Original Research

Journal of Interpersonal Violence
1–30

DOI: 10.1177/08862605251391169
journals.sagepub.com/home/jiv


Technology-Facilitated Intimate Partner Violence: An Examination of Prevalence, Perpetration Type and Methods and the Impact of COVID-19

Jennifer E. Storey[1] **and Afroditi Pina**[1]

Abstract

It is widely acknowledged that with the increased use of technology in society much of the abuse and coercive control perpetrated by intimate partners is now also digital in nature and involves technology as a core conduit. This study examined the presence of Technology-facilitated intimate partner violence (TFIPV) in 4,501 cases of online harm reported to The Cyber Helpline, a charity supporting victims of cyber harm, between March, 2019 and March, 2021. Aims were to identify the prevalence and type of TFIPV perpetrated and the methods of abuse used by perpetrators to commit TFIPV. The study further aimed to determine whether these variables differed based on relationship type and COVID-19 pandemic restrictions. TFIPV was present in 12.3% ($n = 554$) of cases reported and increased by 427.3% during the pandemic. Fourteen types of TFIPV were identified with the most common being cyberstalking and extortion. Varied methods of TFIPV perpetration were identified, with less sophisticated methods such as social media and video call recording being the most common. Types and methods of TFIPV

[1]University of Kent, Canterbury, UK

Corresponding Author:
Jennifer E. Storey, School of Psychology, Keynes College, University of Kent, Canterbury CT2 7NP, UK.
Email: j.storey@kent.ac.uk

varied by relationship type and time period. Extortion was most common in brief relationships and during the pandemic, suggesting opportunity and profit motivations. Conversely, unwanted contact, unauthorised access and device interception were more common in long-term relationships, with the latter also being more common pre-pandemic, likely due to greater victim access and knowledge. Findings have implications for victim protection, including the targeting of education to professionals and victims based on relationship type, common types and methods of TFIPV and dispelling misconceptions around TFIPV.

Keywords
internet and abuse, intimate partner violence/abuse, prevalence, cyberstalking, technology- or image-based, domestic violence

Introduction

The use of technology has become an integral part of our personal and working lives. Global lockdown measures implemented to manage the COVID-19 pandemic resulted in an increase of internet users by 10.2% in 2020, which was the largest increase in a decade (International Telecommunications Union, 2021). Furthermore, there was a notable increase, by 20%, in worldwide social media usage compared to before the pandemic (Dixon, 2022). Despite the multiple benefits of connection and ease, this shift to online communication has also given rise to aggressive and criminal behaviours now being conducted via technological and online means (Pina et al., 2021). Intimate Partner Violence (IPV) saw an upsurge during lockdown (Pina et al., 2021) and the recent Domestic Abuse Act (2021) in the UK acknowledged that not all IPV involves physical or sexual abuse, but can also involve coercive control, emotional, psychological and financial abuse, and much of that abuse can be facilitated by technology, and can be digital in nature (Brookfield et al., 2024).

Although there is no legal or widely agreed-upon definition in the UK, Technology-facilitated intimate partner violence (TFIPV; Pina et al., 2021) is recognised as

> any abuse (financial, sexual, physical, psychological) and coercive control between current or ex-intimate partners that is facilitated or perpetrated using technological means, and causes its recipients to experience fear or intimidation, image-based offenses, privacy violation, unwanted sexual attention or physical offenses (Pina et al., 2021, p. 12; Tanczer et al., 2018; Woodlock, 2017).

To best understand and combat TFIPV, we must identify its prevalence, nature, and the methods by which it is perpetrated.

Prevalence

Prevalence rates of TFIPV vary greatly across studies due to different definitions, measurements, scales, time periods and samples. Of those studies available, few include representative datasets and there is a dearth of research from the UK. To date, studies have focused on adolescents and young adults with limited research on adult populations (Kim & Ferraresso, 2022; Pina et al., 2021). There is also emerging research from services engaged with victims of TFIPV (Douglas et al., 2019; Refuge, 2022) but a great deal remains to be examined from service providers and first responders. Despite the above caveats, making cross-comparison in prevalence rates for TFIPV difficult, current victimisation rates vary from 1.8% to 84% depending on what is being measured [e.g., umbrella terms such as TFIPV that include multiple types of victimisation (Powell & Flynn, 2023) vs. specific behaviours such as cyberstalking or stalkerware and monitoring application use (Tanczer et al., 2018)], and how (e.g., via quantitative representative surveys or qualitative service user feedback; Fernet et al., 2019; Kim & Ferraresso, 2022). Fewer studies have focused on TFIPV perpetration, but of those that have directly measured perpetration, rates vary from 0.6% to 82% (Kim & Ferraresso, 2022; Pina et al., 2021).

Prevalence rates by gender show a mixed picture; some studies report higher prevalence of victimisation among women of sexual coercion, threats and intimate image sharing kinds of TFIPV (Powell & Flynn, 2023), whereas no significant differences were noted in monitoring and controlling TFIPV behaviours (in some items, men overall reported higher victimisation despite a lack of statistical significance). In addition, some other studies reported higher rates of victimisation for men (Hinduja & Patchin, 2020), but overall, lifetime TFIPV victimisation rates between males and females do not appear to differ significantly in the literature (Brown et al., 2021; Powell & Flynn, 2023). In terms of perpetration rates by gender, there appear to be differences between males and females in minor cyber unwanted pursuit behaviours, with 48% of females perpetrating such TFIPV behaviours (e.g., monitoring and tracking partners) versus 34% of men, with no gender difference in severe cyber unwanted pursuit behaviours (Dardis & Gidycz, 2019). There are also a few studies that measure TFIPV perpetration and victimisation concurrently in their samples (Powell & Flynn et al., 2023; Reed et al., 2016), which report that there is a bi-directional and dyadic nature in TFIPV, with most perpetrators of TFIPV also being victims of it.

Types of TFIPV

The nature of TFIPV is diverse and spans a range of direct and indirect, public and private types, some focused on controlling victims, and some on damaging victims' reputations, while others can present simultaneously (e.g., spying as well as doxing; Freed et al., 2018). Several classifications and types of TFIPV perpetration have been put forward in recent years following extensive debates on whether it is an extension of offline IPV and whether it should be classified in similar typologies to offline IPV (e.g., sexual, emotional, and physical). Classifications overall have been based on perpetrator motivation and the nature of harmful behaviour (Fernet et al., 2019).

Pina et al. (2021) in their Home Office report on perpetrators of TFIPV conducted a rapid evidence assessment summarising the TFIPV type literature into two modes and four main types. The two modes identified were *direct* (e.g., using technology to harass, control, and intimidate a victim directly) and *indirect* (using technology or social networking platforms to damage a victim's reputation in a public or social setting) (Fernet et al., 2019). The four types identified were *Cyberstalking and Coercive Control, Harassment, Image Based Sexual Abuse (IBSA)*, and *Indirect Non-sexual Abuse*. Several of these types have overlapping characteristics since the terminology used in the literature is not uniform.

The first of the four types, intimate partner cyberstalking, is characterised by the use of technology to perpetrate control, intimidation and isolation by patterns of repeated and unwanted attention and harassment that cause fear or distress to the victim (Crown Prosecution Service, 2024). Harassment in TIFPV encompasses unwanted sexual and non-sexual behaviours perpetrated via technology in a private or public setting, targeting the victim directly (e.g., direct mode) (Freed et al., 2018). Some of these behaviours also feature as part of cyberstalking behaviours, cyberstalking, however, requires victim fear. IBSA is an umbrella term that refers to increasingly criminalised direct and indirect behaviours that focus on private/sexual material that is created, distributed, and threatened to be distributed to others without consent (Powell et al., 2022). The material can be obtained *directly* from the victim via pressure/blackmail, or consensually during the relationship, and *indirectly* via hacking and Internet of Things (IoT), or physically getting access to victims' devices without permission (Pina et al., 2021). Again, some of these behaviours can also feature in both harassment and cyberstalking, thus denoting the overlap in these categories and also the overlap in types and definitions used in the literature. Finally, indirect non-sexual abuse includes behaviours that involve harassment of the victim via a third party (such as harassment of the victims' partner, family friends and work colleagues), enlisting third parties

in harassment via posting false or defamatory information (e.g., resulting in vigilantism), posting fake services, and enlisting fake items for sale where the victims are contacted by multiple buyers (Lòpez-Cepero et al., 2018; Woodlock, 2017; Woodlock et al., 2020).

Methods of TIFPV

As technology evolves at great speed, researchers from various disciplines are trying to identify and assess the technologies used in TFIPV and the risks associated with them. Most scholars recognise two main forms of technologies (Chatterjee et al., 2018; Fernet et al., 2019; Parsons et al., 2019); (a) those marketed purposely for control, surveillance and harassment (e.g., spyware, stalkerware, hidden cameras, and audio bugs) that are purchased, downloaded and installed by perpetrators and (b) technologies not marketed as such, but repurposed by perpetrators to exercise monitoring, control and manipulation (e.g., baby monitors, smart devices, phone locators, and social media platforms; Pina et al., 2021).

Freed et al. (2019) further classified two methods that TFIPV perpetrators use to target their victims: (a) *ownership-based access* to accounts, whereby perpetrators exploit their ownership of victims' devices or accounts, and can prevent victims from accessing the internet as well as their devices/accounts, track victim location, and monitor victim usage and (b) *account/device compromise*, whereby perpetrators can guess passwords, steal information, impersonate victims and download and install spyware/stalkerware. Freed et al. (2018) stated that attackers with intimate knowledge of victims (as is the case with most TFIPV perpetrators) are the most difficult type of cybersecurity threat to manage because they use unsophisticated methods and standard interfaces and present as authenticated users.

Flach and Deslandes (2019) reported that there existed over 200 apps with stalkerware qualities, and 40 apps specifically marketed for spying, tracking and controlling intimate partners, with other researchers (Harkin et al., 2020; Parsons et al., 2019) stating that developers and companies, in their marketing and optimisation content, made direct references to spousal monitoring and non-consensual use of the technologies. Chatterjee et al. (2018) reported increased interest in spyware apps, with over 600 queries in 1 month.

Scholars and policy makers report that insidious and repurposed technologies pose new challenges in cybersecurity (Leitão, 2019; Lopez-Neira et al., 2019; Tanczer et al., 2021). The IoT is a term used to describe an array of devices that have the capability of communicating with each other (e.g., Amazon's Alexa, Google Home, wearable devices such as iWatch, Nest thermostats, fridges, cameras, smart security, and doorbells etc.) These are

normally share-owned devices in a home setting that have been linked with TFIPV, where perpetrators can access them either physically or remotely. Perpetrators can then control ambient surroundings and monitor or gaslight victims via functionalities such as remote locking and unlocking of doors, triggering alarms, and changing heating settings (Leitão, 2019; Parkin et al., 2019).

The Impact of the COVID-19 Pandemic

During the 2020 global pandemic, governments around the world instructed the public to isolate and minimise movement during a series of national lockdowns to restrict the spread of the SARS-CoV-2 virus. Many countries and domestic abuse organisations reported high rates of IPV due to victims being forced to shelter with abusers for prolonged periods of time (Campbell, 2020; Census, 2021). Several countries reported a 50% to 70% increase in IPV-related calls to police, emergency services, shelters, and helplines (Global News Canada, 2020; Refuge, 2020; Tolan, 2020; Women's Safety New South Wales, 2020), and Refuge also reported a 950% increase in website visits during those periods of lockdown compared to pre-pandemic rates. The pandemic has had a lasting impact on the ways in which we communicate and work, with increased delivery of services online, more flexible working patterns with less stigma around working from home, as well as more flexibility in working and communication methods (Chen et al., 2023).

In the 5 years since the pandemic (also known as the post-pandemic era), as our knowledge of and skills to respond to COVID-19 have improved, our social interactions have returned to some pre-pandemic normalcy with no enforcement of social distancing rules, but many researchers are noting a change in human communication and social interaction. Our reliance on technological means for communication and information gathering has not yet decreased to pre-pandemic levels (Chen et al., 2023). According to Brookfield et al. (2024), the increase in IoT usage and remotely operated technologies can be seen as perpetuated lockdown conditions for IPV victims. The UK Home Secretary, recognising the seriousness of abuse experienced by women and girls in 2023, identified TFIPV and tech abuse as a strategic policing priority, alongside terrorism and organised crime (National Police Chief's Council, 2023). Therefore, our knowledge of the intricacies and forms of TFIPV must be expanded and solidified to effectively prevent perpetration and support victims.

It is evident from the literature that there is significant overlap in definitions of TFIPV, terminology used to describe its types and methods, as well as conceptual overlap in the precise behaviours recognised in each category of abuse. The reviewed literature brings to the fore some question marks

around accurate rates of prevalence, universally agreed categories of TFIPV technology, perpetration behaviours, as well as generalisability of results due to sample categories (i.e., most of the research on TFIPV focuses on females, adolescents and college students). Further, few studies have been reflective of different types of intimate partner relationships (i.e., brief encounters vs. long-term relationships); however, it is known from studies on IPV that relationship status, state and duration matter in the characteristics and type of IPV experienced by its victims (Sutton & Dawson, 2021). Moreover, most studies have imposed a structure on responses from victims by presuming types and methods of TFIPV in psychometric measurements. This has potentially limited the spontaneous self-report from victims, limiting by extension what is reported by researchers and subsequently limiting the help that can be suggested and provided to victims.

To best protect victims of TFIPV, a greater understanding of this offence at a national level is required. This includes a detailed understanding of the offending behaviours that take place (e.g., threats, extortion), referred to herein as *types of TFIPV*, as well as the methods of attack or *TFIPV method* (e.g., spyware, email contact). Improved understanding of TFIPV will identify the critical shifts that are taking place in the perpetration of IPV, a globally prevalent problem. This information will have implications for policing this crime, including the necessary resources and knowledge that the criminal justice system must possess. Further, it will build an understanding of victim experience and the level of harm encountered, as well as what resources and knowledge are necessary for intervention, education, and outreach for victims, perpetrators, and the public.

The Present Study

This study addresses these limitations by examining a representative sample of cases involving victims of any age who sought help for TFIPV from a national UK charity offering technological assistance and signposting to victims of cybercrime and online harm. Intimate relationship type was recorded across all cases and used to examine potential differences across TFIPV type and the methods employed by perpetrators to engage in TFIPV. The sample examined was applied in nature, consisting of cases reported to the charity, meaning that no structure was imposed on the reporting of TFIPV type or method of perpetration by the authors, or by previous literature. The information gathered consisted of what victims and concerned persons who reported online harm to the charity thought was most relevant and helpful in responding to their case.

The following research questions were investigated to identify and assess risks faced by TFIPV victims: (1) What is the prevalence of TFIPV among cases of online harm reported to a national UK cyber helpline? (2) What types of abusive behaviour are TFIPV perpetrators engaging in toward victims? (2a) Did the types of abusive behaviours differ by relationship type? (3) What methods are used by perpetrators to engage in TFIPV? (3a) Did the method of perpetrating abusive behaviours differ by relationship type? (4) Did TFIPV prevalence, type of abusive behaviour, or method differ prior to the COVID-19 pandemic compared to during the pandemic restrictions?

Method

Overview

Information on TFIPV prevalence and type, as well as the methods used to perpetrate TFIPV, was gathered from 554 cases of TFIPV reported to The Cyber Helpline (a national UK helpline for victims of online harm) between March 20, 2019 and March 23, 2021. Information was coded from client records, and access to records was provided by The Cyber Helpline following training and vetting of research assistants (RAs) and ethical approval. The coding sheet used to gather information was developed from the authors' knowledge of the online harm literature (Pina et al., 2021), the expertise of The Cyber Helpline and a review of the helpline database and sample cases. All cases identified as TFIPV were coded by multiple individuals to produce consensus ratings. Given that the charity is national, and the sample includes all cases from the years examined (i.e., is continuous), the data is representative of TFIPV victims and concerned persons in the UK who have reached out for formal support to The Cyber Helpline.

Cases

The Cyber Helpline assists victims of cyber harm to understand, contain, recover and learn from cyber-attacks. The staff of cybersecurity professionals at the helpline respond to requests for assistance from victims and concerned persons. Initial contact with the charity is typically via a Chatbot. The Chatbot attempts to classify cases and provide help and cyber-attack guides. Assistance is also provided via referrals and email. If cases are not resolved using the Chatbot, they are passed to a helpline responder, who communicates with the client to resolve their case. All communication is linked to form a client record.

A total of 4,501 unique client records were created between March 20, 2019 and March 23, 2021 and were examined for inclusion in the study. Cases of TFIPV identified within this sample were then coded in greater detail. Cases were determined to be TFIPV if they met two criteria. First, an intimate relationship was present between the perpetrator and the victim. To be classified as intimate, there had to be a relationship in which the victim had engaged with the perpetrator with romantic intent. This included anything from a brief romantic or sexual encounter (online or offline), to dating, to a long-term partnership, such as marriage. Cases were, therefore, excluded from detailed coding if other types of relationships (e.g., familial, neighbours) were present or if the perpetrator was romantically pursuing the victim but the victim had never returned that interest or engaged with the perpetrator. The second criterion was the presence of online abuse, which was identified and categorised by the CEO of the helpline and is detailed further below. A total of 554 (12.3%) cases met the inclusion criteria for TFIPV. For clarity, hereafter, targets of TFIPV will be referred to as *victims* of TFIPV, the individual(s) engaging in the TFIPV will be referred to as *perpetrators* of TFIPV, the overarching incident reported will be referred to as the *case*, and the cyber-attacks identified by the charity will be referred to as *abusive behaviours*.

Client records contained some demographic information collected by the helpline, such as whether the victim is 18 or older and if they live in the UK. Cases of stalking also included a "cyberstalking form" with more detailed questions about the stalking behaviour perpetrated. The type of abusive behaviour perpetrated was recorded by the helpline. The remaining information required to answer the research questions was coded from the free-text fields, emails and online forms contained in the client records using a coding sheet.

Materials

The information available for the present study was that collected in the context of a report on TFIPV to The Cyber Helpline. No additional scales or questions were added by the researchers. Examining the information available to helpline responders is critical to understanding the type of information that is reported and what details about the harm can be identified and assessed from the client records.

Client records were coded by three PhD-level RAs using a coding sheet to extract demographic information, information on the type of abusive behaviour and information on the method(s) used to perpetrate the abusive behaviour. Demographic information was coded where possible from

identified fields in the client records (e.g., age above or below 18) and otherwise from free text (e.g., gender of the perpetrator and victim). The type of abusive behaviour was coded as it appeared in client records. In each case, the CEO of the helpline identified the type of abusive behaviour being perpetrated in the case, drawing on a list of 40 types developed by the charity. In some cases, multiple types of abusive behaviour were listed in the client records; therefore, clarification was sought from the helpline manager, who had knowledge of the categorisation, to identify the overarching type of abusive behaviour for these cases. The method by which TFIPV was perpetrated was coded based on the free text in client records, and all methods of engaging in abusive behaviour that were mentioned were recorded on the coding sheet.

The coding sheet was developed based on knowledge of the research literature on online harm and IPV and experience reviewing case files for research. The coding sheet was designed so that no identifiable information was coded from helpline records. After development, a sample of helpline cases was reviewed to refine wording and categories on the coding sheet. In particular, sample cases were used to identify methods of engaging in abusive behaviour. The coding sheet was then reviewed by researchers from the fields of Psychology, Information Security and Criminology, who were part of the larger funded project on TFIPV that included this study, and The Cyber Helpline and modifications were made.

The coding sheet was trialled by the first author and the RAs on five cases to assess clarity and consistency. Modifications were then made to clarify definitions. This process was repeated twice, with RAs coding 15 cases each time and then meeting with the first author to review ratings. This process improved agreement between the RAs and expanded the definitions and methods of abusive behaviour categories used in the coding sheet. Finally, 100 cases were coded with the aim of expanding the methods of abusive behaviour and finalising the coding sheet. Cases were reviewed with the research team and The Cyber Helpline to define and classify the methods of abusive behaviour identified. This procedure greatly increased the number of methods identified and allowed coding of the remaining cases to proceed without having to significantly alter the coding sheet again.

Several coding decisions were made to increase data quality and reliability. First, RAs recorded the abusive behaviour type decisions of the CEO and sought clarification from the manager where multiple types were identified; RAs did not impose their judgement. This decision was made to reflect the substantial subject matter expertise of the helpline CEO and manager. Second,

information reported by victims was taken as accurate. For instance, if the victim reported that they had been catfished by a male, the perpetrator was coded as male, while acknowledging that victims can be mistaken due to the online nature of the relationships. Client records are based on victim reporting and thus necessitate the coding of information as reported by the victim, as is the case in other types of file review studies.

Procedure

Permission to conduct the study was obtained from the authors' university ethics committee. RAs passed a Disclosure and Barring Service (i.e., UK criminal record check) check prior to accessing client records. A data sharing agreement was in place between the research team and The Cyber Helpline to ensure data security.

RAs underwent extensive training on the data from The Cyber Helpline and the coding procedures from the lead author. RAs completed The Cyber Helpline online training course, which includes approximately 6.5 hrs of education outlining the different cyber issues the Helpline responds to. Live online training from helpline staff was also provided on the charity's case management system. As above, the RAs were trained in the use of the coding sheet and practiced and refined those skills through the coding and review of cases with the first author. Although this training improved agreement, the helpline cases proved to be very diverse in nature, and the novelty of the methods of abusive behaviour perpetrated meant that cases raised many questions. This slowed and broke-up the coding process. To improve reliability, each case was coded by two RAs, blind to each other's ratings and the resulting consensus ratings were used. To reach consensus ratings where disagreement occurred, RAs would discuss and review the case, where disagreement persisted, it was resolved in discussion with the first author. Where required The Cyber Helpline manager and/or CEO also provided assistance, particularly in relation to clarification of online methods of abuse and for cases that required the addition, or clarification of, an abusive behaviour type. Thus, all cases included in this study are the product of consensus between extensively trained PhD-level raters and in some cases the input of more experienced individuals.

Cases from March 20, 2019 to March 23, 2021 were coded. The dates were selected to reflect 1 year prior to and 1 year post the first UK lockdown for the COVID-19 pandemic. Cases spanning March 20, 2019 to March 21, 2020 will be referred to as *pre-pandemic* and cases spanning March 22, 2020 to March 23, 2021 will be referred to as *during the pandemic*.

Data Analyses

Analyses were conducted using SPSS v. 29, IBM. Descriptive statistics, including frequency analysis, were used to report demographic characteristics, type of abusive behaviour and method of abusive behaviour perpetration. Chi-Square (where cell counts were >5) and *T*-tests were used to examine whether differences existed by relationship type and pre-pandemic compared to during the pandemic. Missing data is reported for sample characteristics. There were no missing abusive behaviour types or methods; thus, no adjustments were required for inferential analyses.

Sample Characteristics

In some instances, sample characteristics included a substantial amount of missing information, and some diversity markers could not be collected (e.g., ethnicity, socioeconomic status). This is to be expected given the applied nature of the sample, where data was gathered by the helpline to assist victims rather than for research. Nevertheless, where high rates of missing data exist, sample characteristics should be considered with caution. Further consideration of the findings with a diversity lens is an important area of future investigation.

Victims of TFIPV were more often female (38.8%, $n=215$) than male (12.3%, $n=68$) or transgender (0.2%, $n=1$) (missing information 48.7.%, $n=270$). Perpetrators were more often male (58.7%, $n=325$) than female (25.6%, $n=142$) or transgender (0.2%, $n=1$) (missing information 15.5%, $n=86$). Most victims were adults, over 17 (42.8%, $n=237$) (missing information 53.1%, $n=294$). Cases were most often reported by the victim (82.3%, $n=456$), not a concerned person.

In terms of relationship type, brief relationships, which constituted anything from a one-night intimate encounter to short-term dating, made up 41.2% ($n=228$) of the sample. Ex-partners, defined as those previously in longer-term relationships, were only slightly less frequent in the sample (39.5%, $n=219$). Less common relationship types included current relationships (7.9%, $n=44$), divorced (6.1%, $n=34$), separated (3.2%, $n=18$) and married (2%, $n=11$). Relationships between perpetrators and victims were most often online only (45.1%, $n=250$); however, some included face-to-face contact (28.5%, $n=158$) (missing information 26.4%, $n=146$). Cohabitation was rare (0.7%, $n=4$) (missing information 24.5%, $n=136$). In line with this, most TFIPV was perpetrated entirely online (60.8%, $n=337$), with 17.5% ($n=97$) of abusive behaviour also including an offline component (missing information 21.7%, $n=120$).

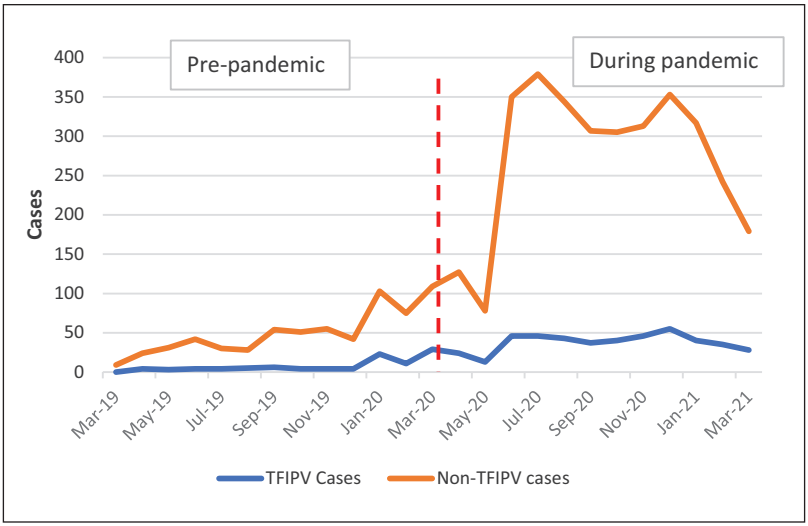

Figure 1. Frequency of helpline contact over time by presence of TFIPV ($N = 4{,}501$).

Results

Prevalence of TFIPV

Of the 4,501 unique cases reported to The Cyber Helpline during the 24-month period examined, 12.3% ($n = 554$) met the criteria for TFIPV, namely that there was (a) an intimate relationship between the victim and perpetrator and (b) an act of online abuse. Case frequency over time is presented by case type (TFIPV or non-TFIPV) in Figure 1. Non-TFIPV cases (i.e., cases of online harm that were not between intimate partners) were consistently more prevalent over time. An overall increase can be seen in cases over time, as would be expected with increased public awareness of the helpline. Several spikes in case numbers are also notable and can be accounted for by different events. First, the spike in January 2020 coincided with a television feature on The Cyber Helpline. Second, in July, 2020 a technical glitch meant that large numbers of cases were uploaded to the system as if they took place on a single day in July. Third, in January, 2021, the helpline provided training to several agencies that act as referral sources for the charity, which would have then increased their awareness of the charity and subsequently reporting. Fourth, staff at the helpline noticed a seasonal increase in cases around January each year, following the December holidays. Increased tension and/

or abuse during the holidays may lead to a decision by victims to change course in the new year and report problems to authorities, and is often seen in IPV reporting (Police Service of Northern Ireland, 2023).

Prevalence of Abuse Prior to and During the Pandemic. Even after considering these spikes in case numbers, a clear increase in cases can be seen following the start of the pandemic and lockdown in March 2020. To investigate the impacts of the lockdown, reports made from March 22, 2019 to March 21, 2020, pre-pandemic, are compared to reports from March 22, 2020 to March 23, 2021, during the pandemic. Pre-pandemic, a total of 663 cases, 13.3% ($n=88$) of which were TFIPV, were reported to the charity, compared to during the pandemic, where 3,838 cases, 12% ($n=464$) of which were TFIPV, were reported. This equates to a 478.9% increase in cases reported to the charity, and a 427.3% increase in TFIPV cases reported. This suggests that the period of pandemic restrictions resulted in significantly more perpetration of online harm generally and TFIPV. The proportion of cases reported that were TFIPV remained the same, with about 12.3% of cases constituting TFIPV over the two-year period.

Types of Abusive Behaviour

One type of abusive behaviour that constituted TFIPV was identified for each case by The Cyber Helpline. Fourteen types of TFIPV abusive behaviour were perpetrated across the 554 cases. The 14 types, along with their description and prevalence, are presented in Table 1. To facilitate analysis, the types of abusive behaviours were grouped into five categories reflecting a common underlying perpetrator behaviour. Categories are presented in descending order of frequency; some categories only include one type of abusive behaviour.

Abusive Behaviour by Relationship Type. The categories of abusive behaviour were examined to determine if variation existed by victim-perpetrator relationship type. Brief relationships, lasting a few months or less (41.2%, $n=228$), were compared to longer-term partnerships (50.9%, $n=282$). Current relationships (7.9%, $n=44$) were excluded from this analysis as relationship length was not recorded. *Extortion* was more common in brief relationships (78.5%, $n=179$) compared to long-term partnerships (10.6%, $n=30$), χ^2 (1, $N=510$) $=240.11$, $p<.001$, Phi $=.686$. Conversely, *Unwanted contact and communication* were more common in long-term partnerships (69.1%, $n=195$) than in brief relationships (21.1%, $n=48$), χ^2 (1, $N=510$) $=116.91$, $p<.001$, Phi $=.479$. The remaining three categories had cell counts under five and thus could not be examined statistically.

Unauthorised access occurred in 14.9% ($n=42$) of long-term and 0.4% ($n=1$) of brief relationships. *Device interception* occurred only in long-term partnerships (5%, $n=14$) as did *Theft* (0.7%, $n=2$). Effect sizes for both significant differences were large.[1]

Abusive Behaviour Prior to and During the Pandemic. The substantial rise in cases reported to the helpline during the pandemic unsurprisingly corresponded to increased frequency of abusive behaviour types during the pandemic (see Table 1). In fact, all but one type of abusive behaviour was more frequently reported during the pandemic (fraud and identity theft were the only exceptions, where the one reported case was pre-pandemic). To investigate whether certain types of abusive behaviour were proportionally more common during the pandemic, inferential statistics were used.

Of the four categories of abuse type with sufficient data to analyse, two showed significant differences across the time periods. *Extortion* was more common during the pandemic (41.4%, $n=193$) than pre-pandemic (28.1%, $n=24$), χ^2 (1, $N=554$)=6.22, $p=.013$, Phi=.106. *Device interception* was more common pre-pandemic (5.7%, $n=5$) than during the pandemic (1.9%, $n=9$), χ^2 (1, $N=554$)=4.23, $p=.041$, Phi=.09.

With respect to individual types of abusive behaviour with sufficient numbers to examine, three behaviours differed significantly in frequency across the time periods. *Cyberstalking* was more common pre-pandemic (38.6%, $n=34$), than during the pandemic (23.6%, $n=110$), $\chi 2$(1, $N=554$)=8.69, $p=.003$, Phi=.125. Conversely, the use of web cameras for *blackmail and sextortion* was more common during the pandemic (25.5%, $n=119$) than pre-pandemic (15.9%, $n=14$), χ^2 (1, $N=554$)=3.76, $p=.052$, Phi=.082. Effect sizes for significant differences across time periods were small.

Methods Used to Perpetrate TFIPV

A total of 21 methods were used by perpetrators to commit TFIPV. The methods identified were used a total of 1,193 times across the 554 cases, with an average of 2 methods per case ($M=2.15$; $SD=1.37$, range: 1-10), 344 (63.2%) cases involved 2 or more methods. The methods and their frequency of use in the 554 cases are displayed in Table 2. To facilitate analysis, methods of TFIPV were organised into four groups based on: (a) the underlying action being taken by the perpetrator (e.g., communicating with the victim vs. spreading information about the victim), and (b) the actions that would be required by the helpline to assist the victim. Given the first criterion, some of the groups are similar to abusive behaviour types. Nevertheless, there is no exact match between TFIPV methods and abusive behaviours for two

Table 1. TFIPV Abusive Behaviour Description and Frequency.

		%(*n*)		
Type of abusive behaviour	Abusive behaviour description		Pre-pandemic	During pandemic
Category 1: Unwanted contact and communication	**Perpetrator correspondence with the victim.**	**50 (277)**	**54.5 (48)**	**49.1 (229)**
Cyberstalking	Persistent and repetitive patterns of online behaviour causing the victim fear of violence or alarm and distress.	26 (144)	38.6 (34)	23.7 (110)
Catfishing	Fake online profiles are used to trick the victim into a romance. The victim may then share private information or send money.	10.6 (59)	6.8 (6)	11.4 (53)
Harassment	Unwanted online behaviour that causes the victim alarm or distress. May cause the victim to feel offended, intimidated or humiliated.	8.5 (47)	5.7 (5)	9 (42)
Non-consensual sharing of intimate images (aka Revenge porn)	Sexual images of the victim are shared online without consent.	4.3 (24)	6.8 (6)	3.7 (18)
Creating fake profiles	Posting fake social media profiles is used to harass or impersonate the victim.	2.3 (13)	2.3 (2)	2.4 (11)
Online grooming	The internet is used to trick, force or pressure someone into doing something sexual (e.g., sending an explicit video or image).	1.8 (10)	0	2.1 (10)
Outing	Private information is shared publicly without the victim's consent.	0.7 (4)	1.14 (1)	0.6 (3)
Online reporting	Misinformation about the victim is spread. Intent is to harass or damage the victim's reputation.	0.2 (1)	0	0.2 (1)
Category 2: Extortion	**Perpetrators demand money or favours from victims for whom they possess compromising information.**	**39.2 (217)**	**28.1 (24)**	**41.4 (193)**
Webcam blackmail sextortion (Image based sexual abuse)	The victim is tricked into performing a sexual act on camera. This act is recorded, and the victim is blackmailed to not share the recording online.	24 (133)	15.9 (14)	25.5 (119)
Content for ransom	Sensitive information about the victim (e.g., images, secrets) is obtained, and a ransom is demanded for to not share the information online.	10.8 (60)	4.5 (4)	11.6 (54)
Category 3: Unauthorised access to technology	**Perpetrators gain or try to gain access to victims' information, accounts (e.g., social media and email) or devices (e.g., gaming, phone) without permission.**	**7.9 (44)**	**11.4 (10)**	**7.3 (34)**
Category 4: Device interception	**Perpetrators cause problems with victims' devices (e.g., with malicious software).**	**2.5 (14)**	**5.7 (5)**	**1.9 (9)**
Category 5: Theft	**Perpetrators take or withhold something that belongs to victims.**	**0.4 (2)**	**1.14 (1)**	**0.2 (1)**
Fraud identity theft	The victim's personal data is used fraudulently to obtain goods or services, often financially motivated.	0.2 (1)	1.14 (1)	0
Website theft	The victim's website is taken or withheld by the perpetrator.	0.2 (1)	0	0.2 (1)

Note. $N = 554$.

Table 2. TFIPV Method Frequency and Description.

Method used to perpetrate TFIPV	Description	% (*n*)
Group 1: Communication methods	**Methods where the perpetrator engaged in unwanted communication with the victim and the helpline tended to advise that victims collect this evidence but not respond.**	**72.9 (404)**
Social media	Communication via social media.	30.7 (170)
Fake profile	Creation of a fake profile to communicate with the victim.	24.9 (138)
Phone	Calling the victim.	21.8 (121)
Unwanted communication	Communication but method was unspecified by the victim.	21.3 (118)
Email	Communication via email.	6.3 (35)
Spoofing	Making it appear as though contact is coming from another person/account.	1.3 (7)
Phone number generator	Using a service that generates phone numbers to mask identity during attempts at communication.	0.7 (4)
Group 2: Information dissemination methods	**Methods where the perpetrator posted or commented about the victim and the helpline advised on how to remove the content.**	**32.5 (180)**
Video call recording	Recording the content of a video call between themselves and the victim. Often used for blackmail or ransom purposes.	21.1 (117)
Non-Consensual Sharing of Intimate Images method	Sharing or uploading sexually explicit/revealing images or videos of the victim without consent.	6.9 (38)
Fake profile victim impersonation	Creating a profile (e.g., on social media) pretending to be the victim.	3.1 (17)
Doxing	Releasing personal information about the victim publicly.	2.5 (14)
Website	Creating defamatory or fake websites, using or withholding the victim's website.	1.6 (9)
Fake account	Signing the victim up for subscriptions or other online accounts.	1.1 (6)
Dark web	Using the dark web to perpetrate abuse.	0.4 (2)
Group 3: Technical surveillance methods	**Methods that allowed the perpetrator to track the victim's location, monitor who the victim interacted with and harass the victim. Methods required specialised investigation or assistance from the helpline.**	**33.9 (188)**
Remote access	Unauthorised remote access of the victim's devices, accounts, social media etc.	28.2 (156)
Monitoring internet use	Monitoring the victim's internet usage, including browsing, searches and websites accessed etc.	10.6 (59)
Spyware	Software that is installed or used on an existing device to spy on the victim.	7.6 (42)
Malware	Malicious software installed onto the victim's device to steal information, access the device remotely or cause damage to the device.	7.2 (40)
Cameras, bugs, and trackers	External devices that are physically planted to watch, track or listen to the victim.	7 (39)
Leveraging existing home smart technology	Using existing devices or technology in the home to track, spy on, listen to or contact the victim (e.g., Amazon's Alexa).	6 (33)
Group 4: Methods involving card fraud	**The perpetrator had card details available to them and used the information without permission. Helpline advice was financially focused.**	**0.9 (5)**

N = 554.

reasons. First, a single method can be used to perpetrate multiple abusive behaviours. For instance, social media can be used to communicate with a victim and to impersonate a victim. Thus, all methods of engaging in TFIPV cannot be classed under one type of abusive behaviour. Second, abusive behaviour types were developed and coded by the Helpline, whereas methods of engaging in those behaviours were developed and coded by researchers, in consultation with the helpline. As such, we were not able to impose a coding structure that would bring both abuse types and methods in line with one another for research purposes.

There was substantial variation in the overall frequency of method use. The use of social media to communicate with the victim (30.7%, $n=170$) was the most common individual method, followed by *Remote access* (28.2%, $n=156$) and the use of a *Fake profile* (24.9%, $n=138$) to impersonate someone other than the victim.

Information was gathered regarding the type of social media used to engage in the methods of TFIPV. *Social media* was used as a method of communication in 30.7% ($n=170$) of cases. Social media was also used in seven additional cases to facilitate other TFIPV methods, such as creating a fake profile or facilitating extortion in Video Call Recording (e.g., a victim reported that "the person. . . recorded it [the naked video] and uploaded it on Instagram"). The specific social media platforms used in the 170 cases were almost always identified (96.5%, $n=164$), with multiple platforms used in 20% ($n=34$) of those cases. When individual platforms were identified and used ($n=164$), the most common was Facebook (40.2%, $n=66$) followed by Instagram (21.3%, $n=35$), Snapchat (9.8%, $n=16$), Facebook Messenger (6.1%, $n=10$), LinkedIn (1.2%, $n=2$) and TikTok (0.6%, $n=1$). When social media was used as a method of contact, the nature of the contact (e.g., via public post or direct message) was recorded. Most commonly, it was unclear whether the use of social media had been public or private (58.2%, $n=99$). Where discernible, social media use was most frequently via direct message (30.6%, $n=52$), followed by public posting (8.2%, $n=14$) and both public and private (2.9%, $n=5$).

Methods of TFIPV by Relationship Type. Independent-measures t-tests were conducted to determine if there were differences between the method groups and the length of the perpetrator-victim relationship. Current relationships were again excluded as the relationship length was unknown. There was a significant difference for method group one, $t(508)=2.87$, $p=.004$, Cohen's $d=.92$, with *Communication methods* occurring more frequently following a brief ($M=1.19$, $SD=0.69$) rather than a long-term relationship ($M=0.96$, $SD=1.10$). There was also a significant difference for method group two,

$t(508) = 7.84$, $p < .001$, Cohen's $d = .55$, with *Information dissemination methods* also occurring more frequently following a brief ($M = 0.61$, $SD = 0.58$) rather than a long-term relationship ($M = 0.22$, $SD = 0.53$). Differences had large and medium effect sizes, respectively. There was no significant difference between method group three, *Technical surveillance methods*, and relationship type.

Methods of TFIPV Prior to and During the Pandemic. All TFIPV methods increased in frequency during the pandemic, which is in line with the substantial increase in case volume. Statistical comparisons were thus made to determine whether there was a proportional change in method use based on the pandemic. At the method group level, three groups had sufficient sample sizes to examine, and two were found to be significantly different across time periods. The use of *Communication methods* (group one) increased significantly during the pandemic ($M = 1.12$, $SD = 0.90$) compared to pre-pandemic ($M = 0.78$, $SD = 0.96$), $t(552) = 3.23$, $p = .001$, Cohen's $d = .91$. Similarly, *Information dissemination methods* (group two) were more frequently used during the pandemic ($M = 0.40$, $SD = 0.59$) than pre-pandemic ($M = 0.19$, $SD = 0.43$), $t(552) = 3.11$, $p = .002$, Cohen's $d = .57$. Differences had large and medium effect sizes, respectively. There was no significant difference between method group three, *Technical surveillance methods*.

Ten of the 21 individual TFIPV methods showed significant variation in their presence or absence across time periods. Methods that had significant differences are presented in Figure 2 with the prevalence of their use across cases. Methods that were more frequently used pre-pandemic included: *Email contact* (χ^2 (1, $N = 554$) $= 6.76$, $p = .009$, Phi $= .11$), *Remote access* (χ^2 (1, $N = 552$) $= 19.57$, $p < .001$, Phi $= .188$), *Monitoring internet use* (χ^2 (1, $N = 554$) $= 19.20$, $p < .001$, Phi $= .186$), *Spyware* (χ^2 (1, $N = 554$) $= 5.48$, $p = .02$, Phi $= .099$), *Malware* (χ^2 (1, $N = 554$) $= 4.30$, $p = .037$, Phi $= .089$), and *Cameras, bugs and trackers* (χ^2 (1, $N = 554$) $= 12.58$, $p < .001$, Phi $= .15$). Methods that were significantly more common during the pandemic were, *Social media* (χ^2 (1, $N = 554$) $= 9.15$, $p = .002$, Phi $= .13$), *Phone* (χ^2 (1, $N = 554$) $= 4.13$, $p = .042$, Phi $= .086$), *Fake profile* (χ^2 (1, $N = 554$) $= 4.53$, $p = .033$, Phi $= .09$) and *Video call recording* (χ^2 (1, $N = 554$) $= 7.45$, $p = .006$, Phi $= .116$). Effect sizes were small.

Discussion

This study presents critical information about the changing nature and future of IPV. The pandemic resulted in a sharp increase in online activities, both good and bad. Although some activities reverted to their original state

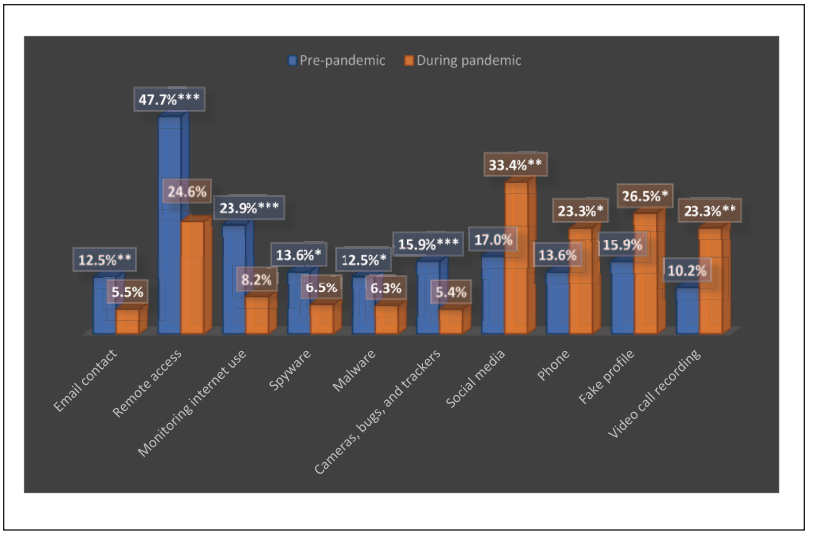

Figure 2. TFIPV methods that showed significant differences in proportional prevalence prior to and during the pandemic ($N = 554$).
*$p < .05$. **$p < .01$. ***$p < .001$.

post-pandemic, many remained online as certain practices were normalised, and as we move forward, the use of technology will increase. Thus, the present results are important to consider in future research and practice.

Summary of Findings

The results revealed three key findings: (a) there was a substantial increase in the perpetration of all online harm and TFIPV during the pandemic, (b) there is large variation in types of abusive behaviour and methods used to perpetrate TFIPV, and (c) both relationship type and the pandemic restrictions impacted the types of abusive behaviour perpetrated and the methods used by perpetrators.

The substantial increase of over 400% in TFIPV during the pandemic recorded by The Cyber Helpline is in line with increases reported in several countries, who had a 50% to 70% increase in IPV-related calls to police, emergency services, shelters, and helplines (Global News Canada, 2020; Tolan, 2020; Women's Safety New South Wales, 2020), as well as a 950% increase in website visits reported by Refuge (2020).

Types of abuse identified by The Cyber Helpline and researchers were in line with previous types of abuse recognised in the literature (Dardis & Gidycz, 2019; Freed, et al., 2018; Woodlock et al., 2020), as well as broadly in line with the four overarching categories identified in the introduction (Pina et al., 2021), with cyberstalking, harassment (e.g., harassment, creating fake profiles, outing, online reporting), IBSA (e.g., non-consensual sharing of intimate images/revenge porn, sextortion, content for ransom), and indirect non-sexual abuse (e.g., unauthorised access, device interception, fraud/identity theft, and website theft). The reader will notice some differences in the groupings of types of abuse in this study compared to those identified in the literature; the present groupings were led by the commonalities in behaviours reported and coded in the data from the helpline, and it was deemed important to represent the data as accurately and clearly as possible.

The Cyber Helpline data confirmed that the expected types of TFIPV were present in the abuse reported by victims accessing their services, but also generated some novel findings regarding the length of the intimate relationship between the perpetrator and victim. *Extortion* was more common in brief relationships and increased during the pandemic. This could be due to more individuals entering online relationships and engaging in online sexual behaviour during the pandemic, which they would have otherwise done in person, thus increasing the opportunity for extortion. It could also be the result of individuals losing employment and/or taking advantage of the increase in online intimate encounters to make money through extortion. This suggests that in at least some cases, length of relationship may have marked a distinction in TFIPV motive, where TFIPV in brief relationships may have included planned crimes for profit and in long-term relationships included more traditional motives for IPV such as control, jealousy, revenge and wanting to maintain/extend the relationship. *Unwanted contact and communication* were more common in long-term relationships. Wanting to remain in contact with the victim following a long rather than brief relationship could be explained by several factors, such as a greater desire to resume the relationship or punish the victim for a perceived wrongdoing and greater opportunity due to shared children, belongings etc. This might also relate to the fact that cyberstalking was proportionally more common pre-pandemic, since during the lockdown, fewer long-term relationships may have begun due to a lack of contact with others. *Device interception* only occurred in long-term relationships and decreased during the pandemic. This TFIPV type is also facilitated by victim knowledge as well as access to victim devices, which may account for it only being perpetrated in long-term relationships and mostly pre-pandemic, where perpetrators would have proximity to the victim and their devices.

TFIPV methods identified varied in nature and frequency but were mostly in line with methods identified in previous literature (Chatterjee et al., 2018; Fernet et al., 2019; Harkin et al., 2020; Parsons et al., 2019). Again, groupings of methods were led by the data and focused on communication, dissemination, surveillance, and card fraud methods and advice given from the helpline. Diverse levels of technological skill were required to use the methods identified in the data, but most commonly, limited technological skill was required, as evidenced by the prevalence of communication through *Social media* and *Phone* and information dissemination via V*ideo call recording*.

As with abuse types, the novelty identified in The Cyber Helpline data pertains to the nature of the relationship between the perpetrator and victim. Perpetrators in brief relationships were more likely to use methods that involved communicating with or about (dissemination) the victim. Based on the categorisation of methods, this likely represents the heightened use of extortion by this group. Specifically, where perpetrators communicated with victims to record video, obtain images and then make demands (i.e., blackmail) as well as threaten victims to force the creation of more content or threaten dissemination for monetary gain.

At the individual method level, the most common pre-pandemic methods included *Email contact, Remote access, Monitoring internet use, Spyware, Malware* and *Cameras, bugs and trackers*. There are several potential reasons for this variation. First, some of these methods are more technically complex than those that were used more frequently during the pandemic (i.e., *Social media, Phone, Fake profile*, and *Video call recording*). This may reflect the fact that pre- and post-pandemic circumstances were markedly different regarding remoteness and access, thereby forcing a change in methods that would have been less available during lockdown (e.g., using simpler methods, such as social media, due to a lack of access). Second, pre-pandemic perpetrators who engaged in TFIPV did so as a first choice based on their technological expertise/experience, while during the pandemic, perpetrators who engaged in TFIPV did so out of necessity due to a lack of contact with victims and thus used less complex methods given their more limited skill sets. A third potential reason for the variation is that the lockdown increased the time that individuals spent online, and by default increased the information they volunteered online as well as normalised certain practices (e.g., video calls over phone calls, sexual encounters via video call). This behaviour change increased the opportunities available to perpetrators to exploit for use in TFIPV. Pre-pandemic perpetrators may have therefore needed to use more complex and surveillance-based methods to access and uncover the same level of information that was more freely available during lockdown.

Data from The Cyber Helpline confirms the mixed findings of previous research with regards to gender and TFIPV. Due to missing data, we were unable to run inferential statistics on gender, but our frequency results showed males to more often perpetrate and females to more often be the victims of TFIPV. This finding is very much in line with the research on IPV (Clemens et al., 2023), and the perpetration aspect of TFIPV, where males are most often reported as perpetrators toward both men and women (Powell & Flynn, 2023). It also aligns with some research findings showing a higher prevalence of victimisation among females (especially in sexual coercion and threat) but contrasts other findings on victimisation that have shown no significant gender differences (Brown et al., 2021; Powell & Flynn, 2023). Our results also directly contradict the findings of Dardis and Gidycz (2019), who found higher rates of female perpetration for less severe TFIPV (such as monitoring and tracking) and no gender differences in perpetration for the more severe types (e.g., IBSA, hacking, harassment). This could be explained by the fact that the TFIPV victims who sought help from The Cyber Helpline were predominantly female. This is in line with IBSA and the Technology Facilitated Sexual Violence literature that shows women to be more likely to report being impacted by their cyber-victimisation compared to men, despite mixed findings with regards to victimisation rates between genders (Powell & Henry, 2019, 2024). As The Cyber Helpline is a charity that helps victims of cybercrime, and women are reported as more impacted by those crimes, it is logical that women would be more likely to recognise their victimisation and seek help.

Finally, most of those in the sample who reported their age were adults (4.2% said they were <18). Also, 85% of those who sought help did so for themselves rather than on behalf of someone else. Literature on young people and children with mental health problems indicates that active help seeking increases with age and that they predominantly do not seek help due to embarrassment, difficulty recognising the problem, and an inability to deal with the difficulty caused by the problem (Radez et al., 2021). Therefore, it is reasonable to surmise that those who would seek The Cyber Helpline's services would be more likely to be adult victims recognising the abuse they are experiencing and looking for advice on removing content or securing their devices.

Results should be interpreted in light of study limitations. First, in August 2020 The Cyber Helpline introduced a Helpdesk to coordinate their files, which previously had been primarily contained in email correspondence. This was an important change to their procedures, which helped them manage the over 400% increase in demand. For the purposes of coding, it meant that files were more detailed and complete after August 2020. To mitigate this

change, The Cyber Helpline made all files available to the coders and assisted with any queries, consulting as needed to ensure accurate coding. Nevertheless, this change may have had an impact on pandemic comparisons. Specifically, although spikes in reporting due to media coverage, technical difficulties or training by The Cyber Helpline staff may have been averaged out in our year-over-year comparisons, we cannot fully account for potential distortions that could affect the analysis and interpretation of longitudinal trends. Second, sample characteristics were missing in a large number of cases. This can occur where data are collected for purposes other than research. The result is that limited conclusions can be drawn about population characteristics and how to target findings at specific demographic groups. This may limit the generalisability of the results and is an important area of future research. Relatedly, the length of current relationships was not recorded by the charity, and thus such relationships could not be categorised as brief or long-term. This impacted a small portion of the sample (7.9%, $n = 44$), and coupled with the self-selection of individuals who have decided to contact The Cyber Helpline for assistance, only gives us information for people who either left abusive relationships or are in the process of leaving one. This will likely underrepresent those individuals who are still in abusive situations or unable to seek help. This may skew the TFIPV patterns we observed and also limit the generalisability of the results, and should be considered in future research.

Beyond the limitations outlined, there are also several strengths to this study. As discussed previously, we examined a current and evolving issue, thus contributing to our understanding of TFIPV and online harm. The study involved a large and representative sample of all online harm cases reported to The Cyber Helpline in a 2-year period. The results enabled us to examine the impact of lockdowns and other restrictions on TFIPV and revealed unique impacts of the pandemic on TFIPV prevalence, type and method.

Implications for Research

The results provide several points of focus for future research. In the first instance, the terminology, definitions, and behaviours comprising TFIPV should be harmonised and agreed upon. Our groupings of types and methods were largely led by The Cyber Helpline data which resulted in some slight variation compared to groupings in previous literature. Harmonisation will result in more accurate prevalence and co-morbidity rates as well as comparable research outcomes in the future.

As indicated by the differences found in both types and methods of TFIPV by relationship type, future research on TFIPV needs to include a wide range of relationship types to identify further differences that may assist with

prevention and case management. Finally, given the ever-changing nature of technology, it will be necessary to keep abreast of evolving types and methods of TFIPV and be vigilant of ways that innocuous technologies may be used for abusive and controlling purposes.

Implications for Practice

The existence of charities, such as The Cyber Helpline, which has since the completion of this study expanded into the USA, is a positive sign of the recognition of TFIPV and significant support to victims. Nevertheless, more work is required, and the results provide some suggested paths forward related to victim and public education and victim protection. Although much public discourse and concern about being online centres around theft and highly technical methods, the present sample demonstrates that in the context of TFIPV, these concerns are misplaced. The primary types of abusive behaviour committed by perpetrators were *Unwanted contact and communication*, such as *cyberstalking, Catfishing* and *Harassment* and *Extortion*, often through simplistic methods such as *Social media* and *Video call recording*. Education that brings perceptions of TFIPV in line with the realities of perpetration might help to dispel misplaced fears and help individuals to protect themselves. For instance, victims may feel powerless against perpetrators whom they believe to be more technologically capable. Thus, learning that most TFIPV behaviours and methods require limited expertise may embolden victims to take action to safeguard themselves or seek help.

The results also suggest that education could be targeted based on relationship type. For instance, those in brief relationships could be targeted with warnings about the images they share and the intimate behaviours that they engage in online that could be recorded. For those in longer-term relationships, education could focus on the access that partners have to devices, apps and passwords and well as limiting the use of personal information in creating passwords.

With respect to victim protection, the results could be used to prioritise professional education and develop a method checklist for victims. Police officers should be equipped with the knowledge and confidence to recognise types and methods of TFIPV. Being able to identify compromised accounts and devices will assist officers in gathering evidence and responding to victims. Our findings could be used to focus training on the most common TFIPV types and methods. Findings could also be used to develop a checklist of all TFIPV methods that officers, charities, and victims could use to systematically check for the presence of methods across devices and accounts.

This could help identify additional covert methods used by perpetrators that victims are unaware of, and also help to uncover evidence.

The use of social media was the most common method employed by perpetrators, which supports calls for additional safety provisions and platform accountability in managing online harm by social media organisations, app developers, and technology companies. The Online Safety Act, 2023 is a set of UK laws that places a range of new responsibilities on social media companies and search engines regarding user safety. Providers will need to implement systems aimed at reducing risks for illegal activity and remove the content if it does appear (Department for Science, Innovation and Technology, 2024).

This study shows TFIPV to be a growing problem that comprises diverse types of abuse and methods of perpetration. TFIPV varied based on the pandemic and the length of the victim-perpetrator relationship. Professional and victim education is needed to enhance victim protection. The results suggest key areas such as dispelling myths around tech-savvy perpetrators, highlighting the most common TFIPV methods and targeting education around relationship type (i.e., brief vs. long-term). Future research to identify and agree upon types of abuse and methods, as well as definitions, is necessary to obtain accurate prevalence rates. Continuous updates based on technological advancement are needed and should be prioritised and captured within the IPV literature, given the growing presence of technology in our lives.

Acknowledgements

We wish to thank Abby Hare, Rachel Tisi and Gaya Ildeniz for their help with data collection.

ORCID iD

Jennifer E. Storey https://orcid.org/0000-0002-6432-2514

Funding

The authors disclosed receipt of the following financial support for the research and/or authorship of this article: Funding was provided by the Home Office under the Domestic Abuse Perpetrator Research Fund 20/21. The views reflected in the research are not necessarily those of the Home Office.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interests with respect to the authorship and/or publication of this article.

Note

1. Phi = .10 represents a small effect size, Phi = .30 represents a medium effect size, and Phi = .50 represents a large effect size (Cohen, 1988). Cohen's *d* can be interpreted as small (*d* = .2), medium (*d* = .5), and large (*d* = .8) (Cohen, 1988).

References

Brookfield, K., Fyson, R., & Goulden, M. (2024). Technology-facilitated domestic abuse: An under-recognised safeguarding issue? *The British Journal of Social Work*, *54*(1), 419–436. https://doi.org/10.1093/bjsw/bcad206

Brown, C., Sanci, L., & Hegarty, K. (2021). Technology-facilitated abuse in relationships: Victimisation patterns and impact in young people. *Computers in Human Behavior*, *124*, Article 106897. https://doi.org/10.1016/j.chb.2021.106897

Campbell, A. M. (2020). An increasing risk of family violence during the Covid-19 pandemic: Strengthening community collaborations to save lives. *Forensic Science International Reports*, *2*, Article 100089. https://doi.org/10.1016/j.fsir.2020.100089

Census (2021). *Domestic abuse during the coronavirus (COVID-19) pandemic, England and Wales: November 2020*. [online] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseduringthecoronaviruscovid19pandemicenglandandwales/november2020

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018, May). The spyware used in intimate partner violence. In *Proceedings – IEEE symposium on security and privacy* (pp. 441–458). https://nixdell.com/papers/spyware.pdf

Chen, A., Cho, H., Evans, R., & Zeng, R. (2023). Reimagining communication in a post-pandemic world: The intersection of information, media technology, and psychology. *Frontiers in Psychology*, *14*, Article 1154044. https://doi.org/10.3389/fpsyg.2023.1154044

Clemens, V., Fegert, J. M., Kavemann, B, Meysen, T., Ziegenhain, U., Brähler, E., & Judd, A. (2023). Epidemiology of intimate partner violence perpetration and victimisation in a representative sample. *Epidemiology and Psychiatric Sciences*, *32*, e25. https://doi.org/10.1017/S2045796023000069

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Erlbaum Associates.

Crown Prosecution Service. (2024). *Legal guidance, domestic abuse, cyber / online crime*. https://www.cps.gov.uk/legal-guidance/stalking-or-harassment

Dardis, C. M., & Gidycz, C. A. (2019). Reconciliation or retaliation? An integrative model of postrelationship in-person and cyber unwanted pursuit perpetration among undergraduate men and women. *Psychology of Violence*, *9*(3), 328–339. https://doi.org/10.1037/vio0000102

Department for Science, Innovation and Technology. (2024). *Online safety act: Explainer*. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

Dixon, S. (2022). *Social media use during COVID-19 worldwide – statistics & facts*. Statista. https://www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/#topicHeader__wrapper

Domestic Abuse Act (2021). [online] www.legislation.gov.uk/ukpga/2021/17/contents

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

Fernet, M., Lapierre, A., Hébert, M., & Cousineau, M. M. (2019). A systematic review of literature on cyber intimate partner victimization in adolescent girls and women. *Computers in Human Behavior*, *100*, 11–25. https://doi.org/10.1016/j.chb.2019.06.005

Flach, R. M. D., & Deslandes, S. F. (2019). Cyber dating abuse or proof of love? The use of apps for surveillance and control in affective-sexual relations. *Cadernos de Saude Publica*, *35*(1), Article e00060118. https://doi.org/10.1590/0102-311x00060118

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018, April). *"A stalker's paradise": How intimate partner abusers exploit technology* [Conference session]. Conference on Human Factors in Computing Systems-Proceedings. https://nixdell.com/papers/stalkers-paradise-intimate.pdf

Global News Canada. (2020). LAWS reports "alarming" surge in demand for services during COVID-19. https://globalnews.ca/news/7764058/lawc-alarming-surge-demand-services-covid-19-pandemic/

Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture*, *16*(1), 33–60. https://doi.org/10.1177/1741659018820562

Hinduja, S., & Patchin, J. W. (2020). Digital dating abuse among a National Sample of U.S. Youth. *Journal of Interpersonal Violence*, *36*, 11088-11108. https://doi.org/10.1177/0886260519897344

International Telecommunications Union (2021). *Measuring digital development: Facts and figures 2021*. ITU Publications [online] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Kim, C., & Ferraresso, R. (2023). Examining technology-facilitated intimate partner violence: A systematic review of journal articles. *Trauma, Violence, & Abuse*, *24*(3), 1325-1343. https://doi.org/10.1177/15248380211061402

Leitão, R. (2019). Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *DIS 2019-proceedings of the 2019 ACM designing interactive systems conference* (pp. 527–539). https://ipvtechbib.randhome.io/pdf/leitao2019_2.pdf

López-Cepero, J., Vallejos-Saldarriaga, J., & Merino-García, M. (2018). Digital Intimate Partner Violence Among Peruvian Youths: Validation of an Instrument and a Theoretical Proposal. *Journal of Interpersonal Violence*, *36*(11-12), 5167–5185. https://doi.org/10.1177/0886260518803610

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of things': How abuse is getting smarter. *Safe-The Domestic Abuse Quarterly*, *63*, 22-26.

National Police Chief's Council. (2023). *Strategic threat and risk assessment of violence against women and girls* [online]. Vulnerability Knowledge and Practice Programme. https://www.npcc.police.uk/SysSiteAssets/media/downloads/our-work/vawg/violence-against-women-and-girls—strategic-threat-risk-assessment-2023.pdf

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). *Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse* [Conference session]. ACM International Conference Proceeding Series. https://www.nspw.org/papers/2019/nspw2019-parkin.pdf

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry*. https://citizenlab.ca/docs/stalkerware-holistic.pdf

Pina, A., Storey, J. E., Duggan, M., & Franqueira, V. (2021). *Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19*. Home Office Report. https://kar.kent.ac.uk/95001/

Police Service of Northern Ireland. (2023). *Domestic abuse incidents recorded by the police in Northern Ireland Update to 31st of December 2024*. https://www.psni.police.uk/system/files/202502/1683686803/Domestic%20Abuse%20Bulletin%20Period%20Ending%2031st%20December%202024.pdf

Powell, A., & Flynn, A. (2023). Technology-facilitated abuse victimisation: A gendered analysis in a representative survey of adults. *Feminist Criminology*, *18*(5), 435-458. https://doi.org/10.1177/15570851231196548

Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, *34*(17), 3637-3665. https://doi.org/10.1177/0886260516672055

Powell, A., Scott, A. J., Flynn, A., & McCook, S. (2022). Perpetration of image-based sexual abuse: Extent, nature and correlates in a multi-country sample, *Journal of Interpersonal Violence*, *37*, 23–24.

Powell, A., Scott, A. J., Flynn, A., & McCook, S. (2024). A multi-country study of image-based sexual abuse: Extent, relational nature and correlates of victimisation experiences. *Journal of Sexual Aggression*, *30*(1), 25-40.

Radez, J., Reardon, T., Creswell, C., Lawrence, P. J., Evdoka-Burton, G., & Waite, P. (2021). Why do children and adolescents (not) seek and access professional help for their mental health problems? A systematic review of quantitative and qualitative studies. *European Child & Adolescent Psychiatry*, *30*, 183–211. https://doi.org/10.1007/s00787-019-01469-4

Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). Snooping and sexting: Digital media as a context for dating aggression and abuse among college students. *Violence Against Women*, *22*(13), 1556–1576. https://doi.org/10.1177/1077801216630143

Refuge. (2020). *70% of refuge service users identify experiencing tech abuse*. https://www.refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/

Refuge (2022). *Marked as unsafe: How online platforms are failing domestic abuse survivors*. https://refuge.org.uk/wp-content/uploads/2022/11/Marked-as-Unsafe-report-FINAL.pdf

Sutton, D., & Dawson, M. (2021). Differentiating characteristics of intimate partner violence: Do relationship status, state, and duration matter? *Journal of Interpersonal Violence*, *36*, 9-10. https://doi.org/10.1177/0886260518795501

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

Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT research report: Internet of things and implications for technology facilitated abuse. https://discovery.ucl.ac.uk/id/eprint/10140276/

Tolan, C. (2020). Some cities see jumps in domestic violence during the pandemic. *CNN*. https://edition.cnn.com/2020/04/04/us/domestic-violence-coronavirus-calls-cases-increase-invs/index.html

Women's Safety New South Wales. (2020). *Impact of COVID-19 on migrant and refugee women and children experiencing DFV*. https://www.womenssafetynsw.org.au/impact/publication/impact-of-covid-19-on-migrant-and-refugee-women-and-children-experiencing-dfv/

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women*, *23*(5), 584–602. https://doi.org/10.1177/1077801216646277

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). Technology as a weapon in domestic violence: Responding to digital coercive control. *Australian Social Work*, *73*(3), 368–380. https://doi.org/10.1080/0312407X.2019.1607510

Author Biographies

Jennifer E. Storey, PhD, is a senior lecturer in forensic psychology in the School of Psychology at the University of Kent. Her research examines stalking, older adult abuse, intimate partner violence and violence risk assessment. She is the author of a violence risk assessment tool for the abuse of older people called the Harm to Older Persons Evaluation or HOPE.

Afroditi Pina, PhD, is a reader in forensic psychology at the Centre of Research and Education in Forensic Psychology (CORE-FP) at the University of Kent. Her main areas of research are online and offline sexual violence, including rape and sexual harassment, image-based sexual abuse, intimate partner violence and self and sexual objectification.