S. (2020b). *Review of eSafety's Existing Technology Related Content*. Office of the eSafety Commissioner, Unpublished report.

Harkin, D., Hanoun, S., Merkel, R., Tanczer, L., Bentley, K., Swain, S., & Brown, A. (2020a). *Provision of a scoping study exploring the availability of specialist technology support for those impacted by technology-facilitated abuse*. Office of the eSafety Commissioner, Unpublished report.

Harkin, D., & Molnar, A. (2020). Operating-system design and its implications for victims of family violence: The comparative threat of smart phone spyware for android versus iPhone users. *Violence Against Women*, *27*(6–7), 851–875. https://doi.org/10.1177/1077801220923731

Harkin, D., Molnar, A., & Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture: An International Journal*, *16*(1), 33–60. https://doi.org/10.1177/1741659018820562

Harris, B. (2020). Technology, domestic and family violence: perpetration, experiences and responses. *Centre for Justice Briefing Paper*, Issue 4.

Harris, B., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, *59*(3), 530–550. https://doi.org/10.1093/bjc/azy052

Haven, J., & Boyd, D. (2020). *Philanthropy's techno-solutionism problem. Democracy and civic life: What is the long game for philanthropy?* Kettering Foundation.

Havron, S., Freed, D, Chatterjee, R., Mccoy, D., Dell, N., & Ristenpart, T. (2019). Clinical computer security for victims of intimate partner violence. *28th USENIX Security Symposium (USENIX Security 19)*, 105–122.

IBM (2020). Five technology design principles to combat domestic abuse. *IBM*. https://www.ibm.com/blogs/policy/design-principles-to-combat-domestic-abuse/

Krahulcova, L. (2021). Techno solutionism—very few things actually need to be an app. *Digital Rights Watch*. https://digitalrightswatch.org.au/2021/03/25/technosolutionism/

Kristof, N. (2020, April 12). The children of PornHub. *New York Times*. https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html?action=click&module=RelatedLinks&pgtype=Article

Larson, R. (2020). Beware tech solutionism and how to avoid it. *Project Times*. https://www.projecttimes.com/articles/beware-tech-solutionism-and-how-to-avoid-it/

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.

Mandau, M. (2020). "Snaps", "screenshots", and self-blame: A qualitative study of image-based sexual abuse victimization among adolescent Danish girls. *Journal of Children and Media*, *15*(3), 431–447. https://doi.org/10.1080/17482798.2020.1848892

Molnar, A., & Harkin, D. (2019). *The consumer spyware industry: An Australian-based analysis of the threats of consumer spyware*. ACCAN. https://accan.org.au/grants/completed-grants/1435-risks-impacts-and-accountability-in-the-consumer-spyware-industry

Morozov, E. (2014). *To save everything, click here: The folly of technological solutionism*. New York: Public Affairs.

Newman, L. (2019). It's time for IoT security's next big step: Connected devices are more secure than ever. That's still not nearly enough. *Wired*. https://www.wired.com/story/iot-security-next-step/

Nguyen, K., & Cockburn, P. (2021). Consent app proposed by NSW Police Commissioner Mick Fuller to address growing rate of sexual assaults. *ABC News*. https://www.abc.net.au/news/2021-03-18/nsw-sexual-consent-app-proposed-by-mick-fuller/100015782

NNEDV (2021). *Technology safety & privacy: A toolkit for survivors*. https://www.techsafety.org/resources-survivors

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. In *NSPW '19: Proceedings of the New Security Paradigms Workshop*. Association for Computing Machinery, New York.

Pfitzner, N., Fitz-Gibbon, K., & True, J. (2020). *Responding to the "shadow pandemic": Practitioner views on the nature of and responses to violence against women in Victoria, Australia during the COVID-19 restrictions*. Monash University. https://doi.org/10.26180/5ed9d5198497c

Quayle, E. (2021). Affordances, social media and the criminogenic nature of the internet: Technology-mediated child sexual abuse. In E. Caffo (Ed.), *Online child sexual exploitation* (pp. 33–48). Springer.

Ruiz, D. (2021). TinyCheck: Stalkerware detection that doesn't leave a trace. *Malware Bytes*. https://blog.malwarebytes.com/privacy-2/2021/03/coalition-against-stalkerware-partners-tool-finds-stalkerware-in-new-way/

Schneier, B. (2000). The process of security. *Information Security*. https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Schneier, B. (2014). The internet of things is wildly insecure—and often unpatchable. *Wired*. https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

Scott, D. (2020). Deepfake porn nearly ruined my life. *Elle*. https://www.elle.com/uk/life-and-culture/a30748079/deepfake-porn/

Stevens, F., Nurse, J., & Arief, B. (2020). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376. https://doi.org/10.1089/cyber.2020.0253

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

Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018) *Gender and IoT research report: The rise of the Internet of Things and implications for technology-facilitated abuse*. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf

Tanczer, L., Parkin, S., & Lopez-Neira, I. (2021). "I feel like we're really behind the game": Perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence*, *5*(3), 431–450. doi:10.1332/239868021X16290304343529

Todd, C., Bryce, J., & Franqueira, V. (2021). Technology, cyberstalking and domestic homicide: Informing prevention and response strategies. *Policing and Society*, *31*(1), 82–99. https://doi.org/10.1080/10439463.2020.1758698

Walsh, S. (2017). Manufacturers may be overlooking IoT security. *RTInsights.Com*. https://www.rtinsights.com/manufacturers-and-iot-csecurity-bdo-report/

WESNET (2020). *App safety centre: 2020 review of DFV apps*. https://techsafety.org.au/resources/appsafetycentre/apps-reviewed/

WESNET (2021). *Women's technology safety & privacy toolkit*. https://techsafety.org.au/resources/resources-women/

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). Technology as a weapon in domestic violence: Responding to digital coercive control. *Australian Social Work*, *73*, 368–380. https://doi.org/10.1080/0312407X.2019.1607510

Author Biographies

Diarmaid Harkin is a senior lecturer in Criminology at Deakin University. He has recently published a book entitled, *Private Security and Domestic Violence: The Risks and Benefits of Private Security Companies Working with Victims of Domestic Violence* (Routledge). His recently completed projects include an exploration of the consumer spyware industry, national responses to the problem of technology-facilitated abuse in the context of domestic and family violence, and the regulation of consumer IoT.

Robert Merkel received his PhD from Swinburne University of Technology and was a Lecturer in Software Engineering at Monash University. His previous published work is in the discipline of software engineering, including the theory of software testing and the personal characteristics of software testers. Over the past several years, he has conducted both unpaid volunteer work and paid consultancy work in the area of technology-facilitated abuse. He currently works in the private sector as a software developer.