Sugiura, Lisa, Button, Mark, Nurse, Jason R. C., Tapley, Jacki, Belen-Saglam, Rahime, Hawkins, Chloe, Frederick, Brian and Blackbourn, Dean (2024) *The Technification of Domestic Abuse: Methods, Tools, and Criminal Justice Responses.* Criminology & Criminal Justice . ISSN 1748-8958.

The Technification of Domestic Abuse: Methods, Tools, and Criminal Justice Responses

Lisa Sugiura: (Corresponding Author) ORCID ID – 0000-0002-2167-3613, Associate Professor in Cybercrime and Gender University of Portsmouth lisa.sugiura@port.ac.uk

Mark Button: ORCID ID - 0000-0002-4169-2619, Professor of Criminology University of Portsmouth mark.button@port.ac.uk

Jason R. C. Nurse: ORCID ID - 0000-0003-4118-1680, Reader in Cyber Security University of Kent J.R.C.Nurse@kent.ac.uk

Jacki Tapley: ORCID ID - 0000-0002-6218-5392, Principal Lecturer in Victimology and Criminology University of Portsmouth jacki.tapley@port.ac.uk

Rahime Belen-Saglam: ORCID ID - 0000-0002-6969-645, Lecturer in Computer Science and Digital Technologies University of East London. r.belen-saglam@uel.ac.uk

Chloe Hawkins: ORCID ID - 009-0000-2435-2658, Senior Lecturer in Criminology and Criminal Justice University of Portsmouth chloe.hawkins@port.ac.uk

Brian Frederick: Assistant Professor in Criminal Justice SUNY Empire State College brian.frederick@sunyempire.edu

Dean Blackbourn: ORCID ID 0000-0003-1265-9745, Senior Lecturer in Counter Fraud Studies University of Portsmouth dean.blackbourn@port.ac.uk

Abstract

Methods of domestic abuse are progressively incorporating computer misuse and other related online offences, and digital tools, escalating opportunities for perpetrators to monitor, threaten and humiliate their victims. Drawing on empirical research involving media case study analysis, a technology review, and interviews undertaken with 21 professionals and service providers supporting domestic abuse victims, this article outlines the context in England and Wales regarding the methods, tools and criminal justice responses involved in what we conceptualise as the *technification of domestic abuse*. As technology continues to deeply intertwine with our daily lives, it is undeniable that its involvement within domestic abuse encompasses harmful behaviours that pose an increasing risk of harm, and unless effective criminal justice interventions are implemented, this risk will inevitably grow even further.

Keywords

Domestic abuse, violence, technology, computer misuse, online, coercive control

In the year ending March 2022 in England and Wales (E&W), approximately 2.4 million individuals aged 16+ (1.7 million women and 699,000 men) experienced domestic abuse (DA) (ONS, 2022). Additionally, of all offences recorded by the police, 17.1% were DA related (ONS, 2022). The Domestic Abuse Act 2021 (DAA), for the first time in E&W, provides a statutory definition of DA that emphasises emotional, coercive, controlling, and economic abuse, not just physical violence. Despite many victims of DA also experiencing technology-facilitated domestic abuse (TFDA) in some form, and there often being digital evidence of abusive behaviours in DA cases, the DAA does not explicitly mention the role of technology in DA, even though the UK Government claims the legislation is designed to be 'future-proof' to address emerging trends, including tech abuse (POST, 2020). The aim of this article is to examine the nature and impact of TFDA, which we refer to as the technification of domestic abuse (TDA) within the E&W criminal justice landscape. By providing an empirically informed perspective on the digital methods and tools utilised by perpetrators, and the application of legislation in response to the problem, this article contributes to the limited evidence base on TFDA in E&W and demonstrates the complexity of potential criminal offences committed by perpetrators of TFDA. While the term intimate partner violence (IPV) acknowledges the context of coercive and controlling relationships (Stark, 2007), DA is more commonly used within E&W criminal justice and other agencies.

We utilise the technification of domestic abuse as an integral aspect of coercive control (Dragiewicz et al., 2018; Yardley, 2020), which encompasses a pattern of behaviour aimed at depriving individuals of their freedoms, liberties, and independence in such situations (Pain, 2014; Pence & Paymar, 1993; Stark, 2007). Our research analysis is grounded in the concept of coercive control (Johnson, 1995; Schechter, 1982; Stark, 2007), which explores how women are coerced and controlled by their male partners. Stark (2007, p.5) describes coercive control as the 'micro-regulation of women's lives', with the sex of the victim and perpetrator and societal gender norms playing significant roles. Section 76 of the Serious Crime Act 2015 (SCA) introduced the offence of coercive and controlling behaviour in E&W. It is important to note that this legislation is gender neutral and encompasses the coercive and controlling effects of a course of conduct between partners, regardless of their gender or sexual orientation. This means it can apply to male victims of DA in heterosexual or homosexual relationships, as well as individuals who identify as non-gender binary. Some research challenges the gendered framework of Stark's concept, suggesting that both women and men can exhibit coercive and controlling behaviours in heterosexual intimate relationships (Bates et al., 2014; Bates & Graham-Kevan, 2016). Nevertheless, the absence of a gendered focus in the legislation limits the potential impact of the offence, particularly considering the alarmingly low number of coercive and controlling offences that are recorded (Barlow et al., 2020). While our research considers individuals of all genders, it is important to note that women were overwhelmingly victims and men were the perpetrators, highlighting the need to understand the technification of domestic abuse through this lens.

Additionally, Harris and Woodlock (2019) have introduced the term digital coercive control (DCC) to describe the utilisation of emerging technologies within the context of DA. DCC encompasses not only the specific technologies employed by perpetrators (such as mobile phones, GPS, and social media), but also considers their intentions, the impact on victims/survivors, and the contextual factors surrounding the occurrence of DCC. This term acknowledges the use of digital technology to engage in behaviours such as stalking, harassment, threats, and abuse against partners or ex-partners, including children. It also addresses the limitations of previous conceptualisations of coercive control, particularly within the specific context of intimate relationships and the broader framework of gender-based inequality (Woodlock et al., 2020).

It is crucial to recognise the significance of context within the realm of DA, especially in our digitally connected society (Powell et al., 2018), where technology is omnipresent, and surveillance has become normalised. As emphasised by Harris et al. (2021, p.7), "behaviours that appear identical may be abusive in the context of coercive and controlling relationships, while being innocuous or healthy in non-abusive relationships". For instance, certain applications may be used consensually in non-abusive relationships to track a partner's location for coordinating meetups. However, within an abusive relationship, the same app can be misused to stalk, monitor, and control the movements of an ex or current partner. Technologies that facilitate connectivity in healthy relationships, such as video calls like FaceTime between a parent and child, can pose risks for victims who share children with abusive partners (Dragiewicz et al., 2020; Leitão, 2018).

Moreover, activities involving technology that may not be illegal can be harmful when conducted within the context of DA. Perpetrators of DA routinely exploit online platforms, particularly social media. Technologies like geolocation software and spyware are used for surveillance, providing new means of monitoring and tracking victims' movements (Dragiewicz et al., 2018; Hand, Chung, & Peters, 2009; Khoo et al., 2019; Tanczer et al., 2018; Woodlock, 2017; Woodlock et al., 2020). According to a survey by UK Women's Aid, nearly a third of victim-survivors reported the use of spyware or GPS locators on their phones or computers by their current or former partners (Laxton, 2014). In 2020, the UK charity Refuge reported that 72% of their clients had been subjected to abuse via technology (Christie & Wright, 2020). Further demonstrating the increasing trend in TFDA, a national survey conducted by Refuge in 2021 found that approximately two million women across the UK, equating to one in six women, had been subjected to online abuse from a current or ex-partner (Refuge, 2021). Additionally, perpetrators have shifted from requiring specialised devices or hardware to track their victims to remotely hacking and monitoring their victims through the victims' own accounts. Nevertheless, such methods of abuse and the associated risks are often inadequately understood by the criminal justice system and practitioners supporting victim-survivors. Brookfield et al. (2023), in their article exploring the implications of TFDA on social work practice, highlight how current guidance and assessment tools for domestic abuse, including coercive control, are outdated, and not equipped to respond to abuse which is increasingly becoming digitised. As they note, TFDA is “rapidly becoming the norm rather than the exception” (Brookfield et al., 2023, p.419).

It is important to acknowledge that within feminist discourse, there has been ongoing debate regarding the suitability of terms such as ‘victim’ or ‘survivor’. In our study, we have employed the term ‘victim-survivor’ where appropriate to recognise the complexity of individuals' experiences. However, the term ‘victim’ is predominantly used in our findings to highlight the behaviours and actions of the perpetrator. It is worth noting that the term ‘victim’ is also commonly used within the criminal justice system (Gill et al., 2012). Furthermore, in this article, we use the terms ‘abuser’, ‘perpetrator’, and ‘offender’ interchangeably to refer to the individual engaging in abusive behaviour. These terms emphasise different aspects of their role and actions within the context of the technification of domestic abuse.

The Technification of Domestic Abuse

To comprehensively capture the diverse range of digital methods and tools employed by DA perpetrators, as well as the resulting harm experienced by victims, we propose the concept of the technification of domestic abuse (TDA). This concept encompasses how technologies are transforming the landscape of domestic abuse by assisting and enabling perpetrators, particularly within coercive and controlling relationships, while also exacerbating the harms inflicted upon victims. As emphasised by Douglas et al. (2019, p.566), it is crucial to examine "the context, meaning, motives, and outcomes of technology-facilitated behaviour" to fully understand the dynamics of DA.

DA is increasingly entwined with digital technologies, leading to significant alterations in the contexts and manifestations of abuse, with a growing reliance on technology. Technology has not only expanded the scope of where and how DA can occur, but it has also widened the range of individuals who can engage in DA and who may be victimised by it, ultimately amplifying the potential extent and impact of harms. Therefore, it is unhelpful to separate DA into distinct categories of in-person versus virtual, as our lives and social interactions are increasingly intertwined both online and offline (Powell et al., 2018). The technification of domestic abuse transcends the artificial divide between online and offline realms. However, it is important to acknowledge that understanding the prevalence and dynamics of technified domestic abuse encounters similar barriers as DA more broadly, including underreporting, under recording, and victims-survivors recognising the abuse they are experiencing (Douglas et al., 2019). The inclusion of technology adds further complexity to understanding, mitigating, and responding to potential criminal offences committed by DA perpetrators.

The technification of domestic abuse also considers the intersection between DA and other online offences, including E&W legislation such as the Computer Misuse Act 1990 (CMA) and the Malicious Communications Act 1998 (MCA). Additionally, it recognises the relevance of offline-oriented legislation, such as the Protection from Harassment Act 1997 (PHA), Fraud Act 2006 (FA), Protection of Freedoms Act 2012 (PFA), Criminal Justice and Courts Act 2015 (CJCA), and the Stalking Protection Act 2019 (SPA), which are increasingly applicable in the context of digital technologies. Moreover, this concept is transferable to international legislation that incorporates digital technologies, as it magnifies stalking, harassment, and threatening behaviours. By considering the interplay between DA and a broader range of legal frameworks, the concept of TDA recognises that the use of technology can intensify and extend the harmful behaviours associated with DA. It highlights the need for legislative responses to account for the evolving ways in which technology is employed to perpetrate abuse, both domestically and across international boundaries.

Computer misuse offences, especially unauthorised access, are often intertwined with other crimes, including DA, as they form part of a broader continuum of offending. Perpetrators of abuse often have physical access to their partners' devices and can either know, predict, or coerce the disclosure of access credentials like passwords, PIN codes, or swipe patterns (Freed et al., 2017; Matthews et al., 2017; Woodlock, 2017). This gives abusers an easy opportunity to install spyware, which can be obtained from app stores like Google Play Store or Apple App Store without requiring sophisticated technical knowledge (Chatterjee et al., 2018). In many cases, all that is necessary for the abuser is an understanding of social media platforms and the ability to manipulate the victim into trusting them with personal details.

The forms of TFDA often overlap with one another, as well as with physical, sexual, and emotional abuse. This complexity makes it difficult to rely solely on legislation to provide a comprehensive solution to the intersecting harms. Leitão (2019) conducted qualitative analysis of online discussion forums for victim-survivors of DA and found that a combination of abusive techniques is commonly employed. Eckstein and Danbury (2020) further elaborate on the means, methods, and tactics of what they refer to as technology-mediated abuse within DA contexts. These tactics include preventing or restricting a partner's access to technology, which in turn limits their communication with others and contributes to isolation and a lack of access to economic and support resources. Other tactics involve using social media to humiliate or damage a partner's reputation, as well as engaging in monitoring and stalking behaviours that may include threats and attacks. These multifaceted methods highlight the complex and intertwined nature of technology's role in domestic abuse.

Methodology

Adopting a constructivist paradigm, our research for this article employed a combination of methods to uncover new meanings and insights based on lived experiences. The following methods were utilised: media case analysis, technology review, and semi-structured interviews with professionals supporting DA victims. The project obtained full ethical approval from the relevant ethical review board. Each of these approaches was chosen for its unique perspective, allowing us to explore the identified issues from multiple angles and gather a comprehensive understanding of the topic.

i. Media case analysis involved a systematic examination of relevant cases reported in various media sources, such as news articles and online platforms. This approach allowed us to analyse real-life instances of TFDA and extract valuable insights from these cases. The selection criteria for the cases included evidence of a current or past relationship (such as marriage, partnership, or sexual relationship) or family relationship, as well as the illegal or unethical use of information communication technology (ICT) and other technological devices. The aim was to focus on cases where ICT was used beyond normal levels of communication or where there was a clear negative intent, illustrating the potential for ICT to enable harassment and abuse.

We utilised the Nexis Uni database, which covers reputable newspapers worldwide, along with specific databases of some UK local newspapers. Various search terms were employed to refine the search and narrow down relevant cases. The searches returned many articles, which were further refined to exclude non-relevant or duplicate cases. The researchers excluded cases that were non-ICT related, covered the same case multiple times, or lacked clear evidence of a relationship between the parties involved. It is important to note that the nature of media reporting sometimes made it challenging to ascertain whether the incidents were related to a specific relationship. In cases where doubt existed, those cases were excluded from the analysis. However, in the selected cases, there was clear evidence of a past, or existing relationship based on the terms used in the reporting (such as partner, husband, wife, boyfriend). In total, 146 cases were identified, with 117 cases from the UK and 29 cases from other countries included for greater context into the issue, including the USA, Australia, New Zealand, Belgium, Switzerland, Singapore, Saudi Arabia, and the Republic of Ireland. The cases demonstrated a wide range of ways in which technology was being used to facilitate abuse. It is important to acknowledge that a media analysis has limitations and does not provide a comprehensive representation of the broader landscape of technological abuse in and after relationships. However, the selected cases provide real-world examples of how ICT is being utilised to enable abuse.

ii. A Technology review to examine the technologies used in DA, their characteristics, and their availability online. The aim was to understand the options provided to perpetrators online, explore the ease of access and use of these technologies, and gather information about their cost, online retailers, and the types of digital data they targeted. The review was designed to fill a gap in previous studies conducted by computing scholars. While previous studies have explored aspects of TFDA, such as the disparity between technologies used by stalkers (Eterovic-Soric et al., 2017) and how perpetrators exploit technologies to harm victims (Freed et al., 2018; Leitão, 2019), not all of them focused on the specific data targeted by these technologies or provided detailed information about the tools and their use for abuse.

To begin the review, a comprehensive search strategy was designed. The initial set of queries was determined through internal project meetings involving domain experts and informed by an investigation into the scientific literature on technology misuse in DA. These queries aimed to be inclusive and cover a wide range of technologies and types of abuse. A total of 40 initial queries were used, which can be found in Table 1 below. Google was chosen as the primary search engine for these queries, given its prominence as the leading search engine. By utilising these queries and conducting searches on Google, the research aimed to identify and analyse the options available to perpetrators of DA online, considering various technologies and forms of abuse. This technology review was an important part of the research to gain insights into the tools and recommendations provided to perpetrators online, understand their capabilities, and assess the potential harm they can cause to victims.

Table 1: Initial Queries

Apps to monitor partners (or children)	Track my wife
Covert cameras	How to catch my cheating spouse on dating sites
Covert CCTV	How to use doorbell cameras to monitor my partner
Covert microphone	How to monitor my partner using key loggers
Covert parental control app or tracker	How to catch my cheating spouse
Couple tracker apps/devices	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s social media
Devices to monitor partners (or children)	Read SMS from another phone
Family tracking apps/mutual tracking	Track my girlfriend’s phone without them knowing
GPS tracker app free phone tracker app	Track my husband’sphone without them knowing
Monitor wife’s emails	How to use Alexa to spy on my wife

Remote control smart technologies abuse violence	Where to place covert camera in bathroom
Remote control technologies for home violence abuse	Read your wife’s messages without touching her phone
Spy on cheating partner	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Whatsapp?
Spy on partner	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Facebook’s account
Stalkerware	Track my husband’s car
Stealth monitorin apps/devices	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Instagram account?

Predictions made by Google for similar search queries in addition to the initial queries were collected. These predictions are based on previous relevant searches and popular search trends, reflecting the actions that potential perpetrators may take when conducting similar searches. This approach aimed to provide insight into the search landscape and the information that may be accessible to perpetrators.

However, it is important to acknowledge the algorithmic bias that exists within search engines like Google. Google's search results are personalised and customised based on various factors, such as location, browsing history, and IP address. The specific details of Google's algorithm is not publicly known, making it challenging for researchers to fully understand the extent of bias or customisation in search results. To mitigate this issue, the research team took precautions such as not being signed into their Google accounts and using browser private modes to minimise personalisation and obtain more neutral search results. However, our approach is not claiming to present the ‘only’ or ‘gold standard’ of search results. Instead, the value of the technology review lies in capturing the types of research results that individuals, including potential abusers, may encounter.

Significantly, the predictions provided by Google for similar search queries were observed to be semantically like the initial queries. This finding suggests that these predicted queries are also likely to be used by potential perpetrators when conducting searches on Google. After the data collection process, a total of 332 queries were obtained. These queries were collected from the initial queries, as well as the predictions made by Google. The sample of these queries can be seen in Table 2.

Table 2: Sample of Queries suggested by Google

Initial Query	Google search predictions
Tracker apps / devices	best phone tracker app without permission best phone tracker app free find my device imei tracker best phone tracker app for android gps tracker gps tracker app free phone tracker app
Spy on partner	spyine spy devices for cheating spouses secret cheating apps spy on spouse cell phone for free how to spy on partners phone uk how to find out if your spouse is cheating for free read cheating spouse text messages free find out if he's cheating app

Duplicate queries suggested by Google and queries that were not directly related to the research aims were removed. Queries were also excluded that did not generate any unvisited webpages on the first two result pages. As a result, the results from 76 queries were analysed in the final stage. The searches conducted on Google yielded a wide variety of resources. These included websites aimed at helping victim-survivors and providing information about digital safety, news articles discussing cases of DA where technology was misused, blogs reviewing different apps or devices, and websites promoting tools, apps, or devices related to TFDA. Due to the large number of results, analysis was focused on the webpages retrieved from the first two pages of Google search results, which amounted to an average of 20 search results per query. During the review of these webpages, the primary focus was on extracting the ‘recommendations’ provided to readers, who may be potential perpetrators of technological abuse. These recommendations were categorised into four broad groups: suggested apps to install, software programs, devices available for purchase, and actions that can be taken without relying on a specific app, software, or device.

iii. Semi-structured interviews (n= 21) were conducted with professionals in E&W who have first-hand experience working with victim-survivors of DA. These interviews provided valuable qualitative data, allowing us to explore the nuances within the technification of domestic abuse, understand the challenges faced by service providers, and uncover emerging trends and patterns in DA cases featuring technology.

The interviewees involved first-response police officers, and a crown prosecutor, as well as DA service providers and charities supporting individuals of any gender or ethnicity, those primarily supporting women, and those specifically supporting men. They were selected from different regions in England, including the South, Midlands, and North. While acknowledging the significance of the experiences of male victims, the gendered nature of domestic abuse, including TFDA, was emphasised during the interviews. Previous research suggests that abuse committed by men is often motivated by power and control (Barlow & Walklate, 2022; Johnson, 2006), which was also a key thread within our research.

The interviewees were instructed to focus on technological abuses that occurred within the context of DA relationships, whether during the relationship or following its breakdown, to identify broader patterns of coercive control. The interviews were conducted online synchronously using Zoom or MS Teams. They were audio recorded and lasted between 45 minutes to 2 hours, except for interviews 20 and 21, which were conducted via email due to time constraints. The interviews were reflexively thematically analysed, following the approach outlined by Braun and Clarke (2019). As scholars committed to critical intersectional feminist praxis, we reflected upon our underlying worldviews, values, and beliefs to acknowledge our position as mainly ‘insiders’ situated within the study in the qualitative research landscape. Our experience of researching in this field and of working with victims/survivors previously, meant that we shared attributes and characteristics with our participants, and not least, mutual goals of tackling abuses, especially against marginalised persons.

By employing these complementary research methods, we aimed to triangulate our findings and achieve a more comprehensive and nuanced understanding of the technification of domestic abuse. The combination of media case analysis, technology review, and interviews with service providers allowed us to gather diverse perspectives and shed light on different aspects, especially the digital methods and tools used within DA.

Methods involved within the Technification of Domestic Abuse

The findings from the media analysis and interviews revealed that computer misuse offences, particularly unauthorised access, are just one aspect of the broader range of abusive behaviours incorporating technology within the context of DA. As noted, these behaviours often overlap and combine with offences already covered by existing legislation. It is important to note however, that some harmful behaviours and activities involving technology, which are part of a wider pattern of DA and coercive or controlling behaviour, are currently not recognised as criminal offences, such as the use of fake accounts and legitimate digital tools to monitor, access and intimidate individuals. This leaves victim-survivors vulnerable to ongoing abuse without apparent legal recourse.

It is important to recognise that many media cases involved multiple forms of abuse, with technology playing a varying role. In some cases, the technological aspects were the primary or most significant part, while in others, there were various types of abuse occurring, some of which were not related to technology. It was observed that in controlling and coercive relationships, the technological abuse was often overshadowed by threats, physical violence, and sexual abuse experienced by the victim. These findings highlight the complex and multifaceted nature of the technification of domestic abuse and emphasise the need for comprehensive legal frameworks and support services that address the multiple forms of abuse perpetrators subject victims to.

i. Unauthorised Access

Perpetrators often gain unauthorised access to their victims' accounts through various means. One common method is by taking advantage of shared devices that have not been properly logged out of. Perpetrators may also exploit their personal knowledge of the victim's patterns to guess their passwords or emotionally coerce the passwords from the victim directly. In more extreme cases, victims may be forced to disclose their passwords under duress, threats, or actual violence.

> *"I think usually that happens when they're in the relationship. They are coerced into agreeing that if you love me and if you have nothing to hide then there's no reason why I can't have the password to your account. You must be doing something wrong otherwise you'd let me see, because you've got nothing to hide, have you?"* (Interviewee 9).

Emails and social media accounts, particularly platforms like Facebook, Instagram, and WhatsApp, are often targeted for unauthorised access. As email accounts serve as gateways to various aspects of individuals' lives and social media has become a prevalent mode of communication, they become prime targets for perpetrators.

In some instances reported in the media, victims of DA were involved with partners who exhibited coercive and controlling behaviours, utilising various methods that ranged from psychological threats of violence to actual acts of violence. In these cases, victims may have complied with their abusers' demands by providing access to their electronic devices, including handing over devices with accounts still logged in or sharing passwords and PINs. This enabled the abusers to gain unauthorised access to the victims' personal information, such as social media accounts and bank accounts. One example, which is representative of similar cases, involves a man in Kent who was convicted of coercive control. He exerted control over his partner's life, including taking control of her Facebook and bank accounts, through a combination of demands and acts of violence. Refusals or attempts to leave the relationship were met with verbal threats or actual physical violence. Such abusive behaviour can escalate the risk of harm to the victim, underscoring the dangerous dynamics present in cases of coercive and controlling relationships.

Theft is another method that perpetrators may use to gain unauthorised access to their victims' devices and accounts. In one case (Echo, 2020), an ex-boyfriend stole his ex-girlfriend's phone during a meeting at her workplace, which allowed him to access the phone and the accounts stored on it. He then proceeded to send explicit content to her friends and family members. In a similar case, a former partner broke into the victim's house, threatening her, and subsequently left with her device (Belfast Live, 2021). These actions demonstrate the lengths some perpetrators are willing to go to gain access to their victims' personal information and devices.

Even with the advent of biometric authentication methods, such as fingerprint or face recognition, some abusers find ways to exploit these security measures. For example, one case involved a partner who used their sleeping partner's thumb to unlock her phone, enabling access to her accounts (MailOnline, 2018). Additionally, there have been instances where perpetrators have enlisted the help of experts or hired individuals to hack into their victims' accounts, further highlighting the extent to which some abusers will go to carry out their abuse. It is important, however, to note that advanced technical skills are not always necessary to perpetrate computer misuse within the context of DA.

These examples highlight the manipulative tactics employed by perpetrators to gain access to their victims' digital accounts and control various aspects of their lives, which are not fully captured within the current criminal justice system in E&W. It demonstrates the need for comprehensive support and intervention to address the power imbalances and protect victims from ongoing abuse.

Spyware is a concerning tool used by perpetrators in DA to gain knowledge, access, and monitor their partners' or ex-partners' devices and activities. Spyware refers to apps or software that are installed on a device without the user's knowledge or consent, allowing the perpetrator to covertly monitor various aspects of the victim's digital life, including communications and location. Certain apps, explicitly marketed as spyware, are designed specifically for surreptitious surveillance, such as ‘Flexispy’, ‘Wife Spy’, ‘Girlfriend Spy’, ‘Spyera’, and ‘ePhoneTracker’ (Levy, 2014). These apps are created with the intention of enabling invasive monitoring and control in intimate relationships. However, there are also seemingly innocent apps that can be exploited by abusers for TFDA. These include GPS and Find My Phone apps, which have legitimate purposes like child or anti-theft protection. Abusers can repurpose these ‘dual-use’ apps to spy on their partners, taking advantage of their functionality to gain remote access to a device's sensors and data without the owner's knowledge (Chatterjee et al., 2018).

Both overt spyware and dual-use apps can cause harm in the context of DA. Dual-use apps are particularly concerning as they can be easily deployed in relatively simple ways. For instance, perpetrators may gift devices, especially to children, that are preloaded with spyware. They may also have access to the victim's device, allowing them to install spyware discreetly. The use of spyware in DA situations raises significant privacy and safety concerns for victims, as it allows abusers to intrude upon their private communications, monitor their movements, and maintain control over their lives. It underscores the need for awareness and vigilance regarding the potential misuse of apps and software, as well as the importance of digital security measures to protect against such invasive surveillance.

> *“A child of separated parents had been gifted a tablet by their father, who had instructed her that the tablet must always be on and charged 24 hours day, whilst she was with her mother, so that he can always speak with her. The father was able to know everything that occurred in his former partner’s new house and intimidate and control her via this means”* (Interviewee 7).

ii. Fake Accounts

The use of fake accounts is a significant method used in abusive relationships. Fake accounts can be created based on a fictitious person, real persons who are known to the victim (e.g., friends), or impersonate the victim themselves. For example, in a media case an ex-husband set up a fake Facebook profile of his former wife in which he detailed her fantasy to be raped, providing contact details, with one random man actually turning up at her work to meet her (The Sun, 2018). Many perpetrators do not have the skills or knowledge to hack victims' accounts, so this is a simpler means. It is also a greyer area legally. Hacking (i.e., applying any means to gain unauthorised access to) a person's account is a clear criminal offence, creating a fake account and impersonating someone is not. Although used with other activities, it can then form the basis of offences under stalking/harassment, malicious communication, etc. Often these fake accounts are set up to abuse and harass victims or are impersonating victims and presenting them in a derogatory manner, generally when relationships have ended. In one case discussed, where fake profiles had been set up on dating sites, Interviewee 7 highlighted that a victim was not only dealing with false representations of herself, but she also had to contend with other men trying to contact her on WhatsApp or text, because her mobile phone number was publicly divulged.

iii. Harassment, Stalking and Image-Based Sexual Abuse

The act of posting harassing and derogatory content about a victim on social media, especially using anonymous profiles, can indeed be a form of online harassment and may contravene the MCA. This Act makes it an offence to send or publish any electronic communication with the intention to cause distress or anxiety to the recipient. This includes messages or content that are grossly offensive, indecent, obscene, or menacing. In cases where perpetrators create anonymous profiles specifically to perpetuate abuse and tarnish their victim's reputation, they may be in violation of the MCA. By spreading false or harmful information about the victim on social media, they not only cause distress and anxiety but also potentially damage their personal and professional life. In one interview a case was described in which a woman's professional reputation was besmirched by her ex-partner using social media.

> *"On Facebook she has a public profile for her business, and he goes on saying she's a sex worker, like putting all this stuff over her Facebook wall, like putting fake reviews on like all of this stuff to sabotage her work"* (Interviewee 17).

Technology provides perpetrators with easy and accessible means to stalk and control their victims in cases of DA. Location apps like 'Find my phone' or geo-location features on social media platforms can be misused by perpetrators to monitor their victims' activities without their knowledge or consent. Perpetrators may use these tools to track the movements and whereabouts of their victims, thereby exerting control and instilling fear. Furthermore, perpetrators may manipulate victims into installing tracking devices on their devices under the guise of safety precautions. This manipulation can take various forms, such as convincing victims that it is for their own protection or falsely claiming that it will help locate lost devices. In reality, these trackers serve as tools for monitoring and further controlling the victims.

> *"One client said that her partner put a tracker on her phone and convinced her that he needed her to have it, so that if anything happened to her he could come and, you know, save her. Or, if she broke down or something he could come and help. And so, he did it in, like, a caring way, I guess convincing her that she needed to do this for her own benefit"* (Interviewee 3).

The combination of activities that, when considered within the broader context of domestic abuse, may fall under existing legislation such as the CMA, the MCA, the PHA, and the SPA. These laws can provide a basis for police intervention when perpetrators engage in a range of abusive behaviours, including persistent and unwanted communication through various channels like texts, emails, and social media messages. Furthermore, the SCA is applicable when coercive and controlling behaviours are present within an intimate relationship.

Perpetrators may engage in the non-consensual sharing or distribution of intimate images or videos to control, intimidate, and harm their victims. In some cases, perpetrators may secretly record intimate experiences and later use those recordings as a form of harassment or revenge after the relationship ends. This behaviour can cause significant distress and harm to the victim, as their privacy is violated, and their personal moments are shared without consent. The DAA has extended the offence of image-based sexual abuse to include the threat to disclose intimate images with the intention to cause distress. This legislative amendment acknowledges the harmful impact of threats related to the sharing of intimate images and provides a legal framework to address this form of abuse. Furthermore, the implementation of the Online Safety Act 2023 specifically criminalises the sharing of 'deepfakes' – explicit images or videos which have been manipulated to look like someone without their consent.

It is crucial for prosecutors to effectively utilise the provisions of the DAA to address image-based sexual abuse and related offences within the context of DA. Monitoring the implementation and application of this legislation will help ensure that victims are protected, perpetrators are held accountable, and the law reflects the evolving nature of the technification of domestic abuse.

The Technification of Domestic Abuse Tools

Our findings obtained via the technology review highlight the diverse range of technologies that are used in DA. These technologies can target different aspects of a person's identity, including their physical identity (such as voice, image, and location) and their digital data (such as messages and app usage). It is important to recognise that the same devices, applications, and behaviours can be used both for abusive purposes and for legitimate and protective purposes. Mainstream devices and services that are commonly used in everyday life can become tools for perpetrating abuse. This underscores the need to consider the context in which TFDA occurs, distinguishing between abusive relationships and healthy relationships or interactions. Understanding the specific dynamics and characteristics of abusive relationships is crucial for identifying and addressing TFDA.

The accessibility of devices used for monitoring the physical identity of individuals, such as covert cameras, microphones, and GPS trackers, through online retailers is indeed concerning. Popular platforms like eBay and Amazon provide a wide range of options for individuals seeking these devices. The availability and ease of purchase can enable perpetrators to obtain these surveillance tools without much difficulty. Furthermore, the ability to hide these devices in various forms raises additional concerns. For example, devices disguised as toys or other innocuous objects can be particularly troubling, as they may be used to exploit children or manipulate partners through the involvement of children. Perpetrators may use these devices to gain access to victims through their children or to control and surveil their partners. It is important to note here that the variety of options is much higher in local retailers in the UK compared to global ones. This underscores the need for increased awareness, education, and regulation surrounding the use and availability of surveillance devices. Efforts should be made to ensure that online marketplaces have appropriate policies and safeguards in place to prevent the misuse of these technologies and protect potential victims from harm. Online marketplaces should proactively address the ethical implications of selling technologies commonly misused in the context of domestic abuse. This involves integrating those issues into their ethical strategy agendas and clearly defining their values and ethical strategies during the development of their search engines. Their search engines could significantly contribute to protecting victims by refraining from prioritising the display of items with user reviews indicating their association with domestic abuse. Furthermore, incorporating legal warnings about the potential consequences of misusing these items would further promote responsible purchasing behaviour and help mitigate potential harm. Additionally, raising public awareness about the potential risks and signs of TFDA can help individuals identify and respond to such situations effectively.

The use of smart devices and the Internet of Things (IoT) in DA contexts is a concerning trend. Perpetrators are adapting to new technology and exploiting legitimate tools to further their abusive behaviours. Voice assistants like Alexa, smart heating systems like Hive, and video doorbells like Ring have been used by perpetrators to exert control and surveillance over their victims. For example, in cases where there has been a joint account for a voice assistant like Alexa that has not been updated after the victim ends the relationship, the perpetrator may have access to information about the victim's activities, including details of a new address. Perpetrators have also manipulated smart heating systems to emotionally abuse and inconvenience their victims by changing the temperature in the house. Video doorbell apps have been accessed by perpetrators to monitor the comings and goings of the victim.

It is important to note that guidance on how to misuse technological tools for abuse can be found online through simple search queries, which we found via our technology review. Perpetrators can learn how to access recordings from voice assistants, allowing them to gather information about instructions, voices, and the timing of interactions. This knowledge can help perpetrators track the presence of individuals in the home and potentially exploit this information for abusive purposes.

> "*Most smart speakers record audio and allow you to search back through those recordings. You could potentially use this to your advantage to find out exactly what your partner has been up to! Perhaps they have brought their lover back to your home and used the smart speaker to play a piece of music? Maybe they have checked their calendar or simply used the smart speaker at a time they were supposedly at work or away from home?*"[1]

Online options provided to perpetrators enable individuals to find, source and apply technologies to harm others in their domestic environment. These apps are marketed and advertised to individuals seeking to abuse or control their victims through technology. It is concerning that some stalkerware apps are presented as parental tools or employee trackers, providing misleading information about their true purpose. One example of such ambiguity is mSpy, which is a popular stalkerware app marketed as a parental control tool. This kind of misleading marketing can contribute to the normalisation of using stalkerware and may encourage individuals to install these apps under the guise of protecting their families[2]. Additionally, the presence of stalkerware apps in Google's search predictions when searching

[1] https://www.diemlegal.co.uk/amazon-alexa-echo-smart-tools-uncover-partners-infidelity/, April 2021

[2] For example, Google's current advertising policy is deficient as those products and apps can be advertised as parental tools and this enables service providers to put ads on Google, and in turn Google can return them without any conflict with its policy.

for terms like ‘Best stalkerware apps,’ as we discovered in our technology review, indicates a worrying normalisation and accessibility of these tools. It is important to address these ambiguities and ensure that the misuse of technology for abusive purposes is not continued to be encouraged.

Furthermore, it is crucial to recognise that abuse extends beyond purpose-built spyware. Dual-use apps, which have legitimate purposes such as tracking children or stolen devices, can be easily repurposed by perpetrators to abuse their victims. This highlights the need for awareness and education about the potential risks associated with these apps and the importance of responsible use of technology.

Discussion and Conclusion

As technology continues to become an integral part of our daily lives, the technification of domestic abuse expands the repertoire of potential criminal offences committed by perpetrators, involving harmful behaviours that can escalate and heighten the risk of harm to victims. This research has enabled us to refine the concept of the technification of domestic abuse to assist us in understanding the impact digital technologies have had upon perpetrator behaviours as well as the effects on victims. Moreover, it provides insight into the scope and reach of domestic abuse contexts that are increasingly intertwined with technology and emphasises how a greater range of persons can now engage in DA as well as be victimised by it, as a result of the merging of DA with technology. Hence, the technification of domestic abuse is also potentially creating new perpetrators and victims, which future research should explore in more detail. It is important to recognise that the methods and tools of perpetrators online are not fundamentally different from those used offline. Domestic abuse has always involved both contact-based (such as physical violence) and non-contact-based (such as coercive and controlling) forms of abuse, as well as physical harassment and stalking. Digital technologies have simply provided new avenues and tools to extend the range of non-contact-based harm. Technology-facilitated domestic abuse is often part of a broader pattern of perpetrator behaviour rather than a distinct type of harm. It is crucial to understand the specific instances and methods of technological abuse to ensure that policy, legislation, and support responses effectively address these evolving forms of abuse. While computer misuse offences, such as unauthorised access, are prevalent in DA contexts, they are only a part of the larger issue. Perpetrators engage in a wide range of abusive behaviours involving technology, including the use of spyware, creation of fake accounts, online harassment, stalking, image-based sexual abuse, and the installation of trackers. Some of these activities may fall under existing legislation, while others may not be explicitly illegal, but are still harmful and part of a broader pattern of coercive control. Furthermore, TFDA can take many forms and with the growth of artificial intelligence (AI) and Generative AI means that these forms of more immersive technology may be more prevalent in the future. For example, perpetrators could ask ChatGPT[3] how to track someone without them knowing. Whilst Google is a portal into searching for items, ChatGPT and similar systems can answer and provide immediate responses. Going forward, future risks arising from the increased technification of domestic abuse is an area requiring greater attention.

Societal challenges surrounding privacy and the right to separate aspects of digital life can contribute to the normalisation of the technification of domestic abuse. It is essential to recognise and address unhealthy behaviours within relationships and promote relationship-based understandings of DA and technology use. Public awareness should be increased regarding abusive relationships, unhealthy behaviours, and the importance of independence and online safety, without discouraging healthy relationships. Efforts should be directed towards comprehensive education, prevention, and support initiatives that address the complex dynamics of DA, including technology-facilitated domestic abuse. This involves challenging societal norms, promoting healthy relationship dynamics, and providing resources and education on digital safety and privacy. By doing so, we can work towards creating a society that rejects all forms of DA, whether conducted via technology or not, and supports the well-being and safety of all individuals.

[3] ChatGPT is a natural language processing chatbot driven by generative AI technology that allows you to have human-like conversations and much more. The AI tool can answer questions and assist you with tasks, such as composing emails, essays, and code. https://www.zdnet.com/article/what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/#google_vignette

For many victim-survivors, technology is not a separate category of abuse, but rather an integral part of a constellation of abusive behaviours. The inclusion of digital technologies intensifies the harm caused by other forms of coercive control, physical violence, and harassment. The research findings suggest that technology-facilitated domestic abuse is pervasive in most E&W DA cases. Interviewees emphasised that technology has become an intrinsic component of abuse, amplifying its insidious nature. However, perpetrators who engage in technology-related offences as part of their pattern of abuse are often not charged specifically for these crimes. Instead, they may be overlooked under broader categories such as stalking, harassment, control, or coercion. The ongoing use of technology in DA has long-term traumatic and psychological impacts on victims. It perpetuates a sense of being trapped and unable to escape the abuse, further exacerbating the victim's distress. Recognising the role of technology in facilitating DA as an aggravating feature is crucial. This recognition should lead to appropriate legal consequences, including increased sentences, to acknowledge the severity and harm caused.

Efforts should be made to raise awareness among legal professionals, law enforcement agencies, and policymakers about the specific dynamics and impacts of the technification of domestic abuse. This includes providing training on identifying and responding to technology-facilitated abuse, ensuring that relevant laws and policies explicitly address these forms of abuse, and consider the inclusion of technology-related offences as aggravating factors in sentencing guidelines. By recognising and addressing the unique challenges posed by increasingly technified domestic abuse, we can better support victims and hold perpetrators accountable for their actions.

Word count:7745

Glossary of Acronyms

AI - Artificial Intelligence

CJCA - Criminal Justice and Courts Act 2015

CMA - Computer Misuse Act 1990

DA - Domestic Abuse

DAA - Domestic Abuse Act 2021

DCC - Digital Coercive Control

E&W - England and Wales

FA - Fraud Act 2006

ICT - Information Communication Technology

IoT - Internet of Things

IPV - Intimate Partner Violence

MCA - Malicious Communications Act 1998

PFA - Protection of Freedoms Act 2012

PHA - Protection from Harassment Act 1997

SCA - Serious Crime Act 2015

SPA - Stalking Protection Act 2019

TDA - Technification of Domestic Abuse

TFDA - Technology-Facilitated Domestic Abuse

Funding Information

This work was supported by the UK Home Office Domestic Abuse Perpetrators Fund [grant number **ITT_178**]

Acknowledgements

Thank you to the professionals supporting victims-survivors of domestic abuse who so generously gave up their time to speak with us.

References

Barlow, C., & Walklate, S. (2022). *Coercive Control*. Oxon, Routledge.

Barlow, C., Johnson, K., Walklate, S., & Humphreys, L. (2020). Putting coercive control into practice: Problems and possibilities. *The British Journal of Criminology*, *60*(1), 160-179.

Bates, E. A., & Graham-Kevan, N. (2016). Is the presence of control related to help-seeking behavior? A test of Johnson's assumptions regarding sex-differences and the role of control in intimate partner violence. *Partner Abuse*, *7*, 3–25.

Bates, E. A., Graham-Kevan, N., & Archer, J. (2014). Testing predictions from the male control theory of men's partner violence. *Aggressive Behaviour*, *40*, 42–55.

Belfast Live (2021) Belfast man who conducted campaign of harassment against ex-partner jailed. Retrieved from https://www.belfastlive.co.uk/news/belfast-news/belfast-man-who-conducted-campaign-19812261

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589-597.

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.

Burke, S. C., Wallen, M., Vail-Smith, K., & Knox, D. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. Computers in Human Behavior, 27, 1162–1167.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., & Ristenpart, T. (2018, May). The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 441-458). IEEE.

Christie L., Wright S. (2020). *Technology and Domestic Abuse* [Online], London, UK Parliament.

Computer Misuse Act (1990). https://www.legislation.gov.uk/ukpga/1990/18/contents

Criminal Justice and Courts Act (2015). https://www.legislation.gov.uk/ukpga/2015/2/contents/enacted

Dimond, J.P, Fiesler, C., &. Bruckman, A. S. (2011) "Domestic violence and information communication technologies," *Interacting with Computers*, vol. 23, no. 5, pp. 413–421.

Domestic Abuse Act (2021). https://www.legislation.gov.uk/ukpga/2021/17/contents/enacted

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*, *59*(3), 551-570.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609-625.

Dragiewicz, M., O'Leary, P., Ackerman, J., Foo, E., Bond, C., Young, A. & Reid, C. (2020). *Children and Technology-facilitated Abuse in Domestic and Family Violence Situations: Full Report.*

Echo (2020) Spiteful ex sent explicit video of woman to her parents, sister and work colleagues. Retrieved from https://www.liverpoolecho.co.uk/news/liverpool-news/spiteful-ex-sent-explicit-video-19319000

Eckstein, J. J., & Danbury, C. T. (2020). What is violence now?: A grounded theory approach to conceptualizing technology-mediated abuse (TMA) as spatial and participatory. *The Electronic Journal of Communication*, *29*(3-4).

Eterovic-Soric, B., Choo, K. K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review. *Computers & security*, *70*, 278-289.

Fraud Act (2006). https://www.legislation.gov.uk/ukpga/2006/35/contents

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & N. Dell, N. (2017) "Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders," *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)*, vol. Vol. 1, no. No. 2, p. Article 46, 2017.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018, April). "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-13).

Gill, A., Radford, L., Barter, C., Gilchrist, E., Hester, M., Phipps, A., & Rummery, K. (2012). *Violence against women: Current theory and practice in domestic abuse, sexual violence and exploitation*. Jessica Kingsley Publishers.

Hand, T, Chung, D, & Peters, M. (2009). The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation. Australian Domestic & Family Violence Clearinghouse. Newsletter, 1-16.

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, *59*(3), 530-550.

Harris, B., Dragiewicz, M., & Woodlock, D. (2021). Harris, Dragiewicz and Woodlock Submission on Online Safety Legislative Reform.

Johnson, M. P. (2006). Conflict and control: Gender symmetry and asymmetry in domestic violence. *Violence against women*, *12*(11), 1003-1018.

Johnson, M. P. (1995). Patriarchal terrorism and common couple violence: Two forms of violence against women. *Journal of Marriage and the Family*, 283-294.

Kent Online (2020) Coercive behaviour conviction for Ramsgate bully who controlled girlfriend's Facebook profile. Retrieved from https://www.kentonline.co.uk/thanet/news/bully-behind-bars-for-controlling-girlfriends-life-223621/

Khoo, C., Robertson, K., & Deibert, R. (2019). Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.

Laxton, C (2014). ‘Virtual World, Real Fear: Women's Aid Report into Online Abuse, Harassment and Stalking. Women's Aid. Retrieved from https://www.womensaid.org.uk/virtual-world-real-fear/

Leitão, R. (2019). Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, 1-40.

Levy, K. E. (2014). Intimate surveillance. *Idaho L. Rev.*, *51*, 679.

Lucero, J., Weisy, A., Smith-Darden, J., & Lucero, S. (2014). Exploring gender differences: Socially interactive technology use/abuse among dating teens. Affilia: Journal of Women and Social Work, 29(4), 478–491.

Maher, J., McCulloch, J., & Fitz-Gibbon, K. (2017). *New Forms of Gendered Surveillance? Intersections of Technology and Family Violence*. In Marie Segrave and Laura Vitis (eds.), Gender, Technology and Violence (Routledge), 19.

MailOnline (2018) Controlling boyfriend, 24, who used sleeping girlfriend's thumb to unlock her phone and spy on her messages before threatening to kill himself if she saw a new man is found guilty of psychological abuse. Retrieved from https://www.dailymail.co.uk/news/article-6462793/Controlling-boyfriend-24-guilty-psychological-abuse.html

Malicious Communications Act (1988). https://www.legislation.gov.uk/ukpga/1988/27/section/1

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J.P, Shelton, M., Manthorne, C., Churchill, E.F, & Consolvo, S. (2017) "Stories from survivors: Privacy & security practices when coping with intimate partner abuse," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, pp. 2189–2201.

McGlynn, C., & Rackley, E. (2016). Not 'Revenge Porn,' But Abuse: Let's Call It Image-Based Sexual Abuse. *Inherently Human: Critical Perspectives on Law, Gender & Sexuality, 41*.

ONS (2020) *Domestic abuse in England and Wales overview: November 2022*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwalesoverview/november2022

Pain, R. (2014). Everyday terrorism: Connecting domestic violence and global terrorism. Progress in Human Geography, 38(4), 531–550. https://doi.org/10.1177/0309132513512231

Pence, E.& Paymar, M. (1993). Education groups for men who batter: The Duluth model. Springer.

POST UK Parliament (2020). *Technology and Domestic Abuse.* Retrieved from: https://post.parliament.uk/technology-and-domestic-abuse/

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.

Protection from Harassment Act (1997). https://www.legislation.gov.uk/ukpga/1997/40/contents

Protection of Freedoms Act (2012). https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Refuge (2021). *Unsocial Spaces: Make Online Spaces Safer for Women and Girls* [Online], London, Refuge.

Schechter, S. (1982). *Women and male violence: The visions and struggles of the battered women's movement*. South End Press.

Stalking Protection Act (2019). https://www.legislation.gov.uk/ukpga/2019/9/contents/enacted

Stark, E. (2007). *Coercive control: How men entrap women in personal life*. New York: Oxford University Press.

Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT research report. Retrieved from: https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf

The Sun (2018) Cruel husband used a fake Facebook profile to encourage men to rape his estranged wife in a sick revenge plot. Retrieved from https://www.thesun.co.uk/news/6889072/husband-fake-facebook-profile-encouraged-rape-wife-revenge-plot/

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

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.

Yardley, E. (2020). Technology-facilitated domestic abuse in political economy: a new theoretical framework. *Violence against women*, 1077801220947172.

Corresponding Author:
Dr Lisa Sugiura
lisa.sugiura@port.ac.uk
University of Portsmouth
02392845243

Authors:

(1) Lisa Sugiura: (Corresponding Author) ORCID ID – 0000-0002-2167-3613, Associate Professor in Cybercrime and Gender University of Portsmouth lisa.sugiura@port.ac.uk

Dr Lisa Sugiura is an Associate Professor in Cybercrime and Gender at the University of Portsmouth. Her research focuses on misogynistic extremism and technology-facilitated domestic abuse, and she publishes extensively and regularly contributes to mainstream media on these topics.

(2) Mark Button: ORCID ID - 0000-0002-4169-2619, Professor of Criminology University of Portsmouth mark.button@port.ac.uk

Professor Mark Button is a Co-Director of the Centre for Cybercrime and Economic Crime at the University of Portsmouth and has written extensively on fraud and cybercrime with particular reference to victimisation, offenders and policing responses to these crimes.

(3) Jason R. C. Nurse: ORCID ID - 0000-0003-4118-1680, Reader in Cyber Security University of Kent J.R.C.Nurse@kent.ac.uk

Dr Jason R.C. Nurse is a Reader in Cyber Security at the University of Kent. His research explores the security and privacy issues that emerge with new technologies, and he has published over 100 peer-reviewed articles across these domains.

(4) Jacki Tapley: ORCID ID - 0000-0002-6218-5392, Principal Lecturer in Victimology and Criminology University of Portsmouth jacki.tapley@port.ac.uk

Dr Jacki Tapley is a Principal Lecturer in Victimology and Criminology at the University of Portsmouth. Her research focuses on victims of crime, impact of victimisation, victims' experiences of the criminal justice system, professional cultures, and the development, evaluation and monitoring of victim-centred policies and legislation.

(5) Rahime Belen-Saglam: ORCID ID - 0000-0002-6969-645, Lecturer in Computer Science and Digital Technologies University of East London. r.belen-saglam@uel.ac.uk

Dr. Rahime Belen Saglam is a lecturer in Computer Science and Digital Technologies at the University of East London. Her interdisciplinary expertise includes data privacy regulations, human factors in cybersecurity, technology-facilitated domestic abuse, and online safety. Recently, her interests have expanded to AI ethics and the development of responsible technologies.

(6) Chloe Hawkins: ORCID ID – 009-0000-2435-2658, Senior Lecturer in Criminology and Criminal Justice University of Portsmouth chloe.hawkins@port.ac.uk

Dr. Chloe Hawkins, Course Leader for Criminology at the University of Portsmouth, specialises in victimisation, focusing on fraud, technology-facilitated domestic abuse, and hard to reach groups. She is the British Society of Criminology theme lead for Online Vulnerabilities.

(7) Brian Frederick: Assistant Professor in Criminal Justice SUNY Empire State College brian.frederick@sunyempire.edu

Dr. Brian J. Frederick is an Assistant Professor of Criminal Justice at SUNY Empire State University; his research focuses on LGBTQIA+ justice-involved persons. A native of Los Angeles, he completed an Erasmus Mundus Joint Doctorate in Cultural & Global Criminology at the University of Kent and Universität Hamburg.

(8) Dean Blackbourn: ORCID ID 0000-0003-1265-9745, Senior Lecturer in Counter Fraud Studies University of Portsmouth dean.blackbourn@port.ac.uk

Dean has been involved a broad range of research activities related to community safety, cold case reviews and victims of crime. He has worked with several police services throughout England and Wales, not only upon improving police relations with minority groups, but towards improving community safety.