Human–Computer Interaction

ISSN: 0737-0024 (Print) 1532-7051 (Online) Journal homepage: https://www.tandfonline.com/loi/hhci20

Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums

Roxanne Leitão

To cite this article: Roxanne Leitão (2019): Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums, Human–Computer Interaction, DOI: 10.1080/07370024.2019.1685883

To link to this article: https://doi.org/10.1080/07370024.2019.1685883

HUMAN–COMPUTER INTERACTION, 2019, Volume 00, pp. 1–40

ISSN: 0737-0024 print / 1532-7051 online
DOI: https://doi.org/10.1080/07370024.2019.1685883

Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums

Roxanne Leitão
Design Against Crime Research Centre, Central Saint Martins, University of The Arts London, London, UK

This article reports on a qualitative analysis of data gathered from three online discussion forums for victims and survivors of domestic abuse. The analysis focussed on technology-facilitated abuse and the findings cover three main themes, namely, 1) forms of technology-facilitated abuse being discussed on the forums, 2) the ways in which forum members are using technology within the context of intimate partner abuse, and 3) the digital privacy and security advice being exchanged between victims/survivors on the forums. The article concludes with a discussion on the dual role of digital technologies within the context of intimate partner abuse, on the challenges and advantages of digital ubiquity, as well as on the issues surrounding digital evidence of abuse, and the labor of managing digital privacy and security.

KEYWORDS Mobile, internet use, privacy, social computing, domestic abuse, communities

1. INTRODUCTION

Intimate partner abuse (IPA) is a global public health concern and a violation of human rights. IPA can be understood as any behavior or pattern of behaviors, perpetrated by an intimate partner or ex-partner, that causes physical, sexual, or psychological harm to the victim, including coercive and controlling behaviors (World Health Organisation, 2017). A study including data from ten countries revealed that between 13% and 61% of women experience physical and/or sexual violence perpetrated by an intimate partner. The same study shows that 12% to 58% of respondents had experienced at least one form of psychological abuse in the 12 months preceding the study (García-Moreno, Jansen,

Roxanne Leitão (r.leitao@csm.arts.ac.uk) is a designer and researcher is a designer and researcher working within the field of social design.

Ellsberg, Heise, & Watts, 2005). In the United States, an estimated 37.3% of women and 30.9% of men will experience IPA at some point in their lifetime. Similarly, 48.4% of women and 48.8% of men have experienced psychological abuse from an intimate partner (Black et al., 2011). In the European Union (EU), it is estimated that 22% of women have experienced sexual and/or physical violence from an intimate partner and 43% have experienced some form of psychological abuse (European Union Agency for Fundamental Rights, 2014). Comparable statistics could not be found for men at an EU level. In the United Kingdom (UK), an estimated 27.1% of women and 13.2% of men have experienced domestic abuse. It is important to highlight that UK statistics refer to the wider umbrella of domestic abuse, which can include abuse between family members and/or intimate partners. However, UK figures do not include stalking and psychological abuse (Office for National Statistics, 2017), which means that actual domestic abuse prevalence rates are likely to be even higher.

Similarly, none of the above statistics include behaviors of cyber-stalking, cyber-monitoring, and/or cyber-harassment within the context of IPA. Studies by Snook, Chayn, and SafeLives (2017, p. 19) and Women's Aid (Laxton, 2014, p. 8) estimate that 45% to 48% of IPA victims experience some form of technology-facilitated abuse. Technology-facilitated IPA is a novel phenomenon and the focus of a growing body of work. Research shows that technology-facilitated IPA extends perpetrators' ability to monitor, harass, threaten, and stalk victims far beyond what was possible before the ubiquity of digital technologies. Technology-facilitated IPA can include behaviors such as monitoring victims contacts, communications, and social media networks (Dimond, Fiesler, & Bruckman, 2011), tracking victims' location and movements (Southworth, Finn, Dawson, Fraser, & Tucker, 2007), as well as sending consistent threats, abuse, and other forms of harassment (Chatterjee et al., 2018; Freed et al., 2017; Freed, Palmer, Ristenpart, & Dell, 2018; Harris & Woodlock, 2018; Matthews et al., 2017).

Existing research has focussed on qualitative studies with professional support workers and victims engaged with professionalized support services. The work reported on in this paper aims to extend previous findings by contributing a qualitative analysis of domestic abuse online forums where victims/survivors are engaged in peer-support. Victims seeking peer-support on forums may, or not, be in contact with professional support. In either case, they are seeking nonprofessional peer-support online. Victims may choose to engage in online peer-support for any number of reasons, from seeking out individuals going through the same experience, to the unavailability of professional local services, or for any number of other cultural and social barriers to service access (Bent-Goodley, 2007; Burman & Chantler, 2005; Duke & Davidson, 2009; Femi-Ajao, Kendal, & Lovell, 2018; Kulwicki, Aswad, Carmona, & Ballout, 2010; McClennen, Summers, & Vaughan, 2008; Robinson & Spilsbury, 2008).

With this in mind, the present work aims to extend current knowledge of technology-facilitated IPA to victims seeking support outside of professionalized support services. More specifically, to understand:

- the forms of technology-facilitated abuse being discussed by victims engaging in online peer-support;
- if and how victims are using technology within the context of IPA;
- and the quality of digital security and privacy advice being exchanged between forum members.

Firstly, our analysis reports on the forms of technology-facilitated abuse being discussed between forum members, including overt and covert surveillance, as well as persistent threats of harassment and abuse enabled by digital ubiquity. Secondly, the analysis reveals how victims are using technology within the specific context of IPA, from evidence gathering to contacting other potential victims. Lastly, the results show the limitations of digital privacy and security advice being exchanged between members on the forums, especially regarding spyware, hacked or hijacked accounts, and covering digital footprints.

1.1. Related work

This section outlines prior research on technology-facilitated IPA and the use of forum data in qualitative studies.

1.1.1. Technology-facilitated IPA

Recent studies have found that digital technologies are increasingly being used by perpetrators in abusive intimate relationships to monitor, harass, stalk, and threaten victims (Dimond et al., 2011; Freed et al., 2017, ; Harris & Woodlock, 2018; Matthews et al., 2017; Snook et al., 2017; Southworth et al., 2007; Woodlock, 2016; Zaidi, Fernando, & Ammar, 2015). Harris and Woodlock (2018) have recently proposed the term digital coercive control to describe perpetrators' use of novel technologies within the context of IPA. They draw upon findings from two Australian studies to describe how digital technologies allow for the emergence of a *spaceless* element to IPA. Or in other words, how the use of technology to track victims' location and communications makes stalking and monitoring possible remotely and at any distance. The remote nature of technology-facilitated IPA leads victims to perceive perpetrators as *omnipresent* and *omnipotent*, whilst removing feelings of safety that may have been achieved, in the past, when victims relocated or were otherwise physically distant from perpetrators.

Freed et al. (2018) conducted a qualitative study in the US, with victims and support workers, exploring how perpetrators of IPA use technology to remotely harass, intimidate, threaten, monitor, and impersonate their victims. In addition to findings that support the *spaceless* element of technology-facilitated IPA, the authors also highlight that IPA perpetrators generally do not have technical capabilities beyond those of the average citizen, which would enable them to remotely abuse their victims. In fact, perpetrators interact with victims' devices through standard user-interfaces (UIs) or use ready-made

downloadable software, such as spyware. Furthermore, Chatterjee et al. (2018) conducted a review of existing mobile apps that could be considered dangerous in IPA contexts. They found dozens of overt spyware tools and hundreds of *dual-use* apps available on app stores. *Dual-use* apps are defined as apps available on official app stores that have a *legitimate purpose*, such as tracking children or stolen devices, but can also be easily repurposed to monitor an intimate partner. They also found a vast amount of online guidance educating perpetrators on how to exploit *dual-use* apps for IPA. Unsurprisingly, their analysis of existing anti-virus and anti-spyware tools found these to be largely ineffective in identifying *dual-use* apps as a threat. What is more, Freed et al. (ibid.) also discuss how these *UI-bound* attacks – using existing apps – are extremely damaging to victims and that they are hard to counteract because they fall outside of systems anticipated external threat models and are, therefore, not flagged by anti-virus tools.

On the other hand, regarding the use of existing apps/software, Zaidi et al. (2015) investigated the use of technology amongst immigrant women survivors of domestic abuse. They found that even though most of the participants rated their technology knowledge levels at *good* or *excellent*, and had access to mobile phones and computers, they did not feel empowered by these technologies. In fact, for most participants, having access to mobile phones or computers did not assist them in escaping the violence. Similarly, Dimond et al. (2011) interviewed female survivors living in a domestic abuse shelter, in the US, about their experiences with technology. Participants also reported a lack of trust in their own limited knowledge of digital privacy and security, opting, for example, to replace devices rather than risk perpetrators being able to track them.

In another study, Freed et al. (2017) report on the socio-technical complexities posed by digital technologies in the interactions between victims, abusers, law enforcement, counselors, and other support professionals. Firstly, the qualitative analysis highlights the technical challenges victims face in managing social circles that are shared with perpetrators. Secondly, the study also reveals that neither victims nor support workers are confident in their expertise in managing the complexities of technology-facilitated abuse, which is consistent with other existing research (Dimond et al., 2011; Harris & Woodlock, 2018; Matthews et al., 2017). Thirdly, Freed at al. (ibid) highlight the complex trade-offs that need to be managed when using technology within the support ecosystem itself. For example, well-intentioned professional advice on *blocking* perpetrators on social media may, in fact, frustrate perpetrators and lead to escalations in abuse.

Finally, in an attempt to provide a framework for understanding technology-facilitated IPA, Matthews et al. (2017) report on interviews with survivors of IPA, in the US, based on which they propose organizing victims' technology practices and challenges into three phases: *physical control, escape*, and *life apart*. The framework is intended to offer an empirically-based method for technology creators to consider how technology may be designed to better support victims of IPA.

All of the research discussed above is based on qualitative studies with professionals and IPA victims engaged with formal support organizations. The qualitative study

reported on in this article extends current knowledge on the role of technology, within the context of IPA, by using data from online discussion forums where victims engage in peer-support. The victims on these forums may, or not, be accessing professional support and may have, therefore, fallen outside the scope of previous work.

1.1.2. Online forum data in qualitative studies

Although it is still an emerging field, forum data is increasingly being used for research purposes (Ackland, 2013, pp. 35–44; Im & Chee, 2012; Zimmer & Kinder-Kurlanda, 2017, pp. xxix–xxx). Forums are generally made up of communities around a shared issue of concern or a shared interest and organized according to message boards dedicated to specific topics. A forum will often have several message boards, which are then structured according to threads and posts. Threads are initiated by a post and then all replies to that post form a thread. In most cases, anyone can sign-up to become a member of a forum and they can do so anonymously by using an alias.

The open and anonymous nature of online forums has made them a popular medium for engaging in 24-hour peer-to-peer information and support. Accordingly, previous work has shown that the most common types of messages exchanged on online support forums are those related to self-disclosure, requests for information, and the provision of emotional support between forum members (Rains, Peterson, & Wright, 2015; Winzelberg, 1997). The anonymity offered by online forums is thought to motivate users toward more openness in sharing stories and opinions, which might otherwise be difficult to divulge in face-to-face interactions (Holtz, Kronberger, & Wagner, 2012). For these reasons, researchers have increasingly become interested in the potential of forums to provide observational data that would be otherwise difficult or impossible to access. Forums can be seen as providing authentic *natural data* because discussions effectively take place in online public spaces and are not influenced by the researcher (Holtz et al., 2012). What is more, because the structure of online forums promotes discussion between peers, a subject is often more thoroughly discussed and clarified, through the exchange of information, opinions, and emotional support, than it would be in an interview with a single participant.

Furthermore, forums can be an effective means of accessing hard-to-reach communities (e.g., victims and survivors of IPA, patients with chronic health conditions) in a less intrusive manner than, for example, participant recruitment for in-person interviews. Unsurprisingly, forum data has been used in a number of studies investigating sensitive topic areas, such as HIV prevention (Crawford, Maycock, Tobin, Brown, & Lobo, 2018), health-related knowledge exchange (Kimmerle, Bientzle, & Cress, 2014), breast cancer (Lovatt, Bath, & Ellis, 2017; Sillence, 2013), weight management (Meng, 2016), eating disorders (Winzelberg, 1997), and Parkinson's disease (Attard & Coulson, 2012). Accordingly, this study uses data from three online domestic abuse discussion forums with the aim of extending existing research

regarding technology-facilitated IPA, beyond victims and survivors engaged with professionalized support services.

The following section details our methodology and the ethical considerations that informed our work. The main findings are then presented and followed by a discussion of their implications and limitations.

2. METHODOLOGY

For this research, data was gathered from three forums specifically dedicated to victims and survivors of domestic abuse. Two of these forums are run by communities and the other is hosted and maintained by an NGO. Forums were identified through the search engine query: "domestic violence forum". Although this work focusses on IPA, this is a term that is not widespread in popular culture. For this reason, the term *domestic violence* was used in the search engine query. Accordingly, all posts that do not refer to abuse specifically between intimate partners were removed from the dataset. The location from where the query was performed has not been included in this article in order to protect the identity of the forums and forum members.

The author reviewed forum guidelines in the order that each forum appeared on the list of search results. Three forums were selected in order of appearance as long as they fulfilled three criteria: 1) they were written in English, 2) they did not prohibit research and 3) did not require user registration, therefore, ensuring all the data was effectively in the public domain. The author chose to use open forums because she felt that registering on a domestic abuse forum implies that the user is either a survivor or victim of IPA, which would be untrue and therefore violate the communities' expected code of conduct. Accordingly, a non-intrusive, observational, approach was taken where forum posts and threads were only viewed. No posts or any other kind of contribution to the public forum discussions were made, nor any clarification on any of the post content was sought.

Where transcripts are used in reporting the findings, users' screen names, timestamps, and location information have been removed to preserve anonymity. Furthermore, any quotes that have been included are not word for word transcriptions. The author has adjusted for abbreviations and language that may be used to identify individuals, corrected grammatical and spelling mistakes, and removed any identifiers (e.g., names, locations), without altering the sentiments, ideas, and/or events that are being described. This has been done so that a simple search engine query of the transcript will not lead to the original forum post, in an effort to preserve forum members' anonymity. Similarly, the forums' names and URLs have not been included in this article. Each of the forums is briefly described below but identifying details are not provided.

Web scraping was used to automatically retrieve data from the forums in question. The files were exported in JSON. An automated scrape of 200 pages was run for each of the forums. Pages were selected, rather than posts, due to

technical issues in distinguishing original posts from posts that are replies to an initial post, resulting from inappropriate HTML markup on one of the forums. The scrape resulted in:

- 189 individual posts from the general discussion board on a specialized domestic abuse forum run by an NGO [NGOF], with posts dating between 13.10.17 and 21.11.17;
- 375 individual posts from the general discussion board on a domestic abuse community forum [CF], with posts dated between 12.05.16 and 9.07.17;
- 181 from a community domestic abuse subforum [CSF] with posts dated between 24.04.17 and 29.07.17. The subforum is hosted on a larger forum with over a 100 subforums dedicated to a wide range of topics. The subforum only has a single board.

One of the initially selected forums underwent a redesign and change to their guidelines while the research was being conducted. The new guidelines prohibited research and therefore that data was excluded from this study. A substitute forum was then selected (from the previously compiled list), which explains the 3-month gap between data collection from [NGOF] as compared to the other forums. One of the three forums had more than one message board. However, only one of those boards was meant for discussion, whereas others contained information related to IPA or legal information about the forum's use.

An initial amount of 200 pages was decided upon, as a figure that seemed appropriate to the researcher. If, however, new insights kept emerging across the 600 pages from 3 forums, more posts would have been scraped. In the case of this work, it was found that a great deal of repetition in codes was already happening within the sample of 600 pages. Therefore, no more than the initial 200 pages were scraped for each forum.

Finally, given the anonymous nature of online forums, it is not possible to report on the sociodemographic characteristics of the users. Even though some of this data can be inferred from the content of individual posts and threads, there is no way of verifying that information.

2.1. Note on ethical considerations

The use of forum data raises a series of ethical considerations relating to informed consent of human subjects, as well as the protection of research subjects' privacy and anonymity. Although forum posts are effectively in the public domain, some authors have argued that users may have the expectation of certain levels of privacy when they are participating in online forums (British Psychological Society, 2017; Eysenbach & Till, 2001). In other words, although a user may have posted content online (publicly) to share with a specific community, this does not mean that they have given consent for this data to be collated, analyzed, and published. Nonetheless, according to the British Sociological Association (Sugiura, 2016) and

The British Psychological Society (2017), if data is available in the public domain, it can be ethically used as research data provided that users are adequately anonymized to guarantee their privacy. This approach has been used in a number of studies using forum data to investigate sensitive topic areas (Attard & Coulson, 2012; Crawford et al., 2018; Hargreaves, Bath, Duffin, & Ellis, 2018; Kimmerle et al., 2014; Lovatt et al., 2017; Meng, 2016; Sillence, 2013; Winzelberg, 1997).

As previously mentioned, all the data used in this study was in the public domain. Firstly, forums did not require registration to read posts. Secondly, they did not prohibit research in their *terms and conditions*, Thirdly, all forums had a warning reminding their users that their posts are public and that, therefore, no identifying information should be included in the posts. Nonetheless, appropriate steps were taken to anonymize all posts included in this article. Once anonymized, posts used in publication materials were submitted to search engine queries to ensure that they did not lead to the original post and forum member's screenname. Forum members' confidentiality was also maintained as forum members' screen names were removed from the dataset. Steps to guarantee anonymity and confidentiality were taken to guarantee that the research brings no potential additional harm to forum members, beyond the already existing risk of posting on publicly available forums. For these reasons, this study was exempt from institutional ethics review board approval and it was not deemed necessary to obtain informed consent from all those who contributed a message to the retrieved dataset.

The researcher has been volunteering with domestic abuse charities for over 3 years. In her role as a volunteer, she has received training on how to support victims of IPA and she currently supports victims directly on a weekly basis. This work is part of a larger research project, in which the author is collaborating with several charities focussed on understanding the use of digital technologies within IPA.

Finally, throughout this article, the term *victim* has been used to refer to those currently in an abusive relationship and *survivor* has been used to refer to those who are no longer in an abusive relationship.

3. ANALYSIS

A total of 745 individual posts were included in the data and analyzed following a keyword search method. The keywords that were used are: Android; App; Facebook; FB; Computer; Camera; E-Mail; Find my; Find my Phone; Find my Friends; GPS; Hacked; Hacking; Hijack; iMessage; Instagram; Internet; Intimate Photos; Intimate Pics; Intimate Pictures; iPad; iPhone; Keylog; Laptop; LinkedIn; Location; Malware; Monitoring; Pics; Phone; Photos; Porn; Recording; Revenge Porn; Sext; Smartphone; Snapchat; Social Media; Spyware; Stalkerware; Stalking; Tablet; Text; Tracking; Twitter; Video; Webcam; WhatsApp.

Initial keywords were compiled based on the author's reading of existing work investigating the role of technology in IPA. The keyword list was iteratively modified as the author of this article performed the first and second phases of coding. In this

manner, initial keywords allowed the author to discover new keywords and modify existing ones. Every time a modification was made to the keyword list, all data would be (re-)searched for the new or modified keyword. Whenever a particular keyword was found, the whole post was read, coded, and a transcript was saved. Transcripts were excluded if it was a substantial repetition of a story that had already been included or if they were mostly unrelated to technology-facilitated abuse. They were also excluded if they did not refer to intimate partner abuse, as was the case with some transcripts that described family abuse by a parent or other relative.

During the first phase of descriptive, in vivo, and process coding (Charmaz, 2014; Saldana, 2015), the author developed a codebook with four columns: *name of code, description of the code, example transcripts, connection to other codes*. The codes emerged through analysis of the data and the codebook was edited and revised throughout the process. Once the first phase was concluded, the codebook was reviewed by another researcher to check for consistency between ideas presented in the descriptions, example transcripts, and relationship to other codes. Consensus on the name of the codes, descriptions, and example transcripts was reached in discussion between the researcher and the author. A second analysis of the coded transcripts was then performed, by the author of this article, to remove redundant or infrequent codes, as well as to review the codes assigned to each transcript by observing the codebook (Charmaz, 2014; Saldana, 2015). Once reviewed, a categorization of the data was performed through a process of axial coding until saturation was achieved (Saldana, 2015, pp. 244–247). In other words, reading and re-reading of the data were performed until no new categories were seen in the data. Axial coding also allowed the researcher to plot the relationships between codes and subcodes. These relationships were the basis of a subsequent process of theming the data and findings are reported on according to themes.

According to guidelines on coding as an individual researcher (Saldana, 2015, pp. 37–40), the author of this article engaged in frequent discussions regarding the coding and analysis with an academic research colleague who is well acquainted with this work. Ongoing discussions allowed the author to continually clarify her own internal thinking processes, clarify emergent ideas, and explore potential new angles in the data. Furthermore, the author allowed for a period of at least two weeks between each cycle of coding as a way of distancing herself from the data.

4. FINDINGS

This section is organized according to three main themes that emerged from the analysis of the data:

1. Forms of technology-facilitated abuse;
2. Victims' use of technology within the context of IPA;
3. Peer-support and advice on digital privacy and security.

Each theme is composed of two to four subthemes. Figure 1 provides an overview of the themes, a description of each subtheme, and illustrative transcripts. It is important to highlight that these three themes are not mutually exclusive and, in fact, often overlap with each other. For example, victims may seek information on monitored accounts because they are experiencing this form of abuse.

4.1. Theme 1: forms of technology-facilitated abuse

The first theme focusses on the forms of technology-facilitated abuse discussed on the forums. Forum posts reveal that a combination of abusive techniques is generally used, which means that the forms of technology-facilitated abuse described in this section often overlap with each other, as well as with physical, sexual, and/or emotional abuse. For example, in the transcript below, a forum member describes how digital surveillance led to verbal and physical aggression.

> *My abusive partner used variations of monitoring and surveillance apps to invade my privacy and to justify physical assaults against me. The monitoring and surveillance often lead to verbal and physical assaults. I contacted [name of support organisation removed] but because I am not a resident in that country, they cannot offer me practical forms of support.* [CF]

FIGURE 1. Themes overview, including descriptions and illustrative quotes.

Theme	Subtheme	Description	Example quote
Forms of technology-facilitated abuse	Overt Surveillance	Surveillance refers to perpetrators monitoring victims in a number of ways, such as tracking their location and/or reading their IMs, emails, etc. Surveillance is overt when the victim is aware of being monitored.	*He will go through my phone to check that I'm not flirting with other boys. He also checks my Facebook and Instagram.* [CSF]
	Covert Surveillance	Covert surveillance describes scenarios in which victims are not aware of being monitored or suspect they are being monitored but cannot prove it.	*Is anyone else findings this forum slow to load? It seems very slow to me. I understand if that is normal but I'm paranoid that he's installed tracking software. I am very scared that he will find my posts on this forum.* [NGOF]
	Physical Restrictions to Devices	Refers to the ways in which perpetrators limit victims' access to devices in order to restrict their access to support.	*When I told him that I was going to call the police, he took all the phones and left me in the room.* [NGOF]
	Threats, Harassment and Abuse	Describes how perpetrators leverage technology to continually threaten, harass, intimidate, and otherwise abuse victims.	*If he continues sending me texts, even after the harassment warning has been put in place. What else will he do? He's already shown that he's capable of nearly killing me.* [CF]
Victims' use of Technology	Evidence Gathering	Evidence gathering refers to victims' gathering digital evidence of abuse for 1) legal purposes or 2) for reminding themselves of perpetrators' behaviour.	*You may need a restraining order to keep safe. I needed one. To get a restraining order you will need proof of the abuse. Save all the threatening texts and emails, do not delete them. Take screenshots of anything that contains threats or verbal abuse.* [CF] *I've started recording him speaking to me. I've also started writing things down because I find that I can't always remember what he has said and done. I feel like I sometimes dissociate.* [CF]
	Social Media	Refers to the ways in which victims are using social media within the context of IPA.	*I went on social media, found his ex-wife and sent her an apology for having been "the other woman". Turns out he was also abusive to her and keeps being abusive long after their divorce. We're friends now and we talk often on social media.* [CF]
Peer-Support and Advice on Digital Privacy and Security	Covering Digital Footprints	Refers to advice being exchanged on the forums on how to cover one's own digital footprints.	*Make sure you wipe your internet history. Don't use passwords for this website that he can guess. Hopefully, he doesn't have spyware on your laptop but, just in case, use a computer that isn't in the home.* [CSF]
	Hacked or Hijacked Accounts	Describes advice exchanged on the forums on how to deal with hacked or hijacked accounts.	[In response to a thread about a hacked email account] *Change the password. Maybe change your email address too. I did and it gave me a lot of peace of mind.* [NGOF]
	Spyware	Describes advice exchanged on the forums on how to deal with spyware.	*Maybe you can find tracking software in the apps section of the control panel? You could also check your firewall to see if there is anything that you do not recognise being allowed through. However, if there is tracking software installed, then uninstalling it could make him suspicious. Equally, I'm not sure that searching for information about tracking software is a good idea if you suspect he might be tracking you.* [NGOF]
	Blocking and Communication	Describes the ways in which victims manage their communications with perpetrators.	*If you maintain contact, at least keep it strictly to email. It's probably less disruptive than phone calls or texts.* [NGOF]

This theme is broken down into four subthemes, namely 1) overt surveillance, 2) covert surveillance, 3) restrictions to device access, and 4) threats, harassment, and abuse.

4.1.1. Overt surveillance

Surveillance was widely discussed among forum members. Overt surveillance, where the victim is aware of being monitored, was the most commonly discussed. The nature of intimate relationships means that perpetrators are often able to gain access to victims' devices and accounts, either because they know or can guess the victims' passwords or by coercing/forcing the victim to give them access.

> *I live in my husband and two children. My husband never leaves home, he also won't agree to end the relationship. He becomes abusive whenever I mention any of these things. He also takes my phone, tablet, etc., and threatens to break them unless I give him my passwords.*

In other cases, perpetrators buy and set up all the devices in a household, giving themselves access permissions to the victims' devices. With the emergence of the cloud and the possibility of automatically backing up devices to a central storage location, this means that perpetrators only need a single password to access a great deal of victims' personal information and communications.

> *He bought all our devices! He set all our devices to upload everything (contacts, messages, etc.) to the cloud, which he owns and has a password for. He would get copies of all my emails, appointments, etc.*

Having access to victims' devices and accounts means that perpetrators can monitor activities such as victims' location, movements, and digital communications. Particularly, overt surveillance restricts the ways in which victims can access support. The quote below demonstrates one forum member's difficulty in getting in touch with a support worker, which led her to seek support on the forum.

> *I wish I could call the support worker back but I am at home. He is sleeping, but I only have my mobile phone and the landline phone, and he has access to both of these.* [CF]

In addition to restricting victims' access to professional support, overt surveillance also limits victims' ability to seek support from friends and family. The following transcriptions illustrate how surveillance forces victims into isolation from their closest social connections and creates an environment stripped of the privacy required to access support.

> *He has access to all my emails, my bank account, my phone. Literally everything. Every time I try to get advice from friends or family, he goes through my messages. Now I delete everything. Even this forum post is sent from an email address he doesn't know about using a browser without trackers. I have no privacy and I am always being watched.* [CSF]

> *He forbids me from speaking with my family, including my brother and sister. He used to delete all the contacts off my phone. Whenever he destroyed my phone, he would buy a new one with a new SIM card. Without any contacts on my phone, there was no one I could tell about the abuse.* [NGOF]

Another forum member describes how the perpetrator read text messages that she had exchanged with a friend. In the messages, the victim seeks support and expresses discontent with the intimate relationship. The forum member reports that the perpetrator became physically aggressive and broke the victim's phone, after reading the texts. Incidents such as this – where digital surveillance leads to physical assault – can understandably have the effect of deterring victims from reaching out for support again.

> *He wanted to read my text messages. I explained that none of them were sexual, romantic, or flirtatious in nature, but I did have some texts complaining about our relationship with a friend. This led him to smash my phone into pieces. He then choked me.* [NGOF]

Furthermore, forum posts reveal that perpetrators will attempt to justify abusive behavior by claiming that the victim is *being* unfaithful or intending to do so. Victims' digital communications and social media activity are carefully monitored for any interactions that could be perceived as a *threat* to the romantic relationship. As one forum member describes,

> *He linked himself to my Amazon account so I cannot buy that book [about understanding abuse] online without him knowing. He also checks my online activity and asks about who I may have been talking to. He goes through my Facebook posts and asks me about every man that has left any type of comment: "Who is he? How do you know him? Has he ever been inappropriate?"* [CF]

What is more, as exemplified in the transcript below, perpetrators will leverage allegations of infidelity to enforce further surveillance. In this way, perpetrators' position surveillance as a reaction to victims' behavior. Behavior which is framed as antagonistic to the romantic relationship and, consequently, in need of being changed and/or monitored.

> *After 3 or 4 months together, I started noticing that he checked my phone and email regularly. He lost control over an innocent text that I received from a male friend. He implied that he would put cameras in the bedroom because he didn't believe me when I told him that I did not know why there was a pillow on the floor.* [CSF]

Most of the above examples of overt surveillance rely on perpetrators having physical access to victims' devices in order to carry out surveillance. However, even without access, surveillance was achieved by monitoring victims' posts and interactions on social media, or as the quote below demonstrates, through simple and common app features such as *read receipts*.

> *The man I am dating says that he will beat me if he ever finds me cheating. He says that he is watching me on social media to make sure that I don't fuck him over.* [CF]

> *He knows when I wake up in the morning because he sends me a text at night, after I'm asleep, and when he sees it's been delivered, he knows I'm up. I noticed this because, within 5 minutes of waking up, he's usually at my door.* [CF]

Victims are also expected to always be available through digital technologies, whether it be instant messages (IMs) or phone calls. Victims fear the consequences of not replying immediately or within the timeframe expected by the perpetrator. As one forum member describes, not being immediately available to answer perpetrators' IMs and calls leads to various forms of threats and abuse.

> *He constantly called me when he was away or I was in another place. If I don't answer the phone, or if I don't answer quick enough, he calls me a whore. He leaves voice messages, texts, and emails that are filled with treats and abuse.* [NGOF]

Even when engaged in professional (e.g., at work), social (e.g., out with friends), or personal activities (e.g., sleeping), victims are expected to be available. In some of these cases, it is clear how the ubiquity of digital technologies allows perpetrators to monitor and control aspects of a victim's life that were not possible in the past. As one forum member discusses,

> *He keeps me on the phone for hours at night until I fall asleep while he is still talking. He checks all my calls and messages and I'm not allowed to work 15 minutes late because he'll accuse me of cheating. I must also always be available to pick up the phone, even if I'm at work.* [NGOF]

In addition to always being available, victims are expected to be locatable. Victims are threatened or coerced into sharing their live location data with perpetrators, which is something that would not be possible prior to the ubiquity of smartphones. It, therefore, constitutes a novel and highly invasive form of coercion and control perpetrated through digital technologies.

> *Does anyone else get texts like this from their abuser for no good reason? I literally live on edge and check my phone incessantly because I'm afraid that if I don't answer him immediately, he will spin out of control. I hate this. [Post includes a screenshot of a text message asking the victim to send the perpetrator a pin of her location].* [CSF]

4.1.2. Covert surveillance

Covert surveillance was less common in the forum data. In covert surveillance situations, victims are (initially) not aware they are being monitored. Surveillance is achieved through the use of spyware, keyloggers, or legitimate apps such as those used to track children, pets, and lost devices. In such scenarios, victims may suspect

they are being monitored but have no confirmation and, quite often, no way of proving the surveillance to others. The transcripts below show how victims can be monitored for a long period of time before becoming aware of it.

> *I am looking for people with similar experiences of being monitored through spy apps. My partner installed Zoemob on my phone. I immediately lost all my privacy. It was the perfect tool to perpetrate abuse. Although these apps are extremely invasive, they do not seem to break any laws in [country removed]. Is there anyone else out there who has been monitored in this way? The app was covertly installed so, for a long time, I did not know I was being monitored.* [CF]

Forum posts also showed that members were unsure about how to identify covert forms of surveillance. The nature of spyware requires victims to possess a certain level of technical knowledge in order to 1) know that spyware exists in the first place, 2) correctly identify spyware, 3) remove or have it removed, and 4) ensure the device is not compromised again. This was clearly observed in forum posts where victims ask each other for advice on how to detect and remove spyware. The following transcript illustrates how a victim discovered spyware only after asking for advice on the forum.

> *You [another forum member] were right! I think my phone has been hacked! I looked online for information on figuring out whether a phone has spyware on it. My phone has all of the symptoms: battery running low even when I'm not using it, notifications of incoming text messages but then no actual text messages, the phone's screen lighting up by itself, strange numbers in my recent calls log, and just being really sluggish.* [CF]

Similarly, forum members did not have the technical knowledge required to effectively assess whether an account has been breached or how it had been breached. The post below illustrates this and the measures that this forum member took to re-secure her accounts.

> *I have been on my cloud account from his computer so I don't know if he knew my password or if he hacked my Facebook. I've gone on the cloud and changed my emails address and password. I've changed my password on Facebook and set up text alerts to notify me if someone is trying to log in.* [NGOF]

4.1.3. Restrictions to device access

Forum members often reported cases where perpetrators would intentionally break and/or confiscate their devices, with the aim of limiting access to support or contact with people outside of the relationship. The transcript below shows how the perpetrator confiscated the victim's phone immediately after a physical assault.

> *Today it escalated and he physically assaulted me. I'm fine. I've only got a few bruises so it's nothing serious. Straight after he showed regret and cradled me, bathed me, and dressed me. He took my phone away from me for a while. He's also taken my car and his keys to work today,*

> *so I'll have to stay home all day. He's broken me. All I can do is sit on the couch. I can't face talking to anyone or going anywhere. I know I need to leave him. I'm trying.* [CSF]

In addition to confiscated devices, victims also report that perpetrators remove SIM cards or break their devices during or after an escalation in abuse. In all of these scenarios, the aim is to restrict victims' ability to access support, including from family, friends, professionals, or anyone outside of the romantic relationship.

> *He made sure I had no contact with anyone who would be able to support me. He used to remove the SIM card from my phone, smash my phone, or throw it out of the window. I cannot remember how many phones I had during that time of my life.* [NGOF]

Given the nature of IPA, where abuse takes place within the privacy of a house, a mobile phone may be victims' only way of reaching support. However, as the transcripts show, perpetrators are well aware of this and effectively take steps to remove victims' access to devices and consequent support.

> *When he found out that I was planning to leave him, he broke my mobile phone, disconnected the landline phones, and locked me in the house for four days. He continuously assaulted me over those four days and told me he was going to kill me. He switched off the electricity (during an incredibly hot summer) and did not allow me to drink any water. I honestly thought I was going to die but then I woke up on the last day and he had just disappeared.* [CF]

4.1.4. Threats, harassment and abuse

In addition to surveillance and restricting victims' access to devices, perpetrators also use digital technologies for the purposes of carrying-out ongoing threats, abuse, and harassment. The ubiquity of digital technologies effectively extends perpetrators' reach into almost every aspect of victims' lives. This includes when victims and perpetrators are not physically co-located or in scenarios where internet connectivity would not have been as ubiquitous as it is now (e.g., outside or when commuting). As illustrated by the transcript below, members report that ongoing technology-facilitated abuse has the effect of wearing them down emotionally.

> *The constant barrage of calls and texts sucks the life out of you.* [CF]

What is more, the possibility of receiving real-time threats, at any moment, keeps victims in a constant state of fear and anxiety.

> *I know he is coming here to hurt me. I received several threatening emails from him stating this.* [CSF]

Forum posts also show that persistent harassment extends to victims' friends and family, often leading to the destruction of those relationships.

> *He bombarded me with text messages and phone calls at 4 am. He also contacted the girlfriend that I was out with, bombarding her with abusive messages too. This led her to not want to go out and celebrate her birthday with me. He got his way again.* [CF]

Once a relationship is over and perpetrators effectively lose physical access to victims, abuse and harassment via digital means seem to escalate. The quote below illustrates how perpetrators leverage digital technologies to continue abusing victims, either long after the victim has left or when the victim is attempting to leave.

> *Later that night, after running an errand with one of my children, I return home and nobody is there. One of my children picks me up and we go to my mother's house. He [the perpetrator] calls an hour later asking me where I am. I tell him, he then screams and tells me to never come back. He then hangs up calls again six times leaving voicemails on my phone and on my parents' phone. He then said: "I'm coming to end all of you".* [CF]

After leaving the abusive relationship, victims and their social connections may continue to experience abuse and harassment through e-mail, social media, and other forms of digital communications. This has the effect of placing victims in a state of constant worry that the ex-partner may find out current information about them, such as a phone number or home address. The transcript below illustrates how remote long-term harassment, enabled by technology, can lead victims to worry that they will never escape the abuser.

> *I've changed my phone number and moved into a new house, but he won't stop emailing. He messages my friends, people from work, and my family. Everyone has had to block him. I'm so paranoid about him finding me or my new address. Will this ever end?* [NGOF]

Furthermore, perpetrators' use of new accounts or phone numbers to carry out abuse makes it more difficult for victims to *block* perpetrators, avoid their texts, calls, e-mails, or prove that the abuse is coming from a specific individual.

> *We became friends through playing video games online. Eventually, we began video calling and talking until he told me that he loved me. He would get angry if I wasn't talking to him whenever I wasn't at work or school. When I tried to break-up he would threaten suicide and engage in self-harm. For about a month he's been creating new accounts to harass me on social media, he's made almost 500 new email accounts from which he sends me messages. He's called my phone more than 100 times. He has contacted at least 10 of my friends and family, almost on a daily basis, and keeps threatening to end my life. It has been six months of getting messages from fake accounts that he's made. He stalks me on social media, which I need for my job.* [CSF]

In other cases, perpetrators leveraged digital communications to make attempts to reconnect with victims. Forum members discussed how perpetrators attempt to reenter victims' lives after a period of separation through social media, IM, and e-mail. The following transcript shows how one victim felt manipulated, over texts, into agreeing to reenter the relationship and attend marriage counseling.

> *You won't believe what I did. His [perpetrator's] friend called me, on his behalf, asking to rescind the protection order I had obtained. My ex and I have now been texting. At first, they were harmless texts but yesterday after 5 hours of constant texting I agreed to marriage counselling. How did this happen? I sat in disbelief. He didn't even apologise for threatening and scaring us. I'm beating myself up.* [CF]

Often, forum members were aware that this behavior would repeat itself every time they attempted to end their relationship with the perpetrator.

> *After a breakup, he eventually starts texting me and reels me back in. He will send me long texts about how he loves me, cares for me, and cries when he looks at old pictures of us together.* [CSF]

These forum discussions reflect the delicate nature of intimate partner abuse as a crime where the victim/survivor maintains romantic feelings for the perpetrator. As exemplified by a forum member's post,

> *It's my birthday today. For most of the night and day, I have been checking my phone constantly to see if he texted or emailed me. He hasn't and I am so upset. I'm crying while typing this.* [CF]

Furthermore, victims blamed themselves for maintaining contact with abusive ex-partners, especially if contact then led to renewed abuse. The knowledge of only being an IM, e-mail, or call away means that victims are required to exert immense levels of self-control in order to not contact or respond to perpetrators' communications. In the transcript below, one forum member describes *craving* contact with the perpetrator and how once contact was established, it quite rapidly fell into old patterns of abuse. The victim then blames herself for exchanging IMs with the abusive ex-partner.

> *I craved his contact and he did contact me on Valentine's Day. He was kind and nice for a few texts and then he turned and hurt me again. I should have predicted this. I should have seen it coming.* [CF]

Communication through digital means was also used by perpetrators to convince victims that they had changed. Particularly, the asynchronous nature of IM means that perpetrators can adjust their behavior and consider their replies, making it a lot easier to convince victims of their changed ways. Forum members warned each other of the dangers of maintaining contact with former abusive partners. The following transcript shows how this forum member is hopeful that the perpetrator has reformed, based on their interactions over IM and phone calls.

> *I've been talking with my former partner for the last few days over the phone and Facebook Messenger. We had been apart for a year. He is behaving completely differently. He seems to have changed. He seems happier, he's laughing, saying sweet things, and not getting angry.*

> *Could it be that he has really changed after this amount of time? I really hope so because I feel happy and in love again.* [CSF]

On the other hand, in situations of shared parental responsibilities, perpetrators do not need to create a line of communication but can exploit obligatory childcare-related contact to continue the abuse. The transcript below illustrates a victim's distress in having to communicate with the perpetrator to arrange child contact.

> *My solicitor advised me to set up email contact just for communicating child contact with him, also so that there's an evidence trail of abuse in the future. This opened me up to his abuse again. I don't understand this, just because I'm a parent I have to keep a line of communication open and be prepared to take his abuse? In his mind, this must be a small victory, after we had no contact for several months.* [CSF]

Furthermore, if access to the survivor is limited, perpetrators often attempt to establish contact or gather information through their children. On the one hand, as parents, perpetrators have legitimate reasons to stay connected with their children via digital technologies. However, perpetrators also use children and their devices as tools to continue to harass, stalk, and abuse victims.

> *I explained to my daughter that her father and I will only be communicating via email from now on. She asked if I had done that today. I said "yes". Then she said she could've guessed that because he's been texting her relentlessly today.* [CF]

Finally, the non-consensual sharing of intimate imagery was also identified within the wider umbrella of ongoing threats, harassment, and abuse. Cases of intimate imagery being distributed online were fewer than those solely involving the threat of sharing. Nonetheless, the threat is enough to control and manipulate victims who fear the consequences of having intimate imagery of themselves distributed on the internet.

> *She asked him if he was going to share their sext pics and he responded with "Bitch, what did I tell you about asking me stupid questions?" She pushed back in a calm manner and he went crazy, verbally and over text until she couldn't get out of bed for days.* [CSF]

In addition to sharing intimate imagery without permission, one forum member describes how the perpetrator attempted to extort money from her in exchange for taking the images down.

> *I tried to report the photos my ex used on his pornography site [removed], without my consent, to the police. Unfortunately, they couldn't help and I felt a bit ridiculous afterwards. The photos weren't nude as such so they didn't think there was much they could do. The photos are still online and my ex wants [amount of money removed] to take them down so that he can get more pictures taken.* [CF]

Based on the forum data, it is unclear whether the imagery was captured with or without victims' consent. What is clear is that the threat, or the actual sharing, implicated non-consensual behavior. In some cases, intimate imagery is also shared with victims' immediate social network, as illustrated by the post below.

> *After we broke up, he retaliated by breaking into my Facebook and sending my nudes to every guy he thought I had fucked or wanted to fuck.* [CSF]

4.2. Theme 2: victims' use of technology

This theme focusses on how victims are using technology within the context of IPA. It includes two subthemes, namely 1) evidence gathering, and 2) victims' use of social media.

4.2.1. Evidence gathering

Forum members advised each other to record evidence of physical and digital abuse for legal purposes, such as child custody cases and protection orders. The forum discussions reveal how victims feel that the responsibility of gathering evidence of the abuse is theirs, in order to avoid situations in which it is the victim's version of events versus the perpetrator's. As exemplified by one forum member's advice to another,

> *If you end up in a custody battle with him, it will be your word against his. You will need to prove that he is abusive towards your baby and yourself. Use your phone to record what he is saying when he is being abusive. Also keep the texts, emails, and take pictures of him being abusive. [CF]*

Similarly, in the case of obtaining protection orders, gathering evidence of abuse is seen as essential to proving the abuse to the police. The nature of IPA means that, quite often, the abuse remains hidden until the victim reports it. However, there is a real fear that the police will not take action unless there is a sufficient amount of evidence.

> *If you have evidence of the constant abuse and harassment, the police will issue him with a harassment warning. Keep all the texts, calls, letters, and take photographs of the balloons [delivered to the victim's house]. Create a file of evidence to show to the police. [NGOF]*

In addition to keeping records of digital abuse, victims encouraged one another to record audio/video of the perpetrator being abusive, and take photographs of physical injuries. Furthermore, forum members advised each other to keep detailed written records of abuse in the form of online journal entries.

> *Take photographs of your injuries with your phone. Then save them on the cloud or email them to yourself. Also, describe the incident in as much detail as you can and email that yourself. Do it now while you have time alone. [CSF]*

Evidence was also gathered as an aid for victims to remind themselves of the abusive partner's behavior. Some forum members felt it was helpful to keep records of the abuse that they could then use to remind themselves of what had happened. Victims discussed dissociative behaviors and lapses in memory in relation to abusive incidents, as exemplified by the post below.

> *I don't know how long I stayed after he got physical, for the simple reason that my mind started blocking out the physical violence. I was going through my phone recently and found evidence of another incident three or four months earlier. The way I recorded it makes me think that it wasn't the first time.* [NGOF]

Recording abuse was also seen as a form of combatting *gaslighting*. *Gaslighting* is defined as a set of behaviors carried out with the purpose of manipulating another into feeling that they cannot trust themselves or their own version of events. With recordings, forum members felt they could verify their own version of events against the perpetrator's version, in an attempt to avoid manipulation.

> *I started recording our arguments because he keeps saying I've said things that I know I didn't. Or that he didn't say things I know he did. He has been away this weekend and it gave me time to listen to the recordings. I can't believe how stupid I've been. I am so fed up.* [CF]

Irrespective of the reasons for which victims are attempting to gather evidence themselves, this places them at further risk of abuse. If caught, recording evidence can lead to escalations in abusive behaviors.

> *He started threatening me again and I was secretly recording what was happening. But he caught me, he took my phone, went outside and smashed it on the floor.* [CF]

What is more, forum members are placing themselves at risk in order to gather evidence without knowing whether the recordings are admissible as evidence. The transcripts below show an example of a question being asked about the validity of self-captured evidence, as well as a typical uncertain response to this sort of question.

> *Yesterday he lost it and was verbally abusive. I managed to record the sound on my phone. I'm wondering if without his consent it would be inadmissible in court as evidence?* [NGOF]

> *I'm still looking into the legality of recordings here. I won't use the recordings unless I know I'm legally able to. In the recording, he says he hopes that I'm recording although he didn't actually know I was. I was holding my phone but I recorded the argument on a mini-recorder in my pocket. I don't know if that amounts to consent or not. But I'll find out before using the recording for anything.* [CSF]

4.2.2. Social media

In addition to using digital technologies to gather evidence, forum members also used them to follow abusive former partners' lives, namely through social media platforms such as Facebook and Instagram. Victims report checking former partners profiles, looking at their photos, and seeking information about any new romantic partners. This led to a range of often negative reactions and feelings, alongside a sense that checking on former partners' profiles was a *compulsion* that needed to be managed.

> *I sometimes look up my ex online (Instagram) and for two years I was secretly hoping his new girlfriend would leave him. This week she did. It took time. I also liked the comparison to an addiction [referring to a previous post in the thread], because trauma really does make us go back for more if we let it. Repetition compulsion.* [CSF]

What is more, victims report feelings of re-traumatization linked to viewing abusive former partners' profiles. As exemplified by the words of a forum member,

> *I cringe every time I look at my ex's Facebook page and I get frustrated with myself for doing it. I have not seen him in almost 3 years. I look at his FB page and it feels like I just saw him yesterday. It all comes back.* [CF]

The post below further exemplifies how victims are aware of the negative emotional impact of viewing ex-partners social media profiles and mentions *no contact* as necessary to the healing process. *No contact* refers to absolutely no communication with perpetrators, including *blocking* them on social media, and was widely discussed as best practice throughout the forums.

> *I often wonder what he is doing and which woman has now assumed the main girlfriend role or in other words the abused homemaker and sex slave. I am still terribly curious about who else he was having sex with while he was with me, but only more pain, anger, and sadness lies there. Some days are very hard though, I land up looking at his social media and regretting it. Each day of no contact is truly another day of healing for us survivors.* [NGOF]

In some cases, victims felt that a former abusive partner was using social media to send them particular *secret* messages, or that perpetrators' posts were intended specifically for them.

> *I sometimes watch his videos on YouTube. He posts instructional videos on playing the guitar. What I see now though is someone who is very calculated and sends "messages" through those videos. He wears a wedding ring now. It sends a message. The background in which he is playing sends a message. I know the "message" my ex sends when he goes on YouTube but I don't fall for it. I also know he is not happy.* [CF]

What is more, posts containing references to former partners' new partners were then either 1) interpreted as being posted for benefit of the victim, or 2) lead victims to question whether the abuse had been their own *fault*. The transcript below illustrates this tension quite clearly.

> *I went on social media and decided to look up my abusive ex-boyfriend. Tonight, I found lots of pictures of him, one of him and his wife smiling and looking like a happy couple. Maybe some of his posts are for my benefit? I just have this very tiny voice inside me that says, "maybe it was me, maybe she makes him happy and it was all my fault, all in my head, all my imagination".* [NGOF]

Finally, forum members also used digital technologies to contact perpetrators' new partners. This was done in an effort to protect new partners by warning them about the perpetrator's abusive behavior. In other cases, contact would be made in an effort to understand if the perpetrator had a history of being abusive, with the aim of validating their own experience. Contact was usually established over social media or e-mail.

> *I also got in touch with my ex-boyfriend's wife. He abused her for most of their marriage. It was so nice to have someone else validate my story. I also got a hold of his new girlfriend's e-mail address and I warned her. Initially, she saw all of the abuse towards me and his wife and she left him. Last weekend she married him.* [CSF]

However, and even though survivors reached out in efforts to protect and warn perpetrators' new partners, this initiative was not always well received nor did it have the desired effect.

> *I had many recordings of when we fought, several police reports, and pictures of bruising when he had violently raped me the second time. He has a new partner. They're acting all happy on Facebook: going to church, cooking together, etc. The same things he did with me. I warned her and she laughed at me. But I wasn't going to walk away and let him get away with the damage he has done to me and so many other women.* [CF]

4.3. Theme 3: peer-support and information on digital privacy and security

The third theme focusses on the support and information, exchanged between forum members, regarding digital privacy and security. It is structured according to the three subthemes below, namely 1) covering digital footprints, 2) hacked or hijacked accounts and spyware, and 3) *blocking* and managing communications with perpetrators.

4.3.1. Covering digital footprints

As illustrated in the first theme – *Forms of technology-facilitated abuse* – victims often do not have easy access to a device that they are sure is not being monitored. Therefore, forum members advised each other to cover their online tracks through private browsing, clearing history logs, or avoiding the use of devices that perpetrators are aware of altogether. The post below portrays a series of steps that a forum member took to cover her digital footprints and safeguard digital evidence of the abuse.

> *I've set up an email account that I only log into using private browsing: that way the username & password aren't remembered. I save any notes as draft emails. You could also use OneNote in the same way if you don't already use it for work or for other notes? Just log into OneNote using private browsing, choose a good password and maybe use an email he doesn't know about to sign-up. This will give you a pretty good way of organising notes in case you do decide to use them as evidence or store advice as well as events.* [NGOF]

In situations where victims may be unsure whether a device is being monitored, they advised each other to use a computer in a public space, such as a library. Completely avoiding one's own devices was seen as a foolproof way of ensuring the perpetrator cannot monitor their digital activity in any way.

> *I can't physically help you but I'm always here online if you need support. Just be certain to wipe your internet history and don't use passwords that he knows or can guess. Hopefully, he's not one of those extremely creepy guys that have spyware on your computer. Although just to be safe, I'd use a computer somewhere else.* [CSF]

4.3.2. Hacked or hijacked accounts

In cases where victims knew or suspected that their accounts had been illegitimately accessed by the perpetrator, advice included changing existing passwords or creating entirely new accounts. Furthermore, advice on how to detect a compromised account involved general actions such as checking whether e-mails had been opened or moved to the *trash* folder. The issue with this advice is that perpetrators with basic technical knowledge could easily take steps to not be discovered in these ways.

> *If he has hacked in and deleted emails, are they in the "Trash" folder? If it's Hotmail then you can recover recently deleted emails (if he's deleted them from the inbox and trash folders). If you recover emails you've never seen then you know someone's been in your account. I'm not sure about other email services. I agree with the others that a new email might be best.* [NGOF]

In other cases, victims were aware that their accounts had been hijacked. The post below depicts how the perpetrator has found a workaround that allowed him to use 2-factor authentication – a security measure intended to provide added protection – against the

victim. In this scenario, the victim cannot change her own passwords without alerting the perpetrator and has been advised to create entirely new accounts.

> *She cannot change her passwords because the perpetrator has set up her accounts to use his phone for 2-factor authentication. What she needs is a new email and a new bank account that he does not know about.* [CSF]

4.3.3. Spyware and location tracking apps

Regarding spyware, advice on how to remove it generally revolved around formatting a device or performing a *factory reset*. However, and contrary to the transcript below, most posts sharing advice on spyware did not mention that this type of malicious software can also be transferred from one device to another through restoring old backups. The following post was the only post, in the dataset, that cautioned against transferring content from a compromised device to a new device.

> *Take your child's birth certificate, medical records, and your banking information. Wipe all the computers in the house, set them back to factory, and reformat the hard drives. You must also get a new mobile phone and do not transfer any apps from your old phone onto the new one, just in case he has spyware on there.* [CSF]

Furthermore, advice was not always accurate regarding how spyware can be installed on devices. The forum post below sets out several assumptions that were made on the forums, namely 1) that installing spyware on a device requires high levels of technical expertise, and 2) that spyware/malware cannot be installed remotely.

> *I don't think that is possible: remote tracking is unlikely unless he is a technology genius. Tracking cookies are set up by sites, not by individuals. I would clear your cache if I were you and run Superantispyware. Then I would run Malwarebytes. When you have finished uninstall these because they take up a lot of space. Very often this will alleviate a slow pc. If you do not live with this man, it is very unlikely he can track you except on social media (like Facebook). In which case delete your account there.* [NGOF]

What is more, in cases where spyware is identified, removing it may not always be the best course of action. Removing spyware effectively alerts perpetrators to victims' knowledge of the surveillance and removes an avenue through which abuse can be carried out, which can lead to increased risk for the victim. Similarly, the post below also demonstrates how searching online for information about spyware may, in itself, be risky for victims.

> *I'm not sure, maybe you can find tracking software in the programs/apps part of your control panel? Or can you check your firewall and see if there's anything that you don't recognise being allowed through? If there is tracking software then uninstalling it could make him suspicious,*

> *so be careful. Also, I don't think Googling information about tracking software is a good idea if you think he's tracking you.* [NGOF]

In addition to spyware, there are many apps on official app-stores that can be used by IPA perpetrators to monitor victims. Examples of such apps are those used to track children, pets, or lost devices. What was found in the data is that victims are generally unclear on the difference between legitimate apps that share users' location data and spyware. This is demonstrated in the post below, where the forum member describes an app that her daughter and the daughter's boyfriend have for consensually sharing each other's location, as a response to a question about spyware. The post goes on to suggest a *factory reset* of the victim's device, which would not necessarily remove a legitimate app such as Find my Friends. The advice exchanged on the forums, regarding these apps, does not necessarily lead to increased security for victims. In fact, the advice could put victims at more risk due to a false sense of security.

> *There are apps that people can download on their phones to know where you are. It isn't difficult to do. My daughter has an app where she and her boyfriend can see each other's location. It is very easy. You should factory reset your phone and change all your passwords. Your phone is probably very compromised at this point.* [CF]

4.3.4. Blocking and managing communication

In cases where victims are required to maintain contact with perpetrators (e.g., shared custody arrangements), forum members advised managing contact through e-mail or another asynchronous mode of communication, instead of face-to-face interactions or phone calls. Asynchronous communication was seen as a way of allowing victims to read communications and reply when they felt able to do so, rather than having to respond to the perpetrator in real-time.

> *If you have children together, create an email account for parenting only and delete any emails that don't relate to the children immediately. That way you can look at the emails when you're feeling strong or when somebody is there to help you.* [CF]

Furthermore, managing communications through IM or e-mail also allows victims to keep records of abusive content. As one forum member advises in response to another's distress regarding court-mandated contact with an abusive ex-partner,

> *A few things that may help to give you back some control: start keeping every text, every e-mail, and record his conversations with you. Start gathering evidence or proof of his abuse. Your ex will do anything to hurt you. Try to be brave and keep a record of what he does.* [CF]

Finally, when communication with perpetrators is not necessary, forum members advised each other to *block* perpetrators on social media, *block* all their shared contacts, and be cautious about who may be able to view their posts. Victims

were also advised to change their phone number and screen any calls from numbers that they did not recognize.

> *You need to keep safe and remove all means of contact. This means blocking her on everything: phone, email, etc. Set your social media profiles to private, block her and everyone related to her, post things as "friends only". Remove everyone that you don't know in real life. Do not answer calls from numbers that you don't know. Change your phone number if she keeps harassing you through unknown numbers.* [CSF]

All these strategies effectively place the burden on victims to protect themselves from perpetrators' digital abuse and harassment. What is more, they require continuous labor in *blocking* new accounts and phone numbers that perpetrators create to continue abusing victims.

5. DISCUSSION

This work builds on previous studies by reviewing data from three online domestic abuse forums where victims of IPA engage in peer-support. Specifically, the purpose of this study was to further current knowledge regarding:

- the forms of technology-facilitated abuse being discussed by victims engaging in online peer-support;
- how victims are using technology within the context of IPA;
- the quality of digital security and privacy advice being exchanged between forum members.

Through a qualitative analysis of the forum data a series of tensions related to digital technologies within the context of IPA were revealed. Firstly, digital technologies play a dual role in that they are being used as tools for abuse but also as means for survivors to manage mandated contact with perpetrators, as well as to warn and communicate with abusive former partners' new and ex-partners. Secondly, the results show that the ubiquity of digital technologies extends perpetrators' reach into almost every aspect of victims' lives, enabling both overt and covert forms of surveillance. Thirdly, victims are engaged in collecting digital evidence of abuse themselves, even though forum discussions also reveal that members are not sure whether such evidence is admissible in court. Finally, managing digital privacy and security is a potentially high-stakes endeavor, which is complex and labor-intensive task for victims. The subsections below discuss each of these tensions in more detail.

5.1. The dual role of digital technologies within IPA

The results reveal that the technologies used to perpetrate abuse against victims of IPA are the same tools that victims often rely on themselves. Perpetrators use digital technologies to monitor, stalk, harass, and intimidate victims. Victims use the same technologies to gather evidence of abuse, to warn perpetrators' other romantic partners, or to contact perpetrators' former partners with the aim of validating their own experiences.

An example of this duality is how social media is used. On the one hand, the findings show that perpetrators leverage social media to harass and monitor victims in a number of ways. This included monitoring victims' activity on social media, hijacking their accounts, and/or sending non-consensual intimate imagery to victims' contacts, which aligns with previous research alongside victims engaged with support services (Dimond et al., 2011; Freed et al., 2017, 2018; Harris & Woodlock, 2018; Matthews et al., 2017; Southworth et al., 2007; Woodlock, 2016). On the other hand, this work extends current knowledge by showing that victims are also using these platforms to contact perpetrators' new partners in an effort to warn them of perpetrators' abusive behavior or to validate their own experiences of abuse by comparing "war stories" – in the words of one forum member. In light of this, and although social media may put victims at risk of further or continued abuse and harassment, it also seems to constitute an important avenue for survivors to take back control by supporting or warning other potential victims. Research has shown that peer-support can be beneficial to recovery in a number of contexts (Coulson & Knibb, 2007; Hargreaves et al., 2018; Kummervold et al., 2002; Melling & Houguet-Pincham, 2011; Naslund, Aschbrenner, Marsch, & Bartels, 2016; Niela-Vilén, Axelin, Salanterä, & Melender, 2014), therefore, maintaining this particular use of social media may indeed be important for some survivors. Accordingly, in order to limit the risk of abuse while still being able to use social media, forum members advised each other to *block* perpetrators across social media platforms.

However, *blocking* perpetrators does not always guarantee victims' privacy. In the context of IPA, where a wide range of social connections is potentially shared, achieving privacy would require victims to remove all shared connections from their social media accounts. Furthermore, it would require victims to constantly monitor whether perpetrators are adding new shared *friends*, which could render content uploaded by victims' *friends* – in which the survivor is *tagged* – available to the perpetrator. On Facebook, for example, a perpetrator that has been *blocked* may still see photos with the victim in them, as long as they were posted by a shared *friend*. Even though solutions that respond to the complexity of multi-party privacy have been proposed and evaluated by researchers (Besmer & Richter Lipford, 2010; Carminati & Ferrari, 2011; Hu, Ahn, & Jorgensen, 2013; Ilia, Polakis, Athanasopoulos, Maggi, & Ioannidis, 2015; Such & Criado, 2016; Thomas, Grier, & Nicol, 2010), these have not been widely adopted by commercial platforms, nor have they been evaluated within the context of IPA.

Furthermore, the findings support the concept of an added layer of tension in IPA where victims/survivors may still have romantic feelings for perpetrators (Dutton & Painter, 1993; Herman, 2015; Kearney, 2001). This was especially evident when victims discussed the *compulsion* of following abusive ex-partners' lives on social media or *craving* contact from perpetrators – which, to the best of our knowledge, has not been discussed in previous research. Such discussions also showed that victims were fully aware of the negative emotional impact of such behaviors, which had to be managed in a conscious effort to refrain from any contact with the abusive ex-partner. This tension renders managing digital privacy and security more of a challenge for survivors of IPA. On the one hand, survivors want to safeguard themselves from further abuse, whilst on the other hand may be reluctant to relinquish access to abusive ex-partners' profiles.

Evidence has shown that monitoring a former partner's online activity increases negative affect and delays recovery (Fox & Tokunaga, 2015; Marshall, 2012). It is, therefore, unsurprising that victims express negative feelings related to viewing ex-partners' profiles. Novel approaches to dealing with privacy management on social networks are necessary as they are currently ill-equipped to deal with the complexity of human relationships online, offline, and at the intersection between on and offline. Recent work has begun to address issues of design around digital decoupling and disentangling following the termination of an intimate relationship (Herron, Moncur, & van den Hoven, 2016, 2017; Moncur, Gibson, & Herron, 2016). Including survivors of IPA, in further work on digital decoupling, is not only essential but may also benefit the design of social networks for anyone experiencing the end of a romantic partnership.

Finally, in the context of the dual role of digital technologies, it is worth considering the current landscape of support provision and access. For example, in the UK where the lead researcher has experience of volunteering with IPA support services, many such services are accessible to the public through websites, phone numbers, and/or e-mail addresses. Victims are required to get in touch through these means, rather than through physical walk-in premises. Alternatively, victims can also be referred to a support service by the police, social services, or another relevant agency. The support service will then attempt to contact the victim via phone call or e-mail, depending on the victim's stated preference. Once a victim has established contact or has been contacted, support is then organized to be delivered over the phone or face-to-face, with dates and times being organized either over e-mail, text, or phone call. This setup effectively means that victims are required to have a safe device in order to access and arrange for support.

Unfortunately, as our findings and other work (Dimond et al., 2011b; Freed et al., 2017, 2018; Marganski & Melander, 2015; Matthews et al., 2017; Snook et al., 2017; Southworth et al., 2007) have shown, victims often experience difficulty in accessing a safe device that is not being overtly or covertly monitored by the perpetrator, which in turn limits their ability to safely access support services. Current risk assessment processes (Campbell, 2004; Campbell & Messing, 2017,

pp. 145–152; Hilton, Harris, & Rice, 2010, pp. 151–170; Richards, 2016) do not include questions specifically aimed at assessing whether the victim has access to a safe device. For example, support workers may ask victims about their preferred mode of contact, but do not generally have the training nor the knowledge to understand whether, for example, spyware may be installed on a device or whether a victim's location is being tracked through legitimate apps such as Find My Friends. Such findings provide further evidence for the need to integrate domestic abuse screening and support into routine medical care (Miller, McCaw, Humphreys, & Mitchell, 2015; Taket et al., 2003; Warren-Gash et al., 2016), mental health services (Hamberger & Phelan, 2006), maternity care services (Rodgers, Grisso, Crits-Christoph, & Rhodes, 2017), accident and emergency (SafeLives, 2016), and other contexts in which individuals come into contact with professionals who could be trained to identify signs of abuse and provide an entry point to support. How support is then managed on a regular basis would require professionals to be capable of assessing whether the victim is being surveilled through digital means.

5.2. The issues and advantages of digital ubiquity

The ubiquity of digital technologies means that victims are required to be available at all times by responding to perpetrators' texts, phone calls, and e-mails. A particular manifestation of these behaviors can be witnessed in victims' accounts of perpetrators leveraging the ubiquitous nature of location data to threaten and/or coerce them into sharing a *pin* of their real-time whereabouts. Previous research highlighted the use of stalkerware or apps such as Find my Friends as means for tracking victims' movements, which would require perpetrators accessing a victim's phone, even if just once for installing an app or authorizing data sharing (Freed et al., 2017, 2018; Matthews et al., 2017). What the forum data shows is that perpetrators can exploit the real-time ubiquity of such data through coercion and control even without compromising victims' devices. This can be achieved simply by demanding that a victim share their location and instilling fear of noncompliance. In this way, perpetrators render it almost impossible for a victim to go anywhere, or access support, without the concern that the perpetrator may demand a *pin* of their location at any time.

Before the ubiquity of digital technologies and in order to monitor an individual's location, perpetrators would have to physically stalk victims whilst expending large amounts of time and effort. Digital surveillance, on the other hand, allows perpetrators to monitor victims remotely with a lot less effort. Nevertheless, it could be argued that digital surveillance may be safer for the victim as it does not require the perpetrator to be physically present, therefore, reducing the risk of bodily harm. However, what the forum data has shown is that even though the victim may not be in immediate physical danger, the knowledge of being monitored and the barrage of abusive and threatening digital communications often leads to constant and heightened states of anxiety and fear.

On the other hand, the ubiquity of digital technologies means that, in some cases, survivors have more control and power in managing their interactions with abusive former partners. Custody arrangements often require survivors to maintain lines of communication open with perpetrators in order to organize and manage contact with shared children (Rizo et al., 2017). Before e-mail and IM were widespread, these conversations would likely need to happen face-to-face or over the phone. What the forum data showed is that survivors are using digital forms of communication to manage such interactions in a way that feels safer and more empowering to themselves. Survivors discussed the asynchronous nature of e-mail and how it allows for messages to be read and replied to when the survivor feels capable of doing so, rather than having to react in real-time. Furthermore, contact via means such as e-mail or IM, rather than phone calls, also enables survivors to save evidence of abusive communications. In scenarios where a survivor is managing custody arrangements via e-mail, these e-mails can be stored and used as evidence if the perpetrator is exploiting court-mandated contact to continue threatening, harassing, and/or any other form of abusive behavior. It would be much more difficult to record these abusive interactions if they were taking place over phone calls or in person.

5.3. The onus of collecting and storing digital evidence

Forum data reveals that victims are making use of digital technologies to record evidence of abuse for legal purposes, which aligns with previous findings (Freed et al., 2017). In the case of IPA, the onus of collecting evidence of abuse is largely placed on the victim (Navarro, Clevenger, & Marcum, 2016, p. 168) and the forum data shows how victims attempt to record video/audio of the abuse, save abusive IMs and posts, and keep an archive of abusive e-mails. However, the findings also demonstrate how perpetrators often have access to victims' devices, meaning that the evidence is vulnerable to being deleted by perpetrators, or in fact that some victims may be reluctant to store evidence in the first place as this may place them at further risk.

What is more, the ephemerality of digital content and the possibility of perpetrators sending content from accounts or phone numbers that would be difficult to track down (e.g., call spoofing (SpoofCard, 2018)), means that victims are required to keep records of the abuse without being sure whether the evidence will be admissible in court. If the source cannot be traced, or if only a section of a conversation is stored as evidence, this may put into question the evidence's validity and the integrity of its chain-of-custody (Prayudi & Sn, 2015). In some cases, it may be possible to rely on evidence gathered by the police, hospital admissions, or third-party witnesses. Yet, recent reports have found the police to be ineffective in gathering evidence from domestic abuse crime scenes (Cerulli, Edwardsen, Hall, Chan, & Conner, 2015; HMIC, 2014; HMICFRS, 2017; PERF,

2015; Ruff, 2012; Westera & Powell, 2017), which effectively means that the burden is shifted onto victims themselves.

What is more, and extending existing research, our findings show how victims are also collecting evidence as a way of reminding themselves of the abusive partner's behavior. Victims of domestic abuse often suffer from memory loss and dissociative behaviors (Ellsberg, Jansen, Heise, Watts, & Garcia-Moreno, 2008; Gleason, 1993), which may explain why forum members recorded evidence of abuse to then replay to themselves. Another explanation may be related to *gaslighting*. *Gaslighting* refers to processes of *"emotional manipulation in which the gaslighter tries (consciously or not) to induce in someone the sense that her reactions, perceptions, memories and/or beliefs are not just mistaken, but utterly without grounds paradigmatically, so unfounded as to qualify as crazy"* (Abramson, 2014, p. 2). In this case, victims may be recording the abuse in order to resist emotional manipulation and verify their version of events.

In either case, if victims are collecting their own evidence of abuse then it needs to be ensured that appropriate structures are put into place to guarantee that such data is retrieved and stored in a manner that is secure and admissible as evidence (Prayudi & Sn, 2015). Even in cases where evidence may initially be captured without the intention of using it for legal purposes, it may nonetheless assume this end if the police and prosecution services become involved. Therefore, there is a role for technologists to play in the development of tools for safely and securely storing evidence of IPA that is collected by victims. What is more, ongoing discussions and training on gathering digital evidence within domestic abuse cases are essential. Such discussions need to include agencies such as the police, health services, social services, prosecution services, as well as third-sector support organizations and victims themselves in an upscaling of competencies in dealing with the capture and storage of digital evidence.

5.4. The labor of managing digital privacy and security

Managing digital privacy and security, whether at a smartphone app level or on social media, has been recognized as a challenge for many users (Felt et al., 2012; Liu, Gummadi, Krishnamurthy, & Mislove, 2011; Yu et al., 2018). The main issues are related to cognitive overload as well as the usability of privacy and security controls. Estimates indicate that, on average, users are required to make over 100 permission decisions for the apps on their mobile devices alone (B. Liu et al., 2016). Prior work has also shown that users are often unaware, or uncomfortable, with permissions they had consented to at some point in the past (Almuhimedi et al., 2015; Felt et al., 2012).

Given this landscape, it is unsurprising that forum members did not always understand how legitimate apps, such as Find My Friends or Facebook, could be sharing their location with other users. The author believes that several scenarios could further complicate understanding which data is being shared, such as situations in which 1) a victim did not set up their own device (e.g., it was a gift from the

perpetrator), or 2) if the perpetrator had access to the victim's phone and granted permission for certain apps to share their location with specific audiences or individuals, or even 3) if the user did not change their devices' and accounts' default settings. It is well documented that the complexity of understanding which information is shared with who can often lead to unintended breaches in privacy (Garg, Benton, & Camp, 2014; Y. Liu et al., 2011; Wisniewski, Knijnenburg, & Lipford, 2017). Previous work has shown that private versus public boundaries on social media are unclear to users (Barth & de Jong, 2017; Yu et al., 2018), who may be sharing information more widely than expected (Barnes, 2006; Mondal, Messias, Ghosh, Gummadi, & Kate, 2017). In the case of victims of IPA, these breaches can have serious consequences and a direct impact on their safety.

In addition to managing the complexities of privacy for legitimate apps, victims may also have to deal with privacy concerns related to illegitimate apps such as spyware. In these situations, and given the covert nature of spyware, the process of managing one's own privacy and security becomes even more complex. Accordingly, forum discussions revealed that detecting spyware on devices is not a straightforward process for victims. Advice exchanged between forum members involved looking for signs of a device's battery running low quicker than usual, screen glitches, and disappearing text messages. Although some of these may be indicators, they are not effective methods of identifying spyware. Forum members also advised each other to perform *factory resets* on their devices in order to remove malicious software. However, advice generally failed to address the issue of restoring devices from backups that may have been compromised. Incomplete or inaccurate advice on how to deal with security and privacy threats can place victims at further risk, related to a false sense of security. Existing research has found similar issues with advice being given by professional support workers regarding digital privacy and security. Support workers are insecure in their own knowledge and ability to provide such support and fear that incorrect advice could increase the risk for the victims they are attempting to support (Freed et al., 2017).

In this context, more effective tools for detecting and removing spyware, as well as for managing privacy and security are necessary. Not only are improved tools required but such tools need to be developed alongside professional support workers, victims, and survivors, in an effort to guarantee that they are context-appropriate, safe, effective, and easy to use. It is therefore essential that research and development, both in industry and academia, engage with these users in developing privacy and security mechanisms. In fact, in many cases involving users with extreme needs regarding privacy and security can be a catalyst for innovations that are valuable to the general public (Lettl, Herstatt, & Gemuenden, 2005; Newell, Gregor, Morgan, Pullin, & Macaulay, 2011; Pullin & Newell, 2007).

Finally, it is the author's aim that these findings inform policy development regarding citizens' digital privacy, in a push for improved privacy-by-design. For example, privacy controls should enable users to more quickly and effectively manage the social connections they are sharing a specific piece of content with, understand exactly which content is available to whom, and determine for how long it will be

available. Given the longevity of data published online that may, in fact, outlive individuals, mistakes related to misunderstandings on how widely information is being shared can have serious and/or long-term consequences, not only for victims of IPA. Although the General Data Protection Regulation has recently implemented corporate regulations for the storing and processing of European Union citizens' data (European Parliament & Council of the European Union, 2016), further efforts are required in developing appropriate standards and controls that enable users to understand and manage the information they are sharing publicly and/or between peers.

5.5. Limitations

The analysis of data from online forums limits the findings' generalizability to victims and survivors of IPA who do not engage in online peer-to-peer support. Not only is the study limited to victims and survivors posting online, but it also refers to only three forums of a much larger body of online domestic abuse forums and is, therefore, not representative of all victims and survivors discussing IPA online. Furthermore, this study focussed on domestic abuse support forums where content was written in English, therefore excluding victims and survivors who communicate in other languages. This may indeed significantly reduce the sources of data to a particular set of geographic locations and, therefore, these findings are not generalizable beyond that scope. Similarly, given the nature of such forums, demographic data was not gathered. The lack of demographic data means that, for example, findings are not differentiated based on gender, sexuality, nor by age of abusers and victims.

6. CONCLUSION

The aim of this work was to extend existing knowledge regarding technology-facilitated IPA, which has focussed on professional support workers and victims engaged with formalized support services, by including the experiences of victims engaged in online peer-support. The findings reveal 1) the ways in which perpetrators are using digital technologies to reach into victims' private, social, and professional lives in ways that were not possible before the ubiquity of these technologies; 2) how victims are using technology within the context of IPA to gather evidence, as well as to support and warn other victims; and 3) that the digital privacy and security advice being exchanged on forums is not always accurate or complete.

In the discussion, the author argues, amongst other points, that improvements need to be made with regards to digital privacy and security tools, as well as policy practices in order to manage the complexities of human relationships and privacy management between peers. Secondly, better tools for securely retrieving and storing IPA evidence gathered by victims are required. Finally, risk assessment

procedures need to be updated and support workers need further training in detecting and dealing with technology-facilitated abuse.

NOTES

Funding. This work is funded by the Arts and Humanities Research Council, through the London Doctoral Consortium.
This article is based on the author's PhD work.

HCI Editorial Record. First received on <date>. Revisions received on <date>, <date>, and <date>. Accepted by <action-editor-name>. Final manuscript received on <date>. – *Editor*

The HCI Editorial Record paragraph will be filled in by the HCI Editors.

REFERENCES

Abramson, K. (2014). Turning up the lights on gaslighting. *Philosophical Perspectives*, *28*(1), 1–30. doi:10.1111/phpe.12046

Ackland, R. (2013). *Web social science: Concepts, data and tools for social scientists in the digital age* (1st ed.). London, UK: Sage Publications Ltd.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., … Agarwal, Y. (2015). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 787–796. doi:10.1145/2702123.2702210

Attard, A., & Coulson, N. S. (2012). A thematic analysis of patient communication in Parkinson's disease online support group discussion forums. *Computers in Human Behavior*, *28*(2), 500–506. doi:10.1016/j.chb.2011.10.022

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday: Peer-Reviewed Journal on the Internet*, *11*(9). doi:10.5210/fm.v11i9.1394

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Bent-Goodley, T. B. (2007). Health disparities and violence against women: Why and how cultural and societal influences matter. *Trauma, Violence, & Abuse*, *8*(2), 90–104. doi:10.1177/1524838007301160

Besmer, A., & Richter Lipford, H. (2010). Moving beyond untagging: photo privacy in a tagged world. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1563–1572. doi:10.1145/1753326.1753560

Black, M. C., Basile, K. C., Breiding, M. J., Smith, S. G., Walters, M. L., Merrick, M. T., … Stevens, M. R. (2011). *National intimate partner and sexual violence survey: 2010 summary report*. Retrieved from National Center for Injury Prevention and ControlCenters for Disease Control and Prevention website: https://www.cdc.gov/ViolencePrevention/pdf/NISVS_Report2010-a.pdf

British Psychological Society. (2017). *Ethics guidelines for Internet-mediated research* (No. INF206/04.2017). Retrieved from Author website: www.bps.org.uk/publications/policy-and-guidelines/research-guidelines-policy-documents/research-guidelines-poli

Burman, E., & Chantler, K. (2005). Domestic violence and minoritisation: Legal and policy barriers facing minoritized women leaving violent relationships. *International Journal of Law and Psychiatry*, *28*(1), 59–74. doi:10.1016/j.ijlp.2004.12.004

Campbell, J. C. (2004). Danger assessment. Retrieved from Danger Assessment website: https://www.dangerassessment.org/DA.aspx

Campbell, J. C., & Messing, J. (2017). *assessing dangerousness, third edition: Domestic violence offenders and child abusers*. New York, NY: Springer Publishing Company.

Carminati, B., & Ferrari, E. (2011). Collaborative access control in on-line social networks. *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)*, 231–240. doi:10.4108/icst.collaboratecom.2011.247109

Cerulli, C., Edwardsen, E. A., Hall, D., Chan, K. L., & Conner, K. R. (2015). Improving coordinated responses for victims of intimate partner violence: Law enforcement compliance with state-mandated intimate partner violence documentation. *Violence Against Women*, *21*(7), 897–907. doi:10.1177/1077801215584072

Charmaz, K. (2014). *Constructing grounded theory: Introducing qualitative methods series* (2nd ed.). London, UK: SAGE Publications.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., … Ristenpart, T. (2018). The spyware used in intimate partner violence. *2018 IEEE Symposium on Security and Privacy (SP)*, 441–458. doi:10.1109/SP.2018.00061

Coulson, N. S., & Knibb, R. C. (2007). Coping with food allergy: Exploring the role of the online support group. *CyberPsychology & Behavior*, *10*(1), 145–148. doi:10.1089/cpb.2006.9978

Crawford, G., Maycock, B., Tobin, R., Brown, G., & Lobo, R. (2018). Prevention of HIV and Other Sexually Transmissible Infections in Expatriates and Traveler Networks: Qualitative Study of Peer Interaction in an Online Forum. *Journal of Medical Internet Research*, *20*(9), e10787. doi:10.2196/10787

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with Computers*, *23*(5), 413–421. doi:10.1016/j.intcom.2011.04.006

Duke, A., & Davidson, M. M. (2009). Same-sex intimate partner violence: Lesbian, gay, and bisexual affirmative outreach and advocacy. *Journal of Aggression, Maltreatment & Trauma*, *18*(8), 795–816. doi:10.1080/10926770903291787

Dutton, D. G., & Painter, S. (1993). Emotional attachments in abusive relationships: A test of traumatic bonding theory. *Violence and Victims; New York*, *8*(2), 105–120. doi:10.1891/0886-6708.8.2.105

Ellsberg, M., Jansen, H. A., Heise, L., Watts, C. H., & Garcia-Moreno, C. (2008). Intimate partner violence and women's physical and mental health in the WHO multi-country study on women's health and domestic violence: An observational study. *The Lancet*, *371*(9619), 1165–1172. doi:10.1016/S0140-6736(08)60522-X

European Parliament, & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council on on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Pub. L. No. 32016R0679, 119 OJ L 1, Official Journal of the European Union, European Union.

European Union Agency for Fundamental Rights. (2014). *Violence against women: An EU-wide survey*. Luxembourg: Author. European Union.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *British Medical Journal*, *323*(7321), 1103–1105. doi:10.1136/bmj.323.7321.1103

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 3. doi:10.1145/2335356.2335360

Femi-Ajao, O., Kendal, S., & Lovell, K. (2018). A qualitative systematic review of published work on disclosure and help-seeking for domestic violence and abuse among women from ethnic minority populations in the UK. *Ethnicity & Health*, 1–15. doi:10.1080/13557858.2018.1447652

Fox, J., & Tokunaga, R. S. (2015). Romantic partner monitoring after breakups: Attachment, dependence, distress, and post-dissolution online surveillance via social networking sites. *Cyberpsychology, Behavior, and Social Networking*, *18*(9), 491–498. doi:10.1089/cyber.2015.0123

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A stalker's paradise". *How Intimate Partner Abusers Exploit Technology. Proceedings Of The*, 1–667. doi:10.1145/3173574.3174241

Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1(CSCW)*, *46*, 1–46: 22. doi:10.1145/3134681

García-Moreno, C., Jansen, H. A. F. M., Ellsberg, M., Heise, L., & Watts, C. (2005). *WHO multi-country study on women's health and domestic violence against women*. Retrieved from World Health Organization website: http://www.who.int/reproductivehealth/publications/violence/24159358X/en/

Garg, V., Benton, K., & Camp, L. J. (2014). *The privacy paradox: A Facebook case study*. Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy. Presented at the The 42nd Research Conference on Communication, Information and Internet Policy, Arlington, VA.

Gleason, W. J. (1993). Mental disorders in battered women: An empirical study. *Violence and Victims; New York*, *8*(1), 53–68.

Hamberger, K., & Phelan, M. B. (2006). Domestic violence screening in medical and mental health care settings. *Journal of Aggression, Maltreatment & Trauma*, *13*(3–4), 61–99. doi:10.1300/J146v13n03_04

Hargreaves, S., Bath, P. A., Duffin, S., & Ellis, J. (2018). Sharing and empathy in digital spaces: qualitative study of online health forums for breast cancer and motor neuron disease (Amyotrophic lateral sclerosis). *Journal of Medical Internet Research*, *20*(6), e222. doi:10.2196/jmir.9709

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

Herman, J. L. (2015). *Trauma and recovery: The aftermath of violence — From domestic abuse to political terror*. New York, NY: Basic Books.

Herron, D., Moncur, W., & van den Hoven, E. (2016). Digital possessions after a romantic break up. *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, *36*, 1–36: 10. doi:10.1145/2971485.2971539

Herron, D., Moncur, W., & van den Hoven, E. (2017). Digital decoupling and disentangling: Towards design for romantic break up. *Proceedings of the 2017 Conference on Designing Interactive Systems*, 1175–1185. doi:10.1145/3064663.3064765

Hilton, N. Z., Harris, G. T., & Rice, M. E. (2010). *Risk assessment for domestically violent men: Tools for criminal justice, offender intervention, and victim services*. Retrieved from http://www.apa.org/pubs/books/4318055.aspx

HMIC. (2014). *Everyone's business: Improving the police response to domestic abuse*. Retrieved from Her Majesty's Inspectorate of Constabulary website: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/improving-the-police-response-to-domestic-abuse/

HMICFRS. (2017). *A progress report on the police response to domestic abuse* (No. 978-1-78655-586–1). Retrieved from Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services website: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/progress-report-on-the-police-response-to-domestic-abuse.pdf

Holtz, P., Kronberger, N., & Wagner, W. (2012). Analyzing internet forums: A practical guide. *Journal of Media Psychology: Theories, Methods, and Applications*, *24*(2), 55–66. doi:10.1027/1864-1105/a000062

Hu, H., Ahn, G., & Jorgensen, J. (2013). Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, *25*(7), 1614–1627. doi:10.1109/TKDE.2012.97

Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., & Ioannidis, S. (2015). Face/off: Preventing privacy leakage from photos in social networks. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 781–792. doi:10.1145/2810103.2813603

Im, E.-O., & Chee, W. (2012). Practical guidelines for qualitative research using online forums. *Computers, Informatics, Nursing*, *30*(11), 604–611. doi:10.1097/NXN.0b013e318266cade

Kearney, M. H. (2001). Enduring love: A grounded formal theory of women's experience of domestic violence. *Research in Nursing & Health*, *24*(4), 270–282. doi:10.1002/nur.1029

Kimmerle, J., Bientzle, M., & Cress, U. (2014). Personal experiences and emotionality in health-related knowledge exchange in internet forums: A randomized controlled field experiment comparing responses to facts vs personal experiences. *Journal of Medical Internet Research*, *16*(12), e277. doi:10.2196/jmir.3766

Kulwicki, A., Aswad, B., Carmona, T., & Ballout, S. (2010). Barriers in the utilization of domestic violence services among arab immigrant women: Perceptions of professionals, service providers & community leaders. *Journal of Family Violence*, *25*(8), 727–735. doi:10.1007/s10896-010-9330-8

Kummervold, P. E., Gammon, D., Bergvik, S., Johnsen, J.-A. K., Hasvold, T., & Rosenvinge, J. H. (2002). Social support in a wired world: Use of online mental health forums in Norway. *Nordic Journal of Psychiatry*, *56*(1), 59–65. doi:10.1080/08039480252803945

Laxton, C. (2014). *Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking*. Retrieved from https://www.womensaid.org.uk/virtual-world-real-fear/

Lettl, C., Herstatt, C., & Gemuenden, H. G. (2005). Learning from users for radical innovation. *International Journal of Technology Management*, *33*(1), 25–45. doi:10.1504/IJTM.2006.008190

Liu, B., Andersen, M. S., Schaub, F., Almuhimedi, H., Zhang, S., Sadeh, N., … Agarwal, Y. (2016). *Follow my recommendations: A personalized privacy assistant for mobile app permissions*. Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (pp. 27–41). Berkeley, CA, USA: USENIX Association.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 61–70. doi:10.1145/2068816.2068823

Lovatt, M., Bath, P. A., & Ellis, J. (2017). Development of trust in an online breast cancer forum: A qualitative study. *Journal of Medical Internet Research*, *19*(5), e175. doi:10.2196/jmir.7471

Marganski, A., & Melander, L. (2015). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, 0886260515614283. doi:10.1177/0886260515614283

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: Associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior, and Social Networking*, *15*(10), 521–526. doi:10.1089/cyber.2012.0125

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., … Consolvo, S. (2017). Stories from survivors: Privacy & security practices when coping with intimate partner abuse. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2189–2201. doi:10.1145/3025453.3025875

McClennen, J. C., Summers, A. B., & Vaughan, C. (2008). Gay men's domestic violence: Dynamics, help-seeking behaviors, and correlates. *Journal of Gay & Lesbian Social Services*, *14*(1), 23–49. doi:10.1300/J041v14n01_02

Melling, B., & Houguet-Pincham, T. (2011). Online peer support for individuals with depression: A summary of current research and future considerations. *Psychiatric Rehabilitation Journal*, *34*(3), 252–254. doi:10.2975/34.3.2011.252.254

Meng, J. (2016). Your health buddies matter: Preferential selection and social influence on weight management in an online health social network. *Health Communication*, *31*(12), 1460–1471. doi:10.1080/10410236.2015.1079760

Miller, E., McCaw, B., Humphreys, B. L., & Mitchell, C. (2015). Integrating intimate partner violence assessment and intervention into healthcare in the United States: A systems approach. *Journal of Women's Health*, *24*(1), 92–99. doi:10.1089/jwh.2014.4870

Moncur, W., Gibson, L., & Herron, D. (2016). The role of digital technologies during relationship breakdowns. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 371–382. doi: 10.1145/2818048.2819925

Mondal, M., Messias, J., Ghosh, S., Gummadi, K. P., & Kate, A. (2017). Managing longitudinal exposure of socially shared data on the Twitter social media. *International Journal of Advances in Engineering Sciences and Applied Mathematics*, *9*(4), 238–257. doi:10.1007/s12572-017-0196-3

Naslund, J. A., Aschbrenner, K. A., Marsch, L. A., & Bartels, S. J. (2016). The future of mental health care: Peer-to-peer support and social media. *Epidemiology and Psychiatric Sciences*, *25*(2), 113–122. doi:10.1017/S2045796015001067

Navarro, J. N., Clevenger, S., & Marcum, C. D. (2016). *The intersection between intimate partner abuse, technology, and cybercrime: Examining the virtual enemy*. Durham, NC, USA: Carolina Academic Press.

Newell, A. F., Gregor, P., Morgan, M., Pullin, G., & Macaulay, C. (2011). User-sensitive inclusive design. *Universal Access in the Information Society; Heidelberg*, *10*(3), 235–243. doi:10.1007/s10209-010-0203-y

Niela-Vilén, H., Axelin, A., Salanterä, S., & Melender, H.-L. (2014). Internet-based peer support for parents: A systematic integrative review. *International Journal of Nursing Studies*, *51*(11), 1524–1537. doi:10.1016/j.ijnurstu.2014.06.009

Office for National Statistics. (2017, November 23). Domestic abuse in England and Wales: Year ending March 2017 [Statistical bulletin]. Retrieved from Office for National Statistics website: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2017

PERF. (2015). Police improve response to domestic violence, but abuse often remains the 'Hidden Crime'. *Police Executive Research Forum Newsletter*, *29*, 1. Retrieved from https://www.policeforum.org/assets/docs/Subject_to_Debate/Debate2015/debate_2015_janfeb.pdf

Prayudi, Y., & Sn, A. (2015). Digital chain of custody: State of the art. *International Journal of Computer Applications*, *114*(5), 1–9. doi:10.5120/19971-1856

Pullin, G., & Newell, A. (2007). Focussing on Extra-Ordinary Users. *Universal Acess in Human Computer Interaction. Coping with Diversity*, 253–262. doi:10.1007/978-3-540-73279-2_29

Rains, S. A., Peterson, E. B., & Wright, K. B. (2015). Communicating social support in computer-mediated contexts: A meta-analytic review of content analyses examining support messages shared online among individuals coping with illness. *Communication Monographs*, *82*(4), 403–430. doi:10.1080/03637751.2015.1019530

Richards, L. (2016). *Domestic abuse, stalking and harassment and honour based violence (DASH, 2009–16) risk identification and assessment and management model*. Retrieved from National Police Chiefs' Council & Safe Lives website: https://www.dashriskchecklist.co.uk/wp-content/uploads/2016/09/DASH-2009-2016-with-quick-reference-guidance.pdf

Rizo, C. F., Macy, R. J., Ermentrout, D. M., O'Brien, J., Pollock, M. D., & Dababnah, S. (2017). Research with children exposed to partner violence: perspectives of service-mandated, CPS- and court-involved survivors on research with their children. *Journal of Interpersonal Violence*, *32*(19), 2998–3026. doi:10.1177/0886260515596534

Robinson, L., & Spilsbury, K. (2008). Systematic review of the perceptions and experiences of accessing health services by adult victims of domestic violence. *Health & Social Care in the Community*, *16*(1), 16–30. doi:10.1111/j.1365-2524.2007.00721.x

Rodgers, M. A., Grisso, J. A., Crits-Christoph, P., & Rhodes, K. V. (2017). No quick fixes: A mixed methods feasibility study of an urban community health worker outreach program for intimate partner violence. *Violence Against Women*, *23*(3), 287–308. doi:10.1177/1077801216640383

Ruff, L. (2012). Does training matter? Exploring police officer response to domestic dispute calls before and after training on intimate partner violence. *The Police Journal*, *85*(4), 285–300. doi:10.1350/pojo.2012.85.4.516

SafeLives. (2016). *A cry for health: Why we must invest in domestic abuse services in hospitals*. Retrieved from SafeLives website: http://www.safelives.org.uk/sites/default/files/resources/SAFJ4993_Themis_report_WEBcorrect.pdf

Saldana, J. (2015). *The coding manual for qualitative researchers* (1st ed.). London, UK: SAGE.

Sillence, E. (2013). Giving and receiving peer advice in an online breast cancer support group. *Cyberpsychology, Behavior, and Social Networking*, *16*(6), 480–485. doi:10.1089/cyber.2013.1512

Snook, Chayn, & SafeLives. (2017). *Tech vs abuse: research findings*. Retrieved from Comic Relief website: https://www.techvsabuse.info/research-findings

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

SpoofCard. (2018). Spoof calls & change your caller ID. Retrieved from Easily Disguise Your Caller ID website: https://www.spoofcard.com/secondary-callerid

Such, J. M., & Criado, N. (2016). Resolving multi-party privacy conflicts in social media. *IEEE Transactions on Knowledge and Data Engineering*, *28*(7), 1851–1863. doi:10.1109/TKDE.2016.2539165

Sugiura, L. (2016). *Researching online forums—Digital research ethics case study 1*. Retrieved from British Sociological Association website: https://www.britsoc.co.uk/ethics

Taket, A., Nurse, J., Smith, K., Watson, J., Shakespeare, J., Lavis, V., … Feder, G. (2003). Routinely asking women about domestic violence in health settings. *British Medical Journal*, *327*(7416), 673–676. doi:10.1136/bmj.327.7416.673

Thomas, K., Grier, C., & Nicol, D. M. (2010). Unfriendly: Multi-party privacy risks in social networks. *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, 236–252. doi:10.1007/978-3-642-14527-8_14

Warren-Gash, C., Bartley, A., Bayly, J., Dutey-Magni, P., Edwards, S., Madge, S., … Rodger, A. (2016). Outcomes of domestic violence screening at an acute London trust: Are there missed opportunities for intervention? *British Medical Journal*, *6*(1), e009069. doi:10.1136/bmjopen-2015-009069

Westera, N. J., & Powell, M. B. (2017). Prosecutors' perceptions of how to improve the quality of evidence in domestic violence cases. *Policing and Society*, *27*(2), 157–172. doi:10.1080/10439463.2015.1039002

Winzelberg, A. (1997). The analysis of an electronic support group for individuals with eating disorders. *Computers in Human Behavior*, *13*(3), 393–407. doi:10.1016/S0747-5632(97)00016-2

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, *98*, 95–108. doi:10.1016/j.ijhcs.2016.09.006

Woodlock, D. (2016). The abuse of technology in domestic violence and stalking. *Violence Against Women*, *23*(5), 584–602. doi:10.1177/1077801216646277

World Health Organisation. (2017). *Violence against women: Intimate partner and sexual violence against women*. Retrieved from World Health Organisation website: http://www.who.int/mediacentre/factsheets/fs239/en/

Yu, L., Motipalli, S. M., Lee, D., Liu, P., Xu, H., Liu, Q., … Luo, B. (2018). My friend leaks my privacy: Modeling and analyzing privacy in social networks. *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, 93–104. doi:10.1145/3205977.3205981

Zaidi, A. U., Fernando, S., & Ammar, N. (2015). An exploratory study of the impact of information communication technology (ICT) or computer mediated communication (CMC) on the level of violence and access to service among intimate partner violence (IPV) survivors in Canada. *Technology in Society*, *41*, 91–97. doi:10.1016/j.techsoc.2014.12.003

Zimmer, M., & Kinder-Kurlanda, K. (2017). *Internet research ethics for the social age: New challenges, cases, and contexts*. Peter Lang: International Academic Publishers, New York, NY, US.