



Computer Misuse as a Facilitator of Domestic Abuse

May 2021

Dr Lisa Sugiura, Professor Mark Button, Dr Jacki Tapley, Dr Brian Frederick, Mr Dean Blackbourn and Dr Chloe Hawkins
Institute of Criminal Justice Studies, University of Portsmouth, UK

Dr Jason R.C. Nurse and Dr Rahime Belen-Saglam
School of Computing and Institute of Cyber Security for Society (iCSS), University of Kent, UK

Project funded by the UK Home Office Domestic Abuse Perpetrators Research Fund

The views expressed within this report are not necessarily representative of those of the Home Office

Acknowledgements

We would like to thank all of the domestic service providers who generously gave up their time to participate in interviews for this project. We are grateful and in awe of the work you do to support victims and survivors.

Table of Acronyms

CCB – Coercive or Controlling Behaviour
CJCS – Criminal Justice and Courts Act 2015
CJS – Criminal Justice System
CSEW – Crime Survey for England and Wales
CMA – Computer Misuse Act 1990
DASH – Domestic Abuse, Stalking and Harassment and Honour-Based Violence
DDoS – Distributed Denial-of-Service Attack
ICT – Information Communication Technology
IPS - Intimate Partner Surveillance
IPV – Intimate partner violence
MCA – Malicious Communications Act 1988
NPCC – National Police Chiefs Council
ONS – Office of National Statistics
PHA – Protection from Harassment Act 1997
SPA – Stalking Protection Act 2019
TFDA – Technology-Facilitated Domestic Abuse

Table of Contents

<i>Acknowledgements</i>	2
<i>Table of Acronyms</i>	2
<i>Executive Summary</i>	5
Introduction	5
Methods and Research Sample	6
Types of Technology-Facilitated Domestic Abuse	6
Tools of Technology-Facilitated Domestic Abuse	9
Scale of Technology-Facilitated Domestic Abuse	11
Spaces of Technology-Facilitated Domestic Abuse	12
Drivers and Motivations of Technology-Facilitated Domestic Abuse	12
Perpetrator Profiles	14
Hidden Groups	16
Harms of Technology-Facilitated Domestic Abuse	16
Support for Victims of Technology-Facilitated Domestic Abuse	17
Criminal Justice System Responses to Technology-Facilitated Domestic Abuse	18
Conclusions and Recommendations	19
<i>Introduction</i>	24
<i>Domestic Abuse</i>	26
The Scale of Domestic Abuse	27
Domestic Abuse Risk Factors	31
<i>Computer Misuse and Technology-Facilitated Domestic Abuse</i>	34
<i>Methods</i>	36
Media Analysis	36
Technology Review	38
Interviews with Domestic Abuse Service Providers	42
<i>Types of Technology-Facilitated Domestic Abuse</i>	44
Unauthorised access	45
Means of unauthorised access	47
Fake Accounts	55
Online Harassment	57
Stalking and Installing Trackers	57
Image-based Sexual Abuse	59
<i>Tools of Technology-Facilitated Domestic Abuse</i>	62
Physical covert devices	62
GPS trackers	62
Covert Cameras	66
Covert Microphones	67

Apps	73
Parental monitoring tools	79
Keyloggers	80
Dating sites	81
Use of drones	84
Excessive and abusive mass communication	84
<i>Scale of Technology-Facilitated Domestic Abuse</i>	86
<i>Spaces of Technology-Facilitated Domestic Abuse</i>	88
<i>Drivers and Motivations of Technology-Facilitated Domestic Abuse</i>	90
Purpose of Unauthorised Access	93
Involvement of Children and Custody Proceedings	94
<i>Perpetrator Profiles</i>	97
<i>Hidden Groups</i>	104
<i>Harms of Technology-Facilitated Domestic Abuse</i>	107
Personal data most commonly targeted for stalking	108
<i>Support for Victims of Technology-Facilitated Domestic Abuse</i>	110
<i>Criminal Justice System Responses to Technology-Facilitated Domestic Abuse</i>	112
<i>Conclusions and Recommendations</i>	115
<i>References</i>	120
<i>Appendices</i>	123
Appendix 1 Media cases	123
Appendix 2 Online Retailers in the UK	126
Appendix 3 Guidance for Victims of TFDA	127

Executive Summary

Introduction

In February 2021 an interdisciplinary team of researchers at the University of Portsmouth and the University of Kent were commissioned by the Home Office to research domestic abuse facilitated through unauthorised access and other Computer Misuse Act (1990) (CMA) and related technological offences, as part of the Domestic Abuse Perpetrators Research Fund¹.

Digital technologies, including the internet, have enabled people to socialise and exchange personal information online, often under the protection of anonymity and with little oversight or accountability. This has enabled the facilitation of different forms of online harms and computer misuse against individuals. With the increased use and development of technology, methods of perpetrating domestic abuse are progressively incorporating computer misuse offences and digital tools, escalating opportunities for perpetrators to monitor, threaten and humiliate their victims. This has been referred to as intimate partner surveillance (IPS) and technology-facilitated domestic abuse (TFDA), and evidence shows that this phenomenon is on the increase (POST, 2020; Refuge, 2019). Many victims of domestic abuse also experience TFDA in some form and often there will be digital evidence of abusive behaviours in domestic abuse cases. Domestic abuse is an abhorrent crime with far reaching impacts upon its victims. In the year ending March 2020 in England and Wales, 2.3 million adults aged 16-74 years (1.6 million women, 757,000 men) were subjected to domestic abuse (ONS, 2020) and more than one in ten of all offences recorded by the police are domestic abuse related (ONS, 2020). The Domestic Abuse Act 2021 received Royal Assent on 29.04.21 and sets out for the first time in England and Wales a statutory definition of domestic abuse. A number of amendments to the Bill during its passage through Parliament have created a number of new offences, two of which are most relevant to this research:

1. extending the controlling or coercive behaviour offence to cover post-separation abuse
2. extending the 'revenge porn' (*sic*) offence to cover the threat to disclose intimate images with the intention to cause distress

The research had the following broad aims:

- To examine the nature of domestic abuse facilitated through unauthorised access and other CMA and related technological offences
- To assess how the link between CMA and domestic abuse can be formally evaluated

The research had the following objectives:

- Identify the types of computer misuse related crimes used by domestic abuse perpetrators
- Identify what forms of technology are being used by perpetrators of domestic abuse
- Identify how technology is being used by perpetrators of domestic abuse
- Gauge the extent of different types of technology-facilitated domestic abuse
- Identify online spaces contributing to technology-facilitated domestic abuse
- Explore the factors that lead to technology-facilitated domestic abuse perpetration
- Identify profiles of technology-facilitated domestic abuse perpetrators
- Identify under researched groups (such as LGBTQI+ and BME) experiences of technology-facilitated domestic abuse, as either perpetrators or victims
- Examine the impacts of technology-facilitated domestic abuse upon victims and the levels of support available

¹ <https://bidstats.uk/tenders/2020/W46/738853319>

The term victim is predominantly used throughout the report; however, the problematic use of terminology is acknowledged. Ordinarily the term victim would be applied to refer to those currently in an abusive relationship, with survivor used for those no longer in an abusive relationship, but highlights the person's agency in dealing with their experience (Radford et al., 2012). It is also recognised, however, that this demarcation is not necessarily always clear - much depends on how individuals view themselves. Within feminist discourse there has been debate about the appropriateness of the terms victim or survivor, however, the former is the common term employed within the criminal justice system (Radford et al., 2012). Furthermore, the terms abuser/perpetrator and offender are used interchangeably throughout the report.

Methods and Research Sample

To conduct the research a literature review was completed, and primary research including an analysis of 146 media cases, an online technology review comprising 1654 technology tools extracted from 330 unique websites, and 21 semi-structured interviews with domestic abuse service providers. The data collection took place from February to May 2021.

It is important to note some caveats relating to the methods used. Although the definition of domestic abuse by the Home Office in England and Wales includes familial relationships, this research uncovered few details about family abuses and so the main focus of this report is on adult intimate relationships.

In regard to the media analysis, it is important to note that newspapers will focus on those stories considered as most 'newsworthy' and only those stories considered as sensational and of a particular interest to the public will be reported, therefore, given the extent of domestic abuse, the majority of cases will not be reported. This will impact on public perceptions of the extent of domestic abuse and the types of abuse that occur, as reports will vary in the level of information provided and there is a risk that the reporting may include inaccuracies.

While the technology review sought to be as grounded as possible, this work is constrained by the fact that we did not access all websites emerging from search queries. This was primarily because of the limited project timeline. That being said, this work does follow a normal pattern to search for items online, i.e., most individuals only look at the first 2-3 pages. This work also does not consider the dark web and any tools/technologies/recommendations that may be found there.

The semi-structured interviews are not representative of professional knowledge and experience across all of England and Wales, as the majority of interviews were conducted with service providers from the South East of England and the Midlands, owing to the location of the researchers and pre-existing contacts. Due to the pandemic, all interviews were conducted virtually, and the audio recordings transcribed, aside from two, which were conducted via email. The team were unable to procure any interviews with organisations specifically supporting the LGBTQI+ community or BAME groups due to lack of staff availability in these agencies during this particularly busy and challenging time; this issue was compounded further by the short timeframe of the project. It is acknowledged that persons from these marginalised groups are more likely to seek support from smaller specialist organisations rather than the larger, better known victim support services, therefore, whilst insight was obtained into these communities, greater understanding from dedicated services is lacking.

Types of Technology-Facilitated Domestic Abuse

Computer misuse offences, especially unauthorised access, are being conducted as part of a wider continuum of domestic abuse, but these only account for part of the picture. Domestic abuse

perpetrators are engaging in a broad range of abusive behaviours involving the use of technology, some of which encompass and combine offences within existing legislation, such as the Malicious Communications Act (MCA) 1988, the Computer Misuse Act (CMA) 1990, the Protection from Harassment Act (PHA) 1997, the Fraud Act 2006, the Protection of Freedoms Act 2012, the Criminal Justice and Courts Act (CJCA) 2015, and the Stalking Protection Act (SPA) 2019, but many harmful behaviours and activities conducted as part of a wider pattern of domestic abuse, including coercive or controlling behaviour, are not currently acknowledged as criminal offences, leaving victims exposed and vulnerable to ongoing patterns of abuse with no apparent recourse to criminal justice. However, the additions made to the Domestic Abuse Act 2021 may now assist in criminalising some of these abusive behaviours.

Unauthorised access

Emails and social media accounts (notably Facebook, Instagram and WhatsApp) are predominantly the targets of unauthorised access. Given that email accounts are now the gateway to all aspects of people's lives and social media has become one of the most ubiquitous means for people to communicate, this is unsurprising. Bank accounts are also being accessed, with perpetrators obstructing accounts or using payment details without authorisation, but such cases are not routinely being reported in the media.

Often joint accounts are held, meaning there would be no offence. Perpetrators are also able to access their victims' accounts via a range of means. Many partners share devices using their login details (which may also be saved) or tell each other their passwords, whilst some perpetrators may be able to guess passwords by already having an intimate knowledge of their partner. Some abusers may know where their partner keeps a list of passwords and some people may have to disclose their passwords to an abusive partner under coercion and duress:

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)

Theft is also a means of procuring unauthorised access. In one case a disgruntled ex-boyfriend turned up at his ex-girlfriend's workplace to meet her and stole her phone, enabling him to access it and the accounts on it, and send an explicit video to friends and family (Echo, 2020). In another case, the former partner broke into the house threatening the woman and left with her device (Belfast Live, 2021). Even the advent of biometric means to access devices has not deterred some. In one case the partner would use his partner's thumb while asleep to open her phone so he could access her accounts (MailOnline, 2018a). There were also a couple of cases where the perpetrators had hired experts to hack accounts.

Control, coercion, threats and actual violence are also used to secure access. In some media cases the victim was, or had been, involved with a coercive and controlling partner who pursued them through a variety of methods, ranging from psychological threats of violence through to actual violence. In some cases, when asked, victims simply handed over devices with accounts open or gave them the passwords or PINs to enable them to access. An example typical of many, was a man convicted of coercive control in Kent who through demands and violence took over his partner's life including her Facebook and bank accounts. Refusals or attempts to leave were met with verbal threats or actual violence (Kent Online, 2020) and could escalate the risk of harm.

Spyware

Perpetrators are also using spyware in order to gain the knowledge required to access their partners' or ex-partners' accounts, but also to monitor their movements. It is often being deployed in relatively simple ways. For example, devices being gifted (especially to children) which are preloaded with spyware or perpetrators having access to devices which they are able to place spyware on.

Fake accounts

The use of fake accounts is a significant method used in abusive relationships. The fake accounts can be created based on a fictitious person, real persons who are known to the victim (e.g., friends), or be set up to impersonate the victim themselves. Many perpetrators do not have the skills or knowledge to hack victim's 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 have been set up on dating sites, Interviewee 7 highlighted that the victim is not only dealing with the false representations of herself, she is also having to contend with other men trying to contact her on WhatsApp or text, because her mobile phone number has been publicly divulged. Fake profiles are also used to try and re-engage with partners after separation has occurred, whilst during ongoing relationships, perpetrators use them to test whether their partner will cheat on them or to prove that their partner was cheating all along.

Online harassment

Perpetrators are also engaging in behaviours that could contravene the MCA, 1988, such as posting harassing and derogatory content about their victim on social media. Often this is not undertaken using the perpetrator's own accounts, rather anonymous profiles have been created in order to perpetuate the abuse. 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)

Stalking and installing trackers

Many of the methods undertaken by domestic abuse perpetrators involve stalking and controlling their victims, with technology providing easy and accessible means to further this form of abuse. Location apps that serve a legitimate purpose, such as *Find my phone*, are being utilised to monitor activities for duplicitous reasons, often without the knowledge of victims. Stalkers also draw on geo-location on social media. Victims can also be manipulated into having trackers put on their devices for 'safety' reasons.

I know I've got one client at the moment who 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)

Combining activities that may not by themselves be illegal, but when acknowledging the wider context could come within both the CMA, 1990 and the MCA, 1988, as well as the PHA 1997 or SPA

2019 (if a relationship has ended), should enable the police to act when perpetrators subject their victims to a barrage of communication, including texts, emails, social media messages and posts. They might also have hacked into accounts, spyware or physical trackers to be able to follow their victim's every movement. This has enabled some abusers to pursue their victim physically, but also maintain an omni-present control over everything their victim does without committing a criminal act. As highlighted by Interviewee 11.

Even if you switch your location settings off, there are certain apps that will still run on your location settings. We did not think about that one and thank goodness someone raised it... he used her Just Eat account to find her address, because she didn't think to change that password. They can log in and there are your address details all set out nicely for them.

But imagine the impact on a victim when they get a message from the perpetrator saying, oh, did you enjoy your pizza last night, that extra topping? That's going to scare the living daylights out of them...

These examples show how easy it is for perpetrators to gain information through the use of everyday apps if the passwords are not changed, and how this information can be used to instil fear and retain some measure of control. Victims are left feeling helpless, as the perpetrator's presence continues to dominate their lives:

They manipulate and gaslight and control them because are you going to phone the police and say my abusive ex-husband phoned me to say did you enjoy the pizza? No. What are the police going to do about that? (Interviewee 11)

Under the new Domestic Abuse Act 2021, extending the coercive or controlling offence to cover post-separation abuse should assist in a range of abusive behaviours, including the one above, now being recognised as part of a pattern of abuse and responded to as a criminal act.

Image-based sexual abuse

Domestic abuse perpetrators are also engaging in so-called revenge pornography, or what is more accurately termed image-based sexual abuse (McGlynn & Rackley, 2016). This can involve situations where perpetrators threaten to release intimate pictures or videos in order to retain control over their victim. Whilst this was not an offence under the CJA 2015, the Domestic Abuse Act 2021 has extended the offence of image-based sexual abuse to include the threat to disclose intimate images with the intention to cause distress. In other instances, perpetrators, in setting up fake social media profiles of their victims, have used these to disseminate indecent images of their victims. Other means of distributing these materials have been to send them directly to friends, family, and employers, as well as publishing them publicly online. These additional forms of abuse could be covered by the amendments made to the Domestic Abuse Act 2021, but how prosecutors decide to use this new legislation will need to be monitored.

Tools of Technology-Facilitated Domestic Abuse

Our findings revealed technologies targeting the physical identity of individuals (voice, image, location); technologies that target digital data (Whatsapp messages, app usage, existence on dating sites etc.); and finally, the ones which target both the physical and digital identities of individuals. Identical devices, applications and behaviours can be both used to abuse and protect. Everyday mainstream devices and services are most commonly used to perpetrate abuse. Context is significant

in establishing TFDA in personal, intimate and familial contexts, distinct from healthy relationships and interactions.

Similar to stalkerware, devices that are used to monitor physical identity of individuals such as location, image or sound are also accessible via websites. Covert cameras and microphones or GPS trackers can even be obtained on popular online retailers such as Ebay and Amazon. The wide range of forms that these devices can be hidden in is also concerning, especially when we consider the ones in toy shapes used by children. These devices enable perpetrators to access victims via their children and the gifts given to children become an issue of conflict, as they will involve devices children want access to, including Playstations, Xboxes and iPads . It is important to note here that the variety of options is much higher in local retailers in the UK compared to global ones.

Among the digital data targeted by the technology misuse, WhatsApp messages were prolific across the interviews and the recommendations in the technology review. This may not be surprising given the fact that this product is widely used all over the world. WhatsApp Web is frequently recommended as a spying tool and is quite easy to exploit for individuals living in the same domestic space. Similar risks that arise due to the nature of close relationships is the possibility of guessing answers to security questions that are asked while resetting passwords. This approach is frequently recommended on sites thus highlighting the openness of such attacks and low initial costs (time or resources).

Perpetrators are adept at adjusting to new technology and exploiting legitimate tools. The Internet of Things (IOT) and smart devices such as Alexa (a voice assistant), Hive (a smart heating system) and Ring doorbell (a smart video doorbell) are being used within domestic abuse contexts. For example, if there is a joint account for Alexa, then if this is not removed after a victim has ended the relationship (which is now acknowledged as a time of escalated risk of serious harm and homicide), the perpetrator will be able to know everything that is being delivered to the property and even the details of a new address. If a victim is planning to leave, then the perpetrator can work out the behaviour of the victim. With Hive, the perpetrator is able to emotionally abuse, gaslight and inconvenience their victim by changing the heating in the house, whilst the Ring app could be accessed by perpetrators to see who is visiting and when the victim enters and leaves the home. The misuse is not only about accessing the information of others, but also taking actions with the aim of abusing and controlling them. Locking people at home, turning on the television or music, setting the thermostat on to very high degrees, controlling lights and alarm systems or ringing the doorbells are examples experienced by victims.

Guidance is provided online as to how to use technological tools for abuse, discoverable via simple search queries about how to spy on partners, for example. Searching through recordings is the main advice which allows a perpetrator to learn the instructions, voices and the time of those instructions. Timing also would enable them to discover when the individual or others who interacted with the voice assistant were present in the home.

“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?”²

The options provided to perpetrators on the web enable individuals to find, source and apply such technologies to harm others in their domestic environment. In particular, stalkerware apps are

² <https://www.diemlegal.co.uk/amazon-alexa-echo-smart-tools-uncover-partners-infidelity/>, April 2021

marketed to information seekers who want to abuse or control their victims via technology. These products are generally advertised on their official webpages as parental tools or employee trackers. Such misleading information is even present for mSpy which appears to be the most popular stalkerware on the Web. The ambiguities around the differentiation of parental tools and stalkerware can also be understood from Google's search predictions. Google returns names of popular stalkerware as search predictions when queries such as "Best stalkerware apps" are executed. This ambiguity is concerning since legitimate statements have the potential to normalise use of those apps and encourage people to install them giving motivations such as protecting their families. Abuse, however, involves common everyday technologies, not just purpose-built spyware. It is known in the literature that dual-use apps, which have a legitimate purpose, such as tracking children or stolen devices, can also be easily repurposed to abuse victims (Chatterjee et al., 2018).

Scale of Technology-Facilitated Domestic Abuse

Technology is featuring in the majority of domestic abuse cases dealt with by service providers, in particular activities that fall within the CMA, 1990. Interview participants have stated that in nearly every case they see, there is some form of a hacked account, or attempts to hack into accounts.

I think what we see most commonly, in absolutely every case, there is some form of hacked account. There isn't any case that's come through to us in the thousands of cases we've had, that there hasn't been a hacked account (Interviewee 1)

Additionally, harassment using technology, involving abusive comments, fake profiles and image-based sexual abuse are common.

Particularly in stalking cases, it's very rare to have cases, as well, like, ex-partner cases, where there isn't some kind of, like, online element to it, digital element to it. Whether that's creating the fake profiles online, threatening to post images, putting software on phone, listening devices, that kind of stuff (Interviewee 7)

The police are also expecting technology to feature in some respect when they respond to domestic abuse cases.

I think most officers are aware that it's likely that any domestic will involve technology to some extent. I mean, you know there's always some sort of argument that's happened over a text message, or social media, in addition to whatever arguments may have happened face to face. You know, it's that prevalent, you know, that I would say the vast majority of domestics are going to involve technology to some extent, without a doubt (Interviewee 15)

TFDA is likely to be part of an ongoing pattern of coercive and controlling behaviour throughout such relationships, where access to victims' accounts is expected along with monitoring of their movements, as outlined in the earlier discussion on unauthorised access. The indication is that where there is coercion and control present in a relationship, technology will also feature as a means to conduct that abuse too. This was also confirmed by the experiences of Crown Prosecution Service prosecutors:

There is no specific data kept on this [TFDA] as we only flag domestic abuse, coercive and controlling behaviour and stalking cases. But in my experience every domestic abuse case involves technology facilitation.... and some are becoming more sophisticated. (Interviewee 21)

Spaces of Technology-Facilitated Domestic Abuse

In addition to apps used to spy on individuals, our analysis revealed some websites that are also used to monitor individuals with relatively more limited functionalities. GPS is the main information proposed to be provided by those services, which mostly require the phone number of the targeted person to be given to the system.

Specific online spaces enabling TFDA were mentioned during the interviews, these are:

- Social media platforms - Facebook, Whatsapp, Instagram, Snapchat, Twitter
- Netflix
- Spotify
- Dating sites - Tinder, Grinder
- Anonymous messages sent through Pandora Jewellery

Drivers and Motivations of Technology-Facilitated Domestic Abuse

Technology as a facilitator of domestic abuse, is generally acknowledged to occur throughout a coercive and controlling relationship. In many cases a perpetrator will have demanded access to their partner's accounts or are already infiltrating them, without their partner knowing. They might have also installed spyware or hidden cameras to constantly monitor their partner's activities. The technological abuse, however, often escalates when a relationship ends, or the perpetrator becomes aware that the victim is planning to leave. In these situations, the surveillance involving these tools increases as the perpetrator attempts to uncover information that will win them back or prevent them from leaving.

And so while they're in a relationship, it's an issue, when they're leaving it's an issue, because they suspect something's happening, they're really on it and they want to check everything to see someone's movements. And when they're left, it really ups the ante then, because then they're hacking into absolutely everything (Interviewee 1)

It is here that perpetrators might employ more severe forms of technological abuses such as the dissemination or threats to disseminate intimate images of their partner, and/or harassment and stalking, particularly to discover where they have gone or are planning to go. These are all indicators of increasing high risk of harm to the victim.

The research uncovered the following motivations, some of which overlap, for engaging in technological abuse:

Control: a prolific motivation. Technology provides a means to control partners, from controlling who they communicate with and what they do (because of the surveillance they know they are under). This could involve creating fake situations to make the partner vulnerable, so they need the offender even more.

Revenge: another common motivation. Disgruntled offenders, especially those abusers angered by the ending of a relationship (due to their loss of control over the victim), or those irritated by the perceived conduct of their partner, pursue behaviours to punish them, which often involves technology, such as disclosing private images, seeking to discredit, degrade or humiliate them, to name just a few.

Surveillance: underpinning some of the other motivations is the pursuit of surveillance to find out what the other person is up to, what they are doing, who they meet, talk to, what they say etc. There is also possibly a sexual, voyeuristic element to this too.

Attempted reconciliation: here, perpetrators do not accept the end of the relationship and use technology as a means to communicate when their former partner has blocked them or if there are legal prohibitions, such as court orders.

Secure evidence of infidelity: fear of infidelity in the other partner, and technology along with other means is pursued to find evidence of this.

Secure evidence for divorce/ child custody proceedings: technology is used to try and secure evidence for an advantage in divorce or child custody proceedings.

Financial gain: technology is used to secure access to the finances of the partner.

Curiosity: the partner is interested to find out what the other is doing, thinking, engaged in.

Perverf justice: where a partner is seeking to implicate the other, by using technology to create evidence to support that, such as creating a false account with abuse coming from it that implicates another.

Sexual: where technology is utilised to help secure sexual gratification.

From the above motivations it was possible to develop a typology of abusers. They include **the curious, the investigator, the deviant, the controller and the avenger** (see Table 1).

Table 1. A typology of abusers

	The curious	The investigator	The deviant	The controller	The avenger
Aim	Just want to know what partner or former partner is doing	Want to secure information for a purpose such as to secure evidence of infidelity or other information which might aid a divorce case	Want to observe, secure data or use person for sexual gratification	Want to control partner and prepared to use means to aid compliance.	Want to cause damage to current or former partner
Technique/ Action/ Method	Could involve searching clothes, looking at bank statements through to technological based hacking, tracking, covert devices etc.	Could involve following a person, asking people, hiring an investigator through to technological based hacking, tracking, covert devices etc.	Could involve watching a person from secret location through to technology based covert devices, use of private images etc.	Technology such as hacking, covert devices, trackers etc is used to control a person (which may be alongside more traditional psychological, physical and sexual forms of abuse).	Desire for revenge could be through violence, sexual assault to murder, but through technology could be via disclosing private images, harassment. Technology could be used to facilitate the traditional, such as to locate a

					person so they can be attacked
--	--	--	--	--	--------------------------------

It is during the break-down of a relationship that another key driver for technological abuse develops - child contact/custody cases. Children are increasingly being involved in technology-facilitated domestic abuse contexts, especially as a means for perpetrators to further control in post-separation shared parental situations. Children are used to abuse the other parent, their devices such as phones, tablets and games consoles, are exploited by perpetrators to monitor and maintain control over victims. Post-separation contact around parenting enables abuse. In some instances, technology-facilitated contact is used in lieu of physical meetings to decrease risk, yet instead it allows persistent harm and can escalate risk.

In some instances, perpetrators have fabricated communication from their ex-partner after hacking into their accounts, so that it appears as if the ex-partner is the abusive party. In other cases, perpetrators have accessed their ex-partners accounts and printed off information to use in court against them. Children’s devices have had listening/tracking apps installed on them and instructed to always have them on and keep them close, so that perpetrators are able to know everything that is happening at their ex-partner’s new house. Children’s devices are also used as a conduit to send abuse to the ex-partner as this quotation demonstrates:

There’s a lot of manipulation through the kids, I mean, I’ve seen people send abusive messages to the children that’s for their parent, so there’ll be some really quite severe allegations, you know, like paedophilic allegations, sexual assault allegations that are being sent to the child, but that’s for their parent (Interviewee 2)

The ambiguity and difficulty of differentiating between dual-use and spyware apps enables perpetrators to exploit technology designed to help parents monitor their children’s devices and online activity, to stalk and abuse their partners/ex-partners. Some apps, however, are blatant about the potential for abuse in their advertising. Statements such as, “A complete parental monitoring software, MobiPast, helps parents carefully keep vigilance on their children’s smartphone activities but also can be used to catch a cheating spouse.” confirm the role of dual apps in TFDA reported in the literature. Similarly, iKeyMonitor requires jailbreaking a device even though it is given as a dual use app for parents.³ KidsGuardPro is particularly interesting since it pretends to be a legitimate app on the main page of its website, however, it includes explanations about using the app to gather evidence from cheating spouses on other webpages. It is also given as a spyware on the blogs that list the best spyware to use.⁴

Perpetrator Profiles

The data indicates that there is no specific profile for perpetrators of technology-facilitated domestic abuse. Any person already being abusive to or having the potential to be abusive to their partner or family member, is also likely to use technology to further the mistreatment. In addition, technical skills do not appear to be necessary in order to perpetuate most forms of technological abuse, particularly as there is a wealth of information and tools readily accessible and available online for would-be TFDA perpetrators. All echelons of society are involved in using technology for abuse in

³ <https://ikeymonitor.com/>, April 2021

⁴ <https://www.clevguard.com/monitor/how-to-catch-a-cheating-husband-on-whatsapp/>, May 2021

relationships. Some indicative distinctions, however, have been made in the forms of abuse and the educational level and professional status of perpetrators. Perpetrators who are less educated (non-graduates) and are unemployed or have minimum wage jobs appear to engage in more overt technological abuse - the abusive commentary on social media and/or the accessing of accounts to disparage their partners/ex-partners (this applies to both male and female perpetrators).

Perpetrators who have higher levels of education (graduates and postgraduates) and occupy professional roles, seem to conduct more covert means of technological abuse, utilising spyware and physical tracking devices to monitor and control their partners/ex-partners. This could also be due to a disparity in socio-economic status and the means to afford and access such digital tools.

Social media abuse is less academic, more overt. The more educated the more insidious...[they] have to the tools to manipulate IT (Interviewee 6)

My view is that the younger generation are all digitally based and so they use tech to facilitate domestic abuse in a basic everyday way and increasingly more sophisticated way. I often find that older perpetrators who are educated are very sophisticated in the way they use tech to facilitate domestic abuse (Interviewee 21)

Perpetrators who work in IT, such as software developers, have been referred to, as well as those who have a personal interest in technology, suggesting that these persons could be more inclined to use technology within the broader pattern of their abuse.

I also find that the more technical software and things like hacking of the Wi-Fi and things like that, it tends to be where the perpetrator has a job in technology. And knows how to evade everything, you know, they can cover their tracks, they know where to get things from (Interviewee 7)

Technology-facilitated domestic abuse, however, does not require technical proficiency. At the base level are acts that any ICT user could do. Setting up a fake account, guessing a password or physically intimidating someone to provide access, all require little skill. Some acts require more skills such as further research or basic training. The use of some apps that enable spyware fit this category. Many of the tools used by perpetrators are everyday technologies, which are readily available, accessible and familiar. Apps are affordable. The majority of them do not need jailbreaking or rooting, which makes them usable for people with average IT skills. Installing covert devices may involve some basic research to do so effectively, although if it is just placing a mobile phone covertly this would also be low skill. Tracking devices/apps similarly fit this same category and could be both depending upon the device or app. Anyone who has flown a drone knows it is not as simple as one might think, and to use one to monitor/harass a person would require some additional skills. Where extensive research and training would be required, such as hacking a person's account via social engineering, requires much more skill.

Age was noted as potentially impacting upon the types of apps or software used in TFDA perpetration, with younger persons (30's and under) engaging in authorised access to accounts and the creation of fake profiles, whilst older people (40+) employed physical covert devices. This could be linked with the educational and professional status of perpetrators as above, as well as the socio-economic means. Social media use is ordinarily more prevalent with younger people and part of their daily activities, which are then drawn upon to perpetuate abuses.

In cases where the victim and perpetrator are younger, I would say it's a lot more hacking Facebook, making the fake profiles, using things such as Snapchat or Strava. In the cases where the perpetrators and victims are a little bit older, I've actually noticed it's more the listening devices and cameras. I find definitely in the under 30s it's more using social media to get what they want (Interviewee 7)

Hidden Groups

Domestic abuse is generally considered a gendered phenomenon, with women perceived to be the victims and men the perpetrators, due primarily to the overwhelming statistical evidence supporting this (ONS, 2020). As a consequence, other victims and indeed perpetrators are often overlooked. This has led to a gap in knowledge about the domestic abuse experiences of hidden groups, such as men as victims, women as perpetrators, persons within the LGBTQI+ community, BME individuals, and disabled victims.

Due to the nature of the majority of organisations which took part in the research, interview participants have primarily spoken about heterosexual relationships, whereby the male is the perpetrator, and the female is the victim. However, some cases have been discussed which involve male victims, same sex couples - both male and male, and female and female, as well as child to parent abuse. Further, due to the type of support provided by one particular charity interviewed, there is also insight into females as perpetrators and males as victims. Gendered roles and stereotypes remain significant in these domestic abuse contexts.

According to this charity, men have reported being victims of image-based sexual abuse, as they have had images taken of them without their consent, for example, whilst asleep or under the influence of drugs or alcohol. Sexual acts have also been committed upon men when they have not been in a conscious state, which have been recorded or photographed, and those images then shared with other people.

Other organisations, however, that support adult victims of any gender, indicate that where the perpetrator is female and the victim is male, women use lower levels of IT, and usually favour using verbal abuse towards their victim via social media and attempt to access their accounts to monitor what they are doing.

Although heterosexual and LGBTQI+ people may experience similar patterns of domestic abuse, national UK LGBTQI+ anti-violence charity Galop⁵ highlights the specific issues unique to the experiences of LGBTQI+ people, such as the threat of disclosure of sexual orientation and gender identity to family, friends, or work colleagues. In some same-sex cases, discussed by Interviewee 1 involving female partners, there was active recruitment of others to join in with the abuse and the selling of data. The perpetrators allowed others online - access to their victim's accounts and encouraged them to harass the victims. This suggests that having a public aspect to the abuse was important to the perpetrators in these situations.

In terms of ethnicity, cultural differences and a lack of legislation recognising coercive control as domestic abuse in their home countries, were suggested as factors influencing the abuse. Perpetrators claim not to realise that they are engaging in abusive behaviours and victims may struggle to recognise the behaviours occurring within a domestic abuse context, despite experiencing harms as a result.

⁵ <http://www.galop.org.uk/wp-content/uploads/DV-A-LGBT.pdf>

Harms of Technology-Facilitated Domestic Abuse

Technology-facilitated domestic abuse has serious impacts upon victims, including psychologically, emotionally, physically and financially. Perpetrators online and their motivations are not different from those offline. Victims have always experienced both contact (physical violence) and non-contact (coercive and controlling) abuses, and physical forms of harassment and stalking. Digital technologies merely provide new tools and opportunities to extend the repertoire of non-contact forms of harm.

Comparisons are made with sexual assault to the intrusive nature of these abuses, which are facilitated as part of a broader pattern of coercive and controlling behaviour.

I'd say that when we've spoken to women, they say it's as intrusive as being assaulted, sexually assaulted. And quite often, there's visual cameras in the property. They suspect there is, they're trying to find them. And they know they're being watched; their every movement is being watched. They can't...there's no safe way to speak to somebody, communicate, get help, you're never left alone. Imagine what that does to somebody's mental health. It really, really makes somebody..., it helps that facilitation of gas lighting, making somebody think they're going crazy (Interviewee 1)

The feeling of constantly being monitored, not having secure means to communicate with others, and questioning one's sanity through being gaslighted, affects the mental and physical health of victims. Technology is utilised to further control victims, leverage structural inequality, and remove what little autonomy and independence they have from the perpetrator. Furthermore, it is not only the direct victim that is harmed by TFDA, children who are involved in the abuse are also damaged by its impacts, despite its non-physical nature.

However, there is some evidence to suggest that some victims use the technology to manage the perpetrator:

We've had one lady who said that she left her social media on, because she knew her partner was following her on it and she said she'd rather he was looking at that, than hanging around in the street. So, that was her way of her managing his behaviour so that it didn't really affect her, she wasn't bothered that he was looking at it (Interviewee 4)

There is also evidence that victims use the technology to appease perpetrators to avoid the abuse escalating. Advice from the police to victims in the past has been for victims to change their number, block the perpetrator or come off social media completely. Whilst this acts to penalise the victim by isolating them from friends and family (often a motivation of the abuser) it can also act as a trigger:

You have to be really careful. You can't even really tell anyone to block anyone 'cause that could escalate things as well. It is literally a case-by-case basis. Some victims know.. I'm keeping him sort of subdued by just taking his behaviours, but if I react then maybe he'll react (Interviewee 4)

The indication thus far, is that the severity of the harms caused through technology-facilitated domestic abuse are minimised by the authorities when compared with physical violence, suggesting that greater awareness and understanding about coercive control in general is still required, despite the introduction of national training programmes aimed specifically at criminal justice professionals (Brennan, Muhill, Tagliaferri and Tapley, 2021).

Support for Victims of Technology-Facilitated Domestic Abuse

Some solutions for TFDA are overly simplistic and/or have perpetuated victim blaming connotations, for example, expecting victims to change their behaviour by changing their contact details and refraining from using technology. Douglas et al. (2019) state that a 'technology detox' or disconnect is unfair because it is the abuser who has misused technology rather than the victim who has been abused, and yet they pay the price. It is also impractical because increasingly even routine services and activities require a connection to technology and is potentially unhealthy because it increases isolation and may obstruct the victim's ability to engage in work, education and social life (Douglas et al., 2019). As such, by refraining from the use of technology, it assists the abuser in achieving their aims, as victims can then become isolated from family, friends, and social and professional networks.

One of the first steps in mitigating TFDA is recognising when and how it is occurring. Victims are often disbelieved or not taken seriously when they have suspicions that their partner or ex-partner is engaging in TFDA against them. They are aware that their abuser is privy to information and knowledge about them that they ordinarily should not have access to, and so victims have concerns that their accounts have been breached and they are being spied on.

It is recognised that a one-size-fits all approach to support victims is not feasible in domestic abuse contexts. The circumstances of each case and the individuals involved need to be taken into consideration. There is, nevertheless, general guidance that can be offered to victims who are experiencing TFDA, which could be implemented if they are able, and it is safe to do so. In providing any advice, service providers have to be careful about alerting the perpetrator and putting the victim at risk of increased harm. For example, the removal of spyware or tracking devices could escalate a perpetrator's behaviour, as they would be aware that their victim knows they have been monitoring them, and the perpetrator no longer has that control over the victim. In situations where victims are planning to leave their abuser, it is pertinent to consider all the protections necessary and be ready to implement them immediately upon ending the relationship.

Although service providers are aware of the significant role that technology is playing within the facilitation of domestic abuse, and are attempting to support victims appropriately, there is still a great deal of knowledge and training required to fully appreciate how technology is changing the nature of domestic abuse.

Right now, no, a lot of our services tend to be very much in the physical space or tend to deal with domestic violence as a physical crime, and I'd say that is where the public sector hasn't really kept pace. We know that domestic violence takes place online as well, like cyber bullying, but our service provisions tend to be very much shelters, workers, keyworkers, support officers, social workers who deal with the physical act and taking people out of a situation. But when you talk about a phone and other digital devices, I don't think we're there yet. I think it's just beginning to change the landscape in terms of what we consider to be domestic abuse. (Interviewee 19)

Criminal Justice System Responses to Technology-Facilitated Domestic Abuse

The Computer Misuse Act offences are rarely used for prosecution. Only 4 cases were found in the sample of media cases in England and Wales and 55 cases in the 108 involved unauthorised access. Clearly prosecutors prefer to use the stalking/harassment legislation and the controlling or coercive behaviour offences.

Perpetrators are also able to evade criminal justice sanctions whilst engaging in TFDA. This is often due to an inability to collect the requisite evidence, as perpetrator's savviness in using technology

enables them to cover their tracks (such as using Snapchat, which automatically deletes messages; or using WhatsApp with automatic removal timers) and the abuses committed are not regarded by themselves as criminal acts. This is exacerbated further by a general lack of understanding by CJ professionals about how technology is utilised within an ongoing pattern of domestic abuse, often with initial police responders not recognising that abuse is being committed, as the actions do not in themselves constitute criminal behaviour.

The lack of applicable legislation to tackle distinct forms of TFDA is problematic. The following quote highlights the necessity for the forthcoming Online Harms legislation to consider this in the context of domestic abuse.

What I've noticed, that there is a gap in terms of provision of keeping people safe from say online harms. And I think the law is still catching up with where technology is, it's only recently in England that we've made say sharing of images by ex-partners or I guess husbands, illegal, while in Wales they had that come into force. Think I guess the judicial system, the police are somewhat behind in terms of where technology is, and law and regulations have to keep up, but for every legislative measure, technology precedes it, there's something new out there, there's a new piece of software which the law doesn't quite cater to just yet and the new crime that's committed (Interviewee 19)

Often, the issue is that coercive and controlling abuses, of which technology is part of, are treated as isolated incidents rather than part of a larger pattern of abuse. This can also mean that unless something serious occurs there is limited recourse via the CJS. In this study, interviewees advised that victims were literally told by responding police officers that nothing could be done until the perpetrator had actually committed an offence (as perceived by the officers), which in some cases would be too late to protect the victim. Where coercive and controlling behaviour is recognised and legislation can be applied, it would be prudent to combine it with computer misuse offences and ensure that criminal justice professionals receive adequate and appropriate training.

Conclusions and Recommendations

As technology becomes ever more ingrained into our everyday lives, hastened further by the Covid pandemic, which has driven many more human interactions and tasks online, technology-facilitated domestic abuse is undoubtedly a harmful behaviour that is only going to escalate and increase further the risk of harm, unless appropriate interventions in prevention and enforcement occur.

Below we set out our key conclusions arising from this research.

- Technology-facilitated domestic abuse (TFDA) very rarely occurs in isolation, it is usually part of a wider continuum of abuse, which is not separate from other coercive and controlling behaviours. Offline and online abuse is interconnected and within the context of domestic abuse, often co-occurring. Therefore, TFDA might be better understood as different tactics of patterns of perpetrator behaviour rather than distinct types of harm. However, it is necessary to highlight the specific instances and tactics of TFDA in order to ensure that policy, legislative and support responses appropriately consider these rapidly developing practices of abuse.
- Computer misuse offences, especially unauthorised access, feature within domestic abuse contexts, however, these only account for part of the issue. Domestic abuse perpetrators are engaging in a broad range of behaviours involving the use of technology – including use of spyware, creating fake accounts, online harassment, stalking and installing trackers, and

image-based sexual abuse, some of which encompass and combine offences within legislation such as the Computer Misuse Act (1990) CMA, Malicious Communications Act (MCA) 1988, the Protection from Harassment Act (PHA) 1997, the Stalking Protection Act (SPA) 2019, the Criminal Justice and Courts Act (CJCA) 2015, and the Fraud Act 2006, but also those not necessarily illegal yet are still harmful activities conducted as part of a wider pattern of coercive control.

- The problem of TFDA is, however, normalised and often considered unremarkable due to societal challenges towards privacy and the right to keep aspects of (digital) life separate. Context is therefore significant in recognising unhealthy behaviours; therefore, relationship-based understandings of domestic abuse and technology use are critical. There is a need to avoid reinforcing the limited public narrative of domestic abuse, where coercion and control are not viewed as significantly harmful as physical violence. Without discouraging healthy relationships, more awareness needs to be publicly available about abusive relationships and unhealthy behaviours, as well as education about independence and online safety.
- The information available to perpetrators on the web enables individuals to find, source and apply such technologies to harm others in their domestic environment. In particular, stalkerware apps are marketed to information seekers who want to abuse or control their victims via technology. These products are generally advertised on their official webpages as parental tools or employee trackers. This ambiguity is concerning since legitimate statements have the potential to normalise the use of these apps and encourage people to install them, providing motivations such as protecting their families.
- Devices used to monitor physical identity of individuals such as location, image or sound are also accessible via websites. Covert cameras and microphones or GPS trackers are easily obtainable from popular online retailers such as Ebay and Amazon. The wide range of forms that these devices can be hidden in is concerning, especially when the ones in toy shapes are considered. These devices enable perpetrators to access victims via their children and the gifts given to children become more of an issue. It is important to note here that the variety of options is much higher in local retailers in the UK compared to global ones.
- Within coercive and controlling relationships, the use of technology to further that abuse is likely. Perpetrators may already have manipulated access to their partner's accounts or are already accessing them or spying on them without their partner knowing. When a victim is considering leaving or has left their perpetrator, the extent of TFDA will probably increase, or where it has not already occurred, it is likely to be implemented. This is because the perpetrator is seeking to regain/gain control, or due to other motivations, which may overlap, such as revenge, surveillance, attempted reconciliation, to secure evidence of infidelity, secure evidence for divorce/child custody proceedings, financial gain, curiosity, to pervert justice, or obtain sexual gratification. From these motivations it was possible to develop a typology of abusers. They include **the curious, the investigator, the deviant, the controller and the avenger**.
- Children are increasingly being involved in technology-facilitated domestic abuse contexts, especially as a means for perpetrators to exert control in post-separation shared parental situations. Children are being used to facilitate the abuse of the other parent, their devices such as phones, tablets and games consoles, are exploited by perpetrators to monitor and maintain control over victims. It is also during the break-down of the relationship that another key driver for technological abuse develops - child contact/custody cases.
- There is no specific profile for perpetrators of technology-facilitated domestic abuse. Any person already being abusive to or having the potential to be abusive to their partner or family member, is also likely to use technology to further the mistreatment. Technology-facilitated domestic abuse does not require technical proficiency. The majority of the tools used by perpetrators are everyday technologies, readily available, accessible and

familiar. Apps are affordable. The majority of them do not need jailbreaking or rooting, which makes them usable for people with average IT skills. There are, however, indications that those with higher levels of education and/or in IT professions are conducting more covert means of technological abuse. There are also potential differences in regard to methods perpetrated by age, with younger persons (30's and under) engaging in authorised access to accounts and the creation of fake profiles, whilst older people (40+) use physical covert devices.

- An Intersectional approach appreciating the converging lived experiences, causes and realities of TFDA is necessary, particularly as the experiences of those suffering TFDA who are not cisgender heterosexual, from the UK, or able-bodied are often missing from the public discussions, rendering the invisibility of these marginalised groups.
- For many victims, there is not domestic abuse and then technology-facilitated domestic abuse; rather, in varying degrees, in different ways, and with very real impacts – digital technologies simply feature in a constellation of violations by an abusive partner or ex-partner. The harms from TFDA, therefore, are no less serious than those arising from other forms of coercive and controlling behaviours and physical violence.
- Solutions to TFDA often involve advising victims to disengage from technology, which is not only unfair to victims, but often infeasible given our increasing reliance on digital technologies. It could also heighten their risk of harm, isolating them from family, friends and professional and social networks, and reducing their ability to request and receive support. Therefore, a one-size-fits-all approach in supporting victims is not possible.
- Perpetrators who are committing computer misuse offences as part of their pattern of abusive behaviour are rarely being charged with these crimes. These offences are often being overlooked in the context of stalking and harassment or control and coercion.
- The ongoing use of technology increases the long term traumatic and psychological impacts on the victim, perpetuating feelings of being trapped and unable to escape the abuse. The use of technology to facilitate abuse should be recognised as an aggravating feature and result in an increased sentence.

Preventative Lessons

This research has identified some key findings that can be utilised to develop improved prevention strategies to tackle some of the technology-facilitated behaviours uncovered in this analysis. Many of these overlap with cyber hygiene advice that is already well publicised, although the research indicates a need for an increase in both public and CJ professional awareness and understanding.

For individuals

Change of all passwords when a relationship ends. It would seem prudent for intimate partners to change all passwords on accounts and devices when a relationship ends. Even if there is no evidence of technology-facilitated abuse, the other party might not know this would seem to be a common risk.

Avoid passwords an intimate partner might guess. If a relationship ends or in a current relationship where the partner does not want the other to have access to their accounts, it would seem prudent not to use passwords that could be guessed.

Be aware of privacy settings on your device: some settings can reveal where you are and if you do not want people to know this, these should be switched off.

Check any devices with internet connectivity given as gifts or which the partner may have access to: Any device which can be linked to the internet which is given as a gift should be checked for any

spyware trackers pre-installed (mobile phones, laptops, fitbits, etc). Cookies should be deleted, and the browser history cleaned. Some devices where it is not easy to check might be better discarded or switched off. In some cases, it might be prudent to secure an IT expert's advice to check devices, particularly as spyware apps work in stealth mode and notify the perpetrator as they are uninstalled.

Be aware of app's remote installation capabilities: Installation becomes easy once cloud credentials are known and, therefore, it is important to check for new apps appearing on devices if your cloud details are known, or you think they might have been uncovered.

Check the privacy and use of facial images and email addresses on social media accounts: These are personal identifiers that can be tracked back easily with Google's different search facilities.

Regularly sweep private residence and vehicle for trackers, covert devices. Persons who have partner's or ex partners who are a concern should regularly check where they live and their vehicle for any devices which might have been placed there for surveillance purposes.

Private images and recordings: Encrypt any files holding such images/recordings. If a relationship ends, destroy images.

Friending: Be careful to check any person seeking to 'friend' you on a social networking website.

Communication: Do not assume a person you know communicating with you is who they say they are. If suspicious, use other means to check.

For government and enforcement

Domestic Abuse Bill: Specific inclusion of the recognition of the role that technologies can play in facilitating and exacerbating domestic abuse within the Domestic Abuse Bill

Fake accounts: There would seem to be a gap in legislation relating to impersonating another person online. Given impersonation seems to be a significant aspect of this type of abuse further research should be undertaken as to whether current legal provisions are appropriate for this and reflect the significant harm that can be caused.

Covert devices and apps: Covert cameras, listening devices and vehicle trackers would seem to be used negatively in many cases. Clearly, they have uses for legitimate purposes, such as for safety, parental controls, and private investigators investigating workplace crime, for example. However, further research into controls on the advertising, sale of such items or regulation of their use should be considered, particularly via the forthcoming Online Harms Bill.

Spyware: Given that spyware are designed and implemented purely for abusive purposes, urgent research into controls on the advertising, sale of such items or regulation of their use should be considered, particularly via the forthcoming Online Harms Bill. Platforms that allow access to technologies that are clearly abusive, such as Google, Amazon and Ebay require stricter controls. For example, Google's policy on stalkerware is inadequate given the fact that those apps are advertised as parental tools⁶.

Risk assessment, repeat offences and serial offenders: Many cases involve repeated acts and, in some cases, regular behaviours that have subsequently escalated. There needs to be a greater understanding and recognition of the indicators of high risk when perpetrators are using technology to facilitate abuse. It needs to be incorporated within the risk assessment models being used. If risks can be identified earlier there will be opportunities to intervene earlier and perhaps prevent

⁶ https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265

behaviours from being repeated or escalating further. Using civil injunctions and criminal behaviour orders earlier could impact upon repeat offending and reduce future serial offending.

Police training: Training policing staff in the full range of potential criminal offences which can be used. Some offences seem to be under-utilised (Computer Misuse Offences), which could often be used earlier in cases against offenders.

Victim centred responses: In responding to victims, responsibility for the abuse must be placed firmly with the perpetrator and there must not be an expectation that the victim change their behaviour in order for the abuse to stop. A thorough risk assessment must be undertaken in order to identify wider patterns of abusive behaviour and to ensure the behaviour is not identified and responded to as a one-off incident, which by itself does not constitute a criminal act.

Children: Children's voices are significant. They are being used to perpetrate abuses, whether overtly or covertly and are victims of technological abuse too. It is important to listen to children's accounts. The forthcoming Domestic Abuse Act will recognise children who witness/live with domestic abuse as victims, regardless of whether they are experiencing physical violence. Where TFDA is occurring, it should be recognised that children are also being victimised.

For tech companies

Fake accounts: More effort to prevent the creation of fake accounts, and removal of those who repeatedly do so.

Algorithms: Algorithms need to be adapted so as to not encourage the sales of spyware and covert devices for abusive purposes and avoid directing perpetrators to guidance informing them as to how to hack into their partner's accounts/ stalk partners. Google's current advertising policy⁷ 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 domestic abuse service providers

Updated training: Technological aspects to be included in domestic abuse training – Domestic Abuse Matters (DA Matters) run by SafeLives

Specialist advocates: The development of specialist advocates with the relevant knowledge and skills. Many services are already developing this specialism, but it must be supported further with sustainable funding.

Further research

This research was predominantly focused on the methods, tools and motivations of perpetrators and though some insight has been provided into the harms experienced by victims, further research could centre upon victims' experiences and utilise their voices to fully appreciate the impact that TFDA is having on people's lives. The inclusion of children and the effects of TFDA upon them also requires more research.

There continues to be gaps in knowledge as to the experiences of underrepresented groups, therefore future research should focus on working with specialist domestic abuse service providers as well as TFDA victims and perpetrators who are BME/ LGBTQI+ / have disabilities.

⁷ https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265

1. Introduction

The UK Government's Violence Against Women and Girls (VAWG) strategy (2016-2020)⁸ set out the ambition to tackle appalling crimes disproportionately impacting upon women and girls, including domestic abuse and violence. Underpinned by four strategic pillars: prevention, provision of services, partnership working, and pursuing perpetrators, the strategy has involved bringing more perpetrators to justice and supporting victims through the criminal justice system. Furthermore, in 2020 a landmark Domestic Abuse Bill⁹ has been introduced to improve the response to domestic abuse.

From 2018-2020 the development of a range of novel approaches to working with perpetrators of domestic abuse were funded by the Government via the Police Transformation Fund¹⁰. Although providing invaluable insight into perpetrators and victims, these and other national projects often neglect the important role that technology is playing within domestic abuse. Where technology has been considered within calls, such as the UK Tech vs Abuse fund 2019¹¹, it has been proposed as the solution to domestic abuse, rather than a key component within its perpetration. There is a lack of understanding about the intersection between computer misuse offences and domestic abuse perpetration, which evidence shows is increasingly part of the process (POST, 2020; Refuge, 2019). Technology, security and privacy are essential to domestic abuse victims but are often compromised. This research project is one of the first UK studies to explore the facilitation of computer misuse and related technological offences within domestic abuse, providing the foundation for the development of research tools to investigate this area.

The report will begin with an overview of domestic abuse, illustrating the severity, scale and risk factors of this crime. The report will then consider the current research on computer misuse and technology-facilitated domestic abuse (TFDA) before setting out the methodology used in this research. The report will then lead into a discussion of the key types of offences, abuses and behaviours involved in TFDA and the current related legislation. The report then moves to explore the particular tools that are employed within TFDA before considering the extent of the different types of TFDA and the online spaces that enable such behaviours. The report then examines the drivers and motivations of TFDA, before presenting perpetrator profiles, including a typology of TFDA offending. The report also considers under researched groups. Much of the current literature focuses on women as victims of domestic abuse and men as perpetrators, due to the evidenced disparity in victimisation and perpetration rates respectively. As a result, other 'hidden' groups such as men as victims, women as perpetrators, BME groups, LGBTQI+ communities, and disabled persons are overlooked - suggesting the need for a greater intersectional approach to developing and implementing responses to domestic abuse perpetrators and victims from these groups. Finally, although the focus of this research is on perpetrators and the facilitation of the abuse, the report also considers the harms of TFDA as well as the levels of support available, and whether there is the necessary awareness, capacity and technical understanding to adequately respond to the issue.

⁸

<https://www.gov.uk/government/publications/strategy-to-end-violence-against-women-and-girls-2016-to-2020>

⁹

<https://www.gov.uk/government/publications/domestic-abuse-bill-2020-factsheets/domestic-abuse-bill-2020-overarching-factsheet>

¹⁰ <https://www.gov.uk/government/publications/police-transformation-fund-investments-in-2019-to-2020>

¹¹ <https://www.techvsabuse.info/>

This report has been produced alongside two other outputs. There is a literature review that was conducted at the start of the project. This has been updated as the project progressed and for this reason this report will only reference relevant literature where necessary. Readers interested in the broader literature should consult that output. Second there is an output of a victim guidance leaflet, produced in conjunction with our network of domestic abuse service providers, which is being disseminated directly to victims via those channels.

Just to note that the term victim is predominantly used throughout the report; however, the problematic use of terminology is acknowledged. Ordinarily the term victim would be applied to refer to those currently in an abusive relationship, with survivor used for those no longer in an abusive relationship but highlights the person's agency in dealing with their experience (Radford et al., 2012). It is also recognised, however, that this demarcation is not necessarily always clear - much depends on how individuals view themselves. Within feminist discourse there has been debate about the appropriateness of the terms victim or survivor, however the former is the common term employed within the criminal justice system (Radford et al., 2012). Furthermore, the terms abuser/perpetrator and offender are used interchangeably throughout the report.

2. Domestic Abuse

Domestic abuse is an abhorrent crime with far reaching impacts upon its victims. In the year ending March 2020 in England and Wales, 2.3 million adults aged 16-74 years (1.6 million women, 757,000 men) were subjected to domestic abuse (ONS, 2020) and more than one in ten of all offences recorded by the police are domestic abuse related (ONS, 2020).

The UK Government (GOV.UK, March 2013) definition of domestic violence and abuse is:

‘Any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. This can encompass, but is not limited to, the following types of abuse:

- Psychological
- Physical
- Sexual
- Financial
- Emotional

The Domestic Abuse Act 2021 received Royal Assent on 29.04.21 and sets out for the first time in England and Wales a statutory definition of domestic abuse, emphasising that it is not just physical violence, but can also be emotional, coercive, controlling and economic abuse. Within this definition, children are now explicitly recognised as victims if they witness abuse. Whilst the Act does not explicitly mention the role of technology in domestic abuse, the Government has said that it is designed to be “future-proof” to combat emerging trends including tech abuse¹². The Act also introduces two new protective measures - Domestic Abuse Protection Notices (DAPN) and Domestic Abuse Protection Orders (DAPO). These do not replace existing measures such as non-molestation and harassment orders, but are intended to become the standard protective measures to be used in domestic abuse cases.¹³ A number of amendments to the Act during its passage through Parliament have created a number of new offences, two of which are most relevant to this research:

1. extending the controlling or coercive behaviour offence to cover post-separation abuse
2. extending the ‘revenge porn’ (*sic*)(image based sexual abuse) to cover the threat to disclose intimate images with the intention to cause distress

On 29 December 2015, the offence of controlling or coercive behaviour (CCB) came into force through Section 76 of the Serious Crime Act 2015. The stated aim of this new offence was to “close a gap in the law around patterns of coercive and controlling behaviour during a relationship between intimate partners, former partners who still live together, or family members.¹⁴” It was also anticipated that the introduction of this offence would enable the criminal justice system (CJS) to move beyond an exclusively ‘violent incident model’ (Stark, 2012), in which cases of domestic abuse are investigated and prosecuted as individual and unconnected occurrences of violence, which can mask the underlying patterns of coercion or control in an abusive relationship (Tuerkheimer, 2003).

¹² <https://post.parliament.uk/technology-and-domestic-abuse/>

¹³ <https://nationallegalservice.co.uk/the-domestic-abuse-bill-2020-2021/>

¹⁴

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/482528/Controlling_or_coercive_behaviour_-_statutory_guidance.pdf

The Government definition of CCB as set out in the statutory guidance is as follows:

- Controlling behaviour: a range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating their everyday behaviour.
- Coercive behaviour: a continuing act or a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim.

In addition, the controlling or coercive behaviour must take place “repeatedly or continuously”; the pattern of behaviour must have a “serious effect” on the victim; and the behaviour of the perpetrator must be such that they knew or “ought to know” that it would have a serious effect on the victim.

This offence does not apply to situations where partners, current or former, do not live together, which is problematic due to the fact that abuse does not just occur whilst a relationship is ongoing, often perpetrators escalate their abusive behaviours after a relationship has ended in order to maintain/regain control over their victim. Furthermore, vulnerable groups living in residential settings or people who live alone are disregarded by the current legislation. In light of this and other gaps in the current legislation, the Home Office has undertaken a rapid review of the CCB offence, to assess its effectiveness and determine whether any changes to the Domestic Abuse legislation, or any wider policy interventions, are needed. In March 2021, A Review of the Controlling or Coercive Behaviour Offence was published.¹⁵ The most prominent suggestion within this review is that the legislation should be extended to include former partners who do not live together, to ensure that post-separation abuse is not overlooked, and to address any confusion among police and prosecutors regarding the recording and charging of abuse that continues beyond the end of a relationship. Additionally, current stalking and harassment offences not being applicable or appropriate in all cases of post-separation abuse, especially where the behaviour is still closer to coercion or control, is highlighted. Such legislation is more relevant to stranger perpetration for example.

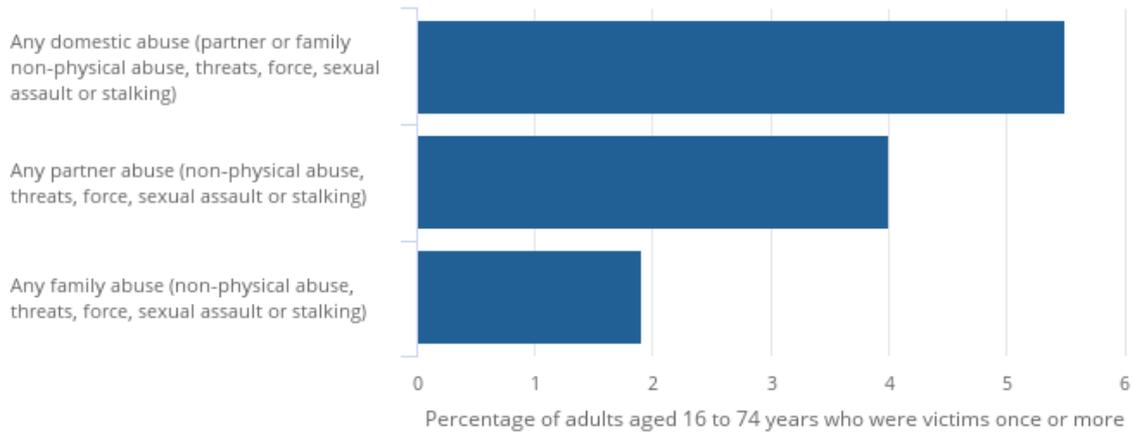
Coercive control was conceptualised by Evan Stark (2007) and refers to the ways in which women are coerced and controlled by their male partners. Stark (2007) describes it as ‘the micro-regulation of women’s lives’ – with the sex of the victim and perpetrator and gendered norms regarding women and men’s behaviours being significant. Section 76 of the Serious Crime Act 2015 created a new offence of coercive and controlling behaviour in England and Wales (2015) and in Scotland as part of the Domestic Abuse (Scotland) Act 2019. It is gender-neutral in its legal application and acknowledges that anyone can become a victim of domestic abuse. Yet, there is a paucity of research on what coercive control looks like when it is perpetrated against men – in either heterosexual or gay relationships. Furthermore, greater understanding of how technological abuse can form part of a larger pattern of coercive domestic offending is needed.

2.1. The Scale of Domestic Abuse

¹⁵https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/965361/review-of-the-controlling-or-coercive-behaviour-offence-horr122.pdf

Figure 1: A higher percentage of adults were victims of partner abuse than family abuse

Prevalence of domestic abuse in the last year for adults aged 16 to 74 years, by perpetrator-relationship, England and Wales, year ending March 2020



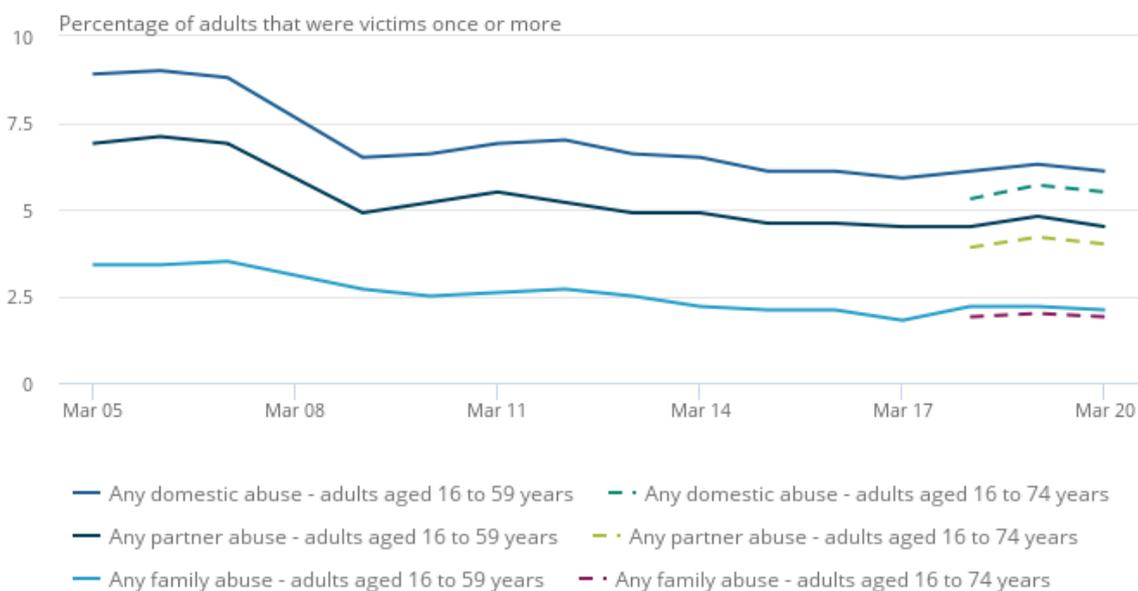
Source: Office for National Statistics - Crime Survey for England and Wales

According to the Crime Survey for England and Wales (CSEW) year ending March 2020, an estimated 5.5% of adults aged 16 to 74 years (2.3 million people) experienced domestic abuse in the last year (Figure 1) (ONS, 2020). As seen in previous years, a higher percentage of adults experienced abuse carried out by a partner or ex-partner (4.0%) than by a family member (1.9%).

The police recorded a total of 1,288,018 domestic abuse-related incidents and crimes in England and Wales (excluding Greater Manchester Police) in the year ending March 2020. Of these, 41% (529,077) were incidents not subsequently recorded as a crime. The remaining 59% (758,941) were recorded as domestic abuse-related crimes.

Figure 2: Domestic abuse estimated by the survey has not changed significantly over the last year

Prevalence of domestic abuse in the last year for adults aged 16 to 59 years and 16 to 74 years, England and Wales, year ending March 2005 to year ending March 2020



Source: Office for National Statistics - Crime Survey for England and Wales

There was no significant difference in the prevalence of domestic abuse experienced in the last year, for men and women aged 16 to 74 years in the year ending March 2020 compared with the year ending March 2019.

The cumulative effect of small year-on-year reductions, including a significant decrease in the year ending March 2009, has resulted in a significantly lower prevalence of domestic abuse experienced by adults aged 16 to 59 years in the year ending March 2020, compared with the year ending March 2005 (Figure 2). For example, 4.0% of men and 8.1% of women aged 16 to 59 years had experienced domestic abuse within the last year in the year ending March 2020. This compared with 6.5% of men and 11.1% of women in the year ending March 2005. The downward trend in prevalence over time is driven by reductions in the prevalence of partner abuse, which has decreased from 6.9% to 4.5% over the same period.

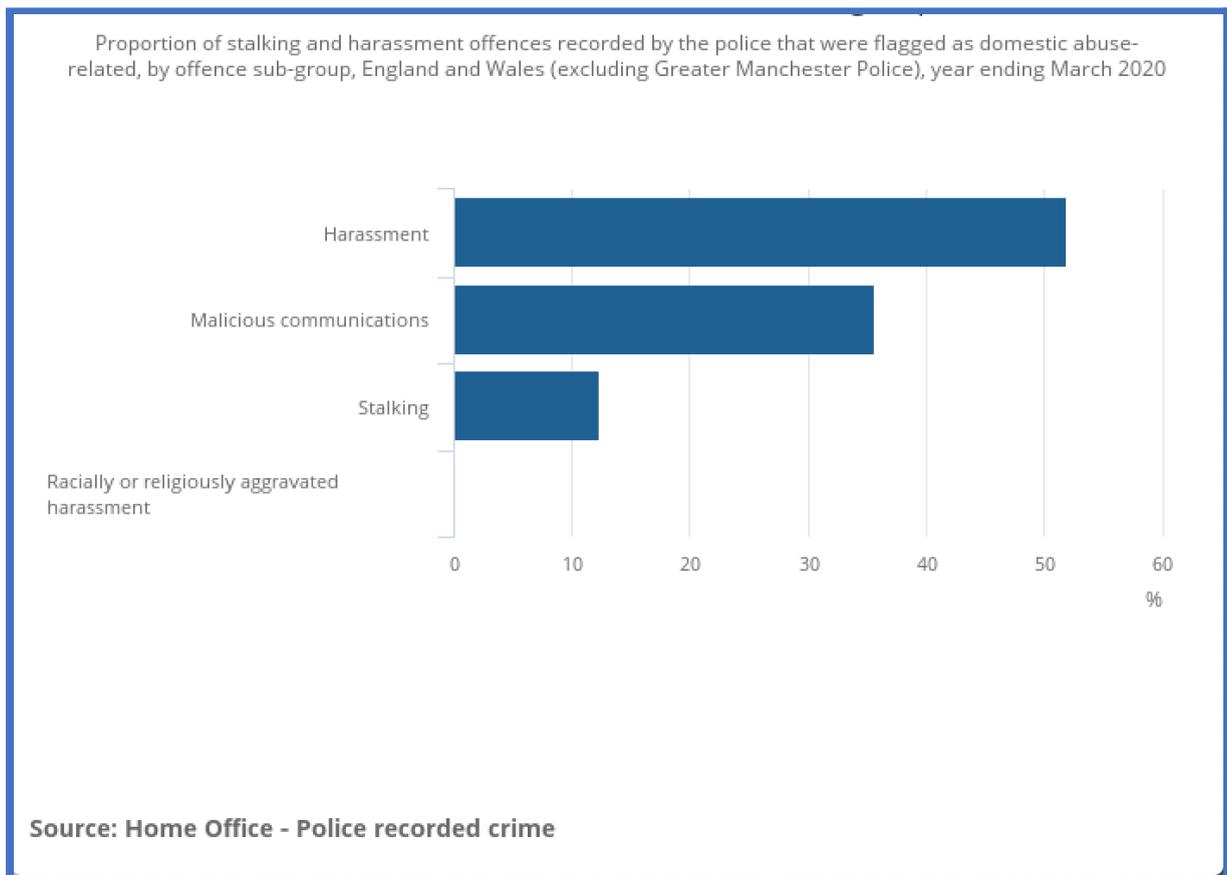
Coercive and controlling behaviour includes both physical and on-physical forms of abuse. The CSEW asks respondents questions in order to identify types of non-physical abuse, such as whether their partner has:

- isolated them from relatives and friends
- humiliated or belittled them
- controlled their access to household money and/or controlled how much they spend
- monitored their letters, emails or texts
- kept track of where the respondent went

Non-physical abuse is the most prevalent type of domestic abuse reported by CSEW respondents. The proportion of those reporting non-physical abuse by a partner has remained at approximately 3% of adults aged 16-59 since 2012/13. Since 2009/09 the proportion of those reporting non-physical abuse by a family member has remained between 1% and 1.5%. Force, threats and stalking behaviours are also experienced by victims of both partner abuse and family abuse.

Regarding police recorded crime, the majority of domestic abuse-related stalking and harassment offences were in the harassment sub-group (see Figure 3).

Figure 3. The majority of domestic abuse-related stalking and harassment offences were in the harassment sub-group



During the COVID pandemic in the UK there was a 7% increase in police recorded offences flagged as domestic abuse related between March and June 2020, compared with the same timeframe in the previous year (ONS, 2020). It should be noted, however, there has been a gradual increase in these offences over recent years, and so it cannot be determined whether this increase is directly attributable to the pandemic (ONS, 2020). Additionally, there has been a noticeable increase in demand for domestic abuse support following the easing of lockdown measures in mid-May 2020, including a 12% increase in the number of domestic abuse cases handled by Victim Support during the week lockdown restrictions were eased, compared with the week prior; indicating the difficulties experienced by victims in safely seeking support during lockdown. As such, increases in demand for domestic abuse victim services, do not necessarily reflect an increase in victims, but may instead demonstrate an increase in the severity of abuse being experienced, and a lack of coping mechanisms like having the ability to leave the home to escape the abuse, or have counselling (ONS,

2020). Nevertheless, Womens Aid report that domestic abuse has worsened during the pandemic, with over 90% (91%) of individuals currently experiencing domestic abuse stating that the Covid-19 pandemic had negatively impacted in at least one way. Of those women living with their abuser during lockdown, 61% said the abuse had worsened. More than two-thirds (68%) said they felt they had no one to turn to during lockdown.¹⁶ Technology may assist with victims' access to support, however with abusers also exploiting technology to facilitate their coercive control and abuse, victims may also have reduced possibilities of safely accessing digital devices away from the monitoring of their abusers during the pandemic (Slakoff et al., 2020). Lockdown has compelled many victims to live in close quarters with their perpetrators with little respite. Whilst forced separation of couples during lockdown may lead to an increase in the use of digital technologies to monitor and harass victims in lieu of physical contact. As victims have spent more time online during lockdown, so too the opportunities for cyber abuse have increased. For example, the antivirus software provider Avast, has reported that detections of stalkerware in the UK rose by 83% between March and June 2020, one of the sharpest rises globally¹⁷.

2.2. Domestic Abuse Risk Factors

Risk factors associated with domestic abuse occur at individual, family, community and wider societal levels. These include:

- past history of violence
- marital discord and dissatisfaction
- difficulties in communicating between partners
- male controlling behaviours towards their partners (WHO, 2017)

Other vulnerability factors include drug and alcohol dependency, financial constraints.¹⁸ Social exclusion and loneliness can also be triggering factors, leading to victims seeking contact with abusive ex-partners. Furthermore, domestic abusers often deliberately socially isolate their victims.

The National Police Chiefs Council (NPCC) domestic abuse, stalking and harassment and honour-based violence (DASH) risk assessment tool has been used as standard practice throughout the UK since 2009, for assessing the risk of the suspect committing a further domestic abuse offence (Almond et al., 2017). The NPCC DASH contains four sections: current situation, children/dependants, domestic violence history and abuser. The assumption is that the greater the number of risk factors, the greater the risk of the suspect committing a further domestic violence offence. Individuals completing the checklist are then required to categorise their assessment as "standard" (likelihood of no further serious harm), "medium" (offender has potential to cause serious harm but is unlikely to do so unless there is a change in circumstances) or "high" (a risk of serious harm that could happen at any time).

Jane Monckton-Smith (2019) has created an eight-stage intimate partner homicide timeline in which the escalation of risk factors in domestic abuse situations are outlined. Informed by the analysis of 575 homicide cases involving women killed by men using Karen Ingala Smith's *Counting Dead Women* database¹⁹ Monckton-Smith's timeline is placed into a temporal sequence, with control considered to influence every stage.

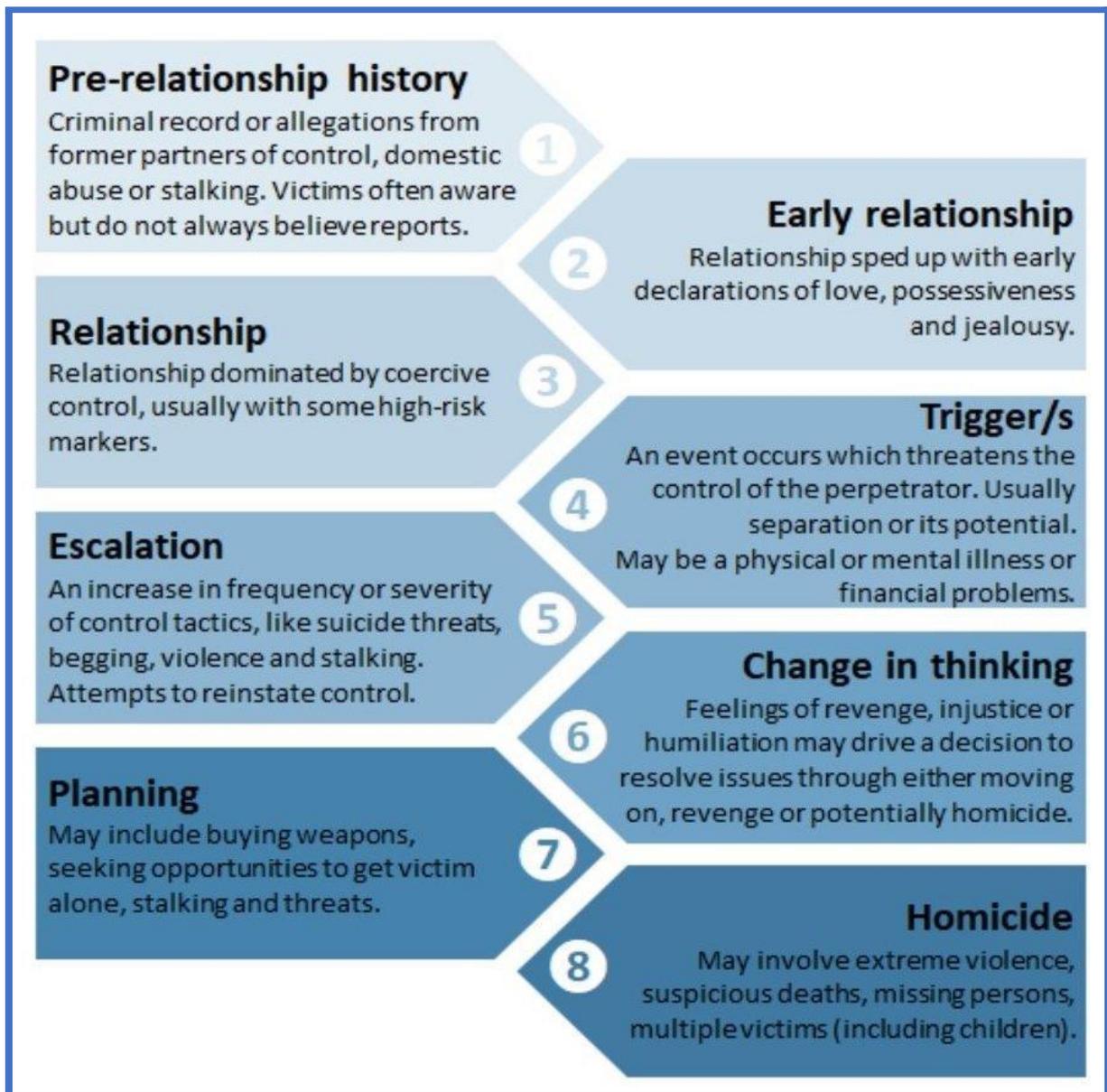
¹⁶<https://www.womensaid.org.uk/a-perfect-storm-the-impact-of-the-covid-19-pandemic-on-domestic-abuse-survivors-and-the-services-supporting-them/>

¹⁷<https://www.wired.co.uk/article/stalkerware-spyware-monitoring-apps-uk>

¹⁸<https://www.addictioncenter.com/addiction/domestic-violence/>

¹⁹<https://kareningalasmith.com/counting-dead-women/>

Figure 4. Eight Stage Intimate Partner Homicide Timeline (Monckton-Smith, 2019)



The implication is that technology has a greater chance of coming into the equation or being a focal part of the abuse, between stages 5 – ‘escalation’ and 6 – ‘change in planning’, with perpetrators highly likely to use technological tools or engage in computer misuse to further the control of their victim, especially when the victim is planning to or has ended the relationship. Recent separation is when the victim is at the highest risk of harm from the perpetrator. The Femicide Census (2020: 30) found that of the 888 women killed by partners or former partners, at least 378 (43%) were known to have separated, or taken steps to separate, from the perpetrator. However, Monckton-Smith also discusses how, within stage 3 - ‘living with control’ - victims may allow their partners access to their phone and device passwords in order to assuage their jealousy. Even though access has been provided by the victim, this is not necessarily through the victim’s own choice and enables the perpetrator further control. As Monckton-Smith (2021, p.147) notes: “Many controlling people will have been monitoring and tracking their partners during the relationship, not just after it ends.” Box 1 presents a case example outlining the 8 steps of the intimate partner homicide timeline.

Box 1.

Case Example – Alice Ruggles

In January 2016 Alice began a brief relationship with Trimaan Dhillon. Initially he was charming and attentive, but this soon changed into controlling and abusive behaviour, and Alice began to be cut off from her friends and family. During this time, Dhillon had taken control of Alice's Facebook account by changing the password (she later shut this down and created a new one). Upon discovering that Dhillon was cheating on her, Alice ended the relationship, however he was not prepared to accept no for an answer. Amongst the obsessive and persistent contact, she also discovered that he had hacked into her social media accounts, and it became clear that he was reading all her messages so that he knew who she was speaking to and where she was. Despite Alice changing her passwords, reporting the stalking to the police and a Police Information Notice (PIN) issued against Dhillon, he was able to track her movements and break into her house and murder her when she was alone. (Alice Ruggles Trust <https://www.alicerugglestrust.org/alices-story>).

3. Computer Misuse and Technology-Facilitated Domestic Abuse

Digital technologies, including the internet, have enabled people to socialise and exchange personal information online, often under the protection of anonymity and with little oversight or accountability. This has enabled different forms of computer misuse and online harms against individuals. With the increased use and development of technology, methods of perpetrating domestic abuse are progressively incorporating computer misuse offences and digital tools, enabling perpetrators more opportunities to monitor, threaten, and humiliate their victims. Many victims of domestic abuse also experience TFDA in some form and often there will be digital evidence of abusive behaviours in domestic abuse cases.

There is a growing body of academic research in the field of TFDA (Yardley, 2020), mostly originating from the US and Australia, with existing literature focusing upon the medium and the acts it enables, rather than the actors or the context in which the abuse occurs (Harris & Woodlock, 2019). TFDA is a key component of coercive control, a course of conduct intended to deprive others of their liberties, freedoms, and independence in such situations (Pain, 2014; Pence & Paymar, 1993; Stark, 2007).

Online platforms and especially social media are routinely used by perpetrators of domestic abuse. Technologies such as geolocation software and spyware for surveillance deliver new mechanisms for 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). Nearly a third of survivors responding to a Women's Aid survey on online abuse have reported the use of spyware or GPS locators on their phone or computer by a partner or ex-partner (Laxton, 2014). Indeed, there has been a move away from perpetrators needing to obtain specialist devices or hardware to track their victims, towards hacking and monitoring their victims remotely via the victims' own accounts. Within the IPV literature there is discussion about the installation of IPS apps on victim's mobile devices (Dimond et al., 2011; Fraser et al., 2010; Freed et al., 2017; Levy, 2014; Matthews et al., 2017; Woodlock, 2017). Whilst Matthews et al., 2017 interviewed 15 US survivors of IPV and found that 20% reported being monitored via spyware.

In the 2016 Tech vs Abuse study, which involved over 200 female domestic violence victims in the United Kingdom, 47% of victims reported to have been monitored via technology, and a quarter were unsure (Chayn, SafeLives & Snook, 2017). These findings are consistent with the Women's Aid study, which surveyed 307 women in 2013. It was found that 48% of respondents experienced TFDA by their former partner after ending the relationship (Laxton, 2014) and a further 45% reported that their intimate partner had abused them online during their relationship. These findings support a claim contrary to the popular belief that domestic abuse ends when the victim ends the relationship (Rempel et al., 2019). Moreover, research shows that technology-facilitated domestic abuse can occur at all stages of a relationship, including while the relationship is ongoing (Belknap et al., 2012); however, relationship breakdown can be a common trigger, with such abuse often escalating when the victim leaves or attempts to leave their abuser (Woodlock, 2017). As per Monckton Smith's intimate partner homicide timeline (discussed previously), this is a period identified as the most dangerous point in an abusive relationship for women (Dimond et al., 2011). The heightened abuse victims experience when they attempt to or do leave includes increased stalking, harassment, and the risk of being killed (Rempel et al., 2019) as the perpetrator attempts to maintain control after their victim has physically distanced themselves. In the Women's Aid study, 38% of the victims surveyed reported that they had been stalked online after ending their relationship with their ex-partner (Laxton, 2014). Divorce and child custody disputes are also trigger points for TFDV, with perpetrators attempting to obtain an unfair advantage in legal proceedings by accessing confidential correspondence. Perpetrators might hack into victim's accounts in an attempt

to access private correspondence with their solicitor for example, and/or could delete pivotal evidence to the victim's case, enabling them to gain a more favourable outcome in the proceedings - either in terms of finances or access to children, but could also be about removing evidence of the perpetrator's abusive behaviour. The BBC reported that the family courts have seen an increasing number of incidents of digital manipulation of documents used as evidence in such proceedings, including written evidence such as bank statements, bills, drug test documentation, as well as audio files²⁰.

Domestic abuse perpetrators can commit offences breaching the UK Computer Misuse Act 1990 (CMA) and other related offences, by exploiting their knowledge of partners to unlawfully access their online personal and financial accounts, continuing patterns of harassment, intimidation and stalking. Often abusers have physical access to their partners devices and can know, predict or force disclosure of access credentials such as passwords, PIN codes or swipe patterns (Freed et al., 2017; Matthews et al., 2017; Woodlock, 2017). This provides abusers with easy opportunities to install spyware, including via app stores such as Google Play Store or Apple App Store, which does not require sophisticated technical knowledge.

Though there is established knowledge regarding the nature of how Computer Misuse Act (CMA) 1990 offences (such as unauthorised access to computers or personal accounts and developing or supplying ransomware or malware) enable financial crimes such as fraud and extortion (Button and Cross, 2017; Button et al, 2009; Cross et al 2014; Cross, 2015; Whitty & Buchanan, 2016), there is a lack of research evidence on how CMA offences facilitate other crimes, particularly domestic abuse. Estimates on the prevalence of CMA offences and police-recorded CMA offences do not intrinsically capture when a CMA offence is a precursor to, or an inherent part of, another crime type recorded as the primary offence. For example, there is no domestic abuse 'flag' with the main CMA reporting system - Action Fraud. These reports have to be manually identified using text searches and inclusion relies upon the victim explicitly detailing their relationship to the suspect in their report. This is in addition to the significant under reporting of cybercrime to law enforcement. The CSEW found that only 4% of victims of computer misuse crime reported the matter to Action Fraud in 2019-20.²¹ When asked why they did not report, the most common reasons provided by victims were that the matter was 'too trivial' or 'not worth reporting' (32%), or that it was a 'private matter' which they had dealt with themselves (30%)²². Therefore, understanding in regard to the scale and characteristics of CMA offences in relation to domestic abuse is a crucial yet current gap in knowledge.

²⁰ <https://www.bbc.co.uk/sounds/play/m000p10c>

²¹ <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesannualltrendanddemographicictables>

²² Other reasons cited for not reporting included the following, 'Police or Action Fraud could not do anything' (12%), 'Other' (8%), 'No loss / damage or attempt at offence unsuccessful' (8%), 'Police or Action Fraud would not have been bothered / interested' (7%), 'Reported to financial authorities (e.g. bank, building society)' (7%), 'Common occurrence / just something that happens' (7%) etc.

4. Methods

The research for this report involved the following methods: literature review, media case analysis, technology review, and interviews with domestic abuse service providers.

4.1. Media Analysis

Analysis of cases found in the media which involved the use of technology to facilitate abuse within a relationship or after a relationship, was undertaken. In total 146 cases were found, and these revealed a wide range of ways in which technology was being used.

To do this we used the following search criteria:

- Cases where there was evidence of current or past relationship (marriage, partners, sexual relationship) or family relationship.
- Cases where information communication technology (ICT) and other technological devices such as covert cameras, tracking devices were illegally/unethically used, or where ICT was used beyond 'normal' levels of communication. For example, there were lots of cases where an ex-husband threatened an ex-wife using email, text etc. This was considered no different to using traditional communications such as the telephone or mail, so such cases were not included. If they had, virtually every case would have needed to be included, which would have made the selected cases less meaningful, as virtually everyone uses such means to communicate. However, if communication using such methods became excessive, such as "bombardment" with emails, such cases were included as they illustrated the potential for ICT to "industrialise" harassment and abuse.
- Cases from 2015 onwards, unless there was some rare or novel element to the case that warranted inclusion. One case prior to this date was used from 2011 involving a son abusing their father in the USA. The year 2015 was chosen to manage the expected number of cases and because it also suited changes in legislation creating new offences (coercive control and disclosing private sexual images).
- UK cases have all been added where found, while non-UK cases have been added to illustrate rare issues not generally found in the UK.
- Where there has been conviction, admission or allegation in a reputable news outlet, these cases have been added.

The search terms which were used included:

- Convicted Computer Misuse Act
- Convicted stalking/harassment
- Convicted revenge porn
- Convicted coercive control
- Convicted malicious communication
- Hacking: ex, smart home, husband, wife, boyfriend, girlfriend
- Divorce hacking, spyware
- Husband, wife, boyfriend, girlfriend ex., revenge
- Husband, wife, boyfriend, girlfriend ex.. spying, covert cameras/CCTV, tracker, fake account
- Husband, wife, boyfriend, girlfriend ex.. sabotage

The search engines used included: Nexus, local newspaper searches throughout UK and specialist publications. Some searches brought up large numbers of articles, many of which were not relevant, and were refined further using some of the terms above. For example, the search "husband hack wife" on Nexus for 2015+ produces over 10,000 items on news alone. Many of these were not relevant and further refinement was required.

Caveats

There are a number of caveats that must be noted with the approach used in this report:

- Newspapers often focus on sensational cases;
- Newspapers vary in the amount of information covered in a case;
- Not all information is always covered in a case; and
- Risk that the reporting may include inaccuracies

The nature of the sample means that sophisticated statistical analysis is pointless, but where appropriate, descriptive statistics will be used to illustrate issues.

Overview of cases

Using the criteria above we were able to identify 146 cases. Of these 117 of these cases were from the UK, with 29 cases from other countries including: USA, Australia, New Zealand, Belgium, Switzerland, Singapore, Saudi Arabia, Republic of Ireland. In some cases it was not possible to determine the exact location, due to the way the report was presented. In terms of the UK cases table 1 below illustrates the breakdown of cases by region and nation.

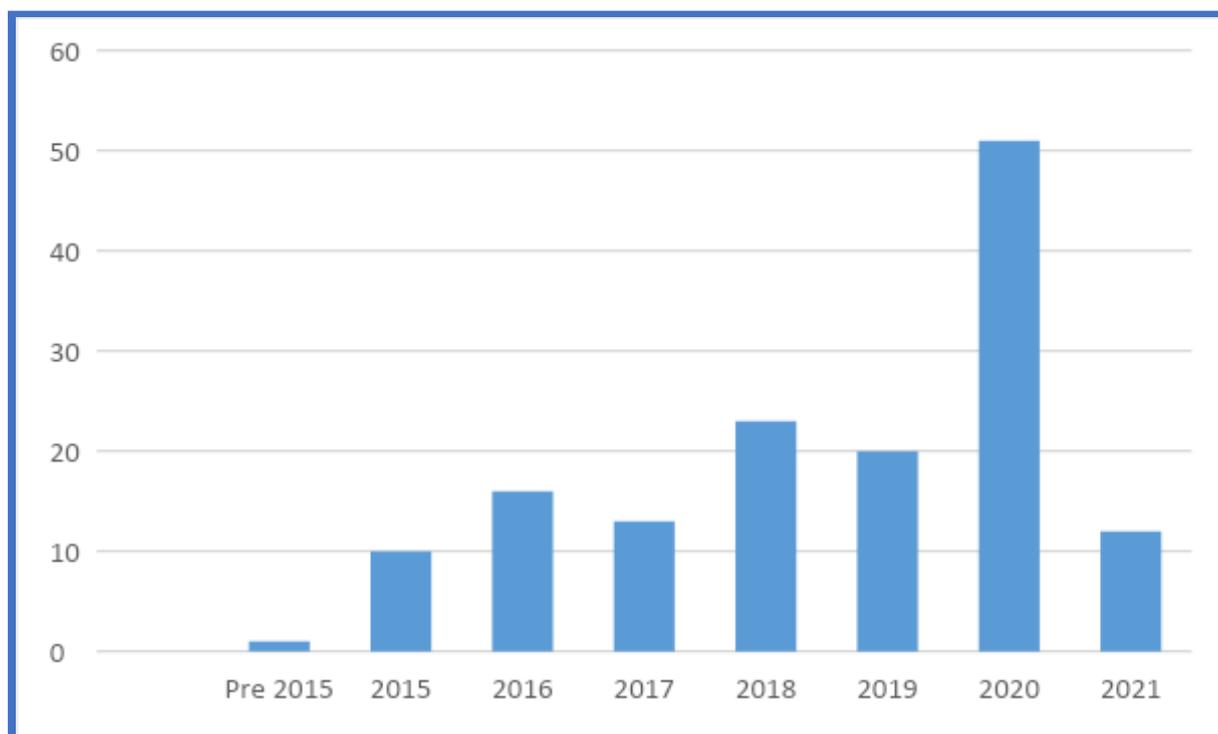
Table 1. UK sample by region and nation

Location	Total	Total by Nation	Percentage of Sample
England (South West)	16		13.7
England (South East)	8		6.8
England (London)	5		4.3
England (Eastern)	17		14.5
England (West Midlands)	5		4.3
England (East Midlands)	7		6.0
England (North West)	28		23.9
England (Yorkshire and Humberside)	9		7.7
England (North East)	5		4.3
Total England		100	85.5
Wales		8	6.8
Scotland		6	5.1

Northern Ireland		2	1.7
UK (Unable to determine specific location in UK)		1	0.9
Total UK		117	

The starting point for the research was 2015. One case prior to this date was included due to its unique characteristics. Figure 5 shows a gradual rise each year in cases. Given that in 2021, only 10 weeks in at the time of research (March 2021), the upward trend in cases looks set to continue. In part this is the result of two pieces of legislation: Criminal Justice and Courts Act 2015 Section 31, which criminalised so-called ‘revenge porn,’ and the Serious Crime Act of the same year, Section 76, which created the offence of ‘Controlling or Coercive Behaviour in an Intimate or Family Relationship’. As law enforcement and prosecutors have begun to understand and make greater use of these new legal tools more cases have been prosecuted, therefore coming into the public domain, and in doing so illustrated technological abuse.

Figure 5. Cases by year reported



4.2. Technology Review

Survivors of domestic violence increasingly report that abusers make use of technology to monitor or control their victims. We hypothesise that most abusers find these technologies online using simple web searches. In this part of the project therefore, we undertook a technology review to examine

technologies used in TFDA, their nature and where they can be found online (including how they are marketed). This allows us to understand the options provided to perpetrators online and explore the ease of access and ease of use.

To conduct this review, we first designed a comprehensive search strategy in order to understand the technology options provided to domestic abuse perpetrators online. We started our search using a small set of queries (e.g., “track my girlfriend’s phone without them knowing”) which were determined during internal project meetings involving local teams of domain experts. The queries used have also been informed by an investigation into the scientific literature on the role of technology misuse in domestic abuse. This search aimed to be inclusive and thus considered a wide variety of the technologies and types of abuse. In total, this analysis led to 40 initial queries, which can be viewed in Table 2. We used Google for these queries, primarily due to its prominence as the leading search engine.

Table 2: Initial Queries

Stalkerware	Track my husband’s car
Technology to monitor partners or children	Track person
Apps to monitor partners (or children)	track my wife
Devices to monitor partners (or children)	read SMS from another phone
Covert parental control app or tracker	how to catch my cheating spouse
Remote control technologies for home violence abuse	Read your wife’s messages without touching her phone
Remote control smart technologies abuse violence	Where to place covert camera in bathroom
Tracker apps / devices	Where to place tracking device on car
gps tracker app free phone tracker app	track my husband’s phone without them knowing
Family tracking apps/mutual tracking	track my girlfriend’s phone without them knowing
Spy on partner	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Facebook’s account
Spy on cheating partner	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Whatsapp?
Stealth monitoring apps / devices	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Instagram account?
Couple tracker apps / devices	How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s social media?
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?
Monitor wife’s emails	How to use Alexa to spy on my wife
Track car	employee monitoring’ software

Track my wife's car	iCloud spying features
---------------------	------------------------

In addition to those initial queries, we collected predictions made by Google for similar search queries; these were consequently added to our sample of queries. Google makes predictions based on the relevant searches done in the past and what other people are searching for, including trending searches. We believe that this approach is quite informative and comprehensive revealing the similar searches executed by individuals.

From a reflection on these predictions, we noted that these provide semantically similar queries and are thus likely to also be used by potential perpetrators when searching via Google. At the end of this process, we collected 332 queries; a sample of which can be seen in Table 3.

Table 3: 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

From this list we removed the duplicate queries suggested by Google, queries that are not directly related to our goals (“covert cctv cameras uk law”, “is it illegal to spy on your spouse”, “track all mutual funds in one app” etc.) at the beginning of our study. During execution of searches, we also removed queries that do not return any unvisited webpages on the first two result pages. This led us to analyse results coming from 76 queries at the final stage.

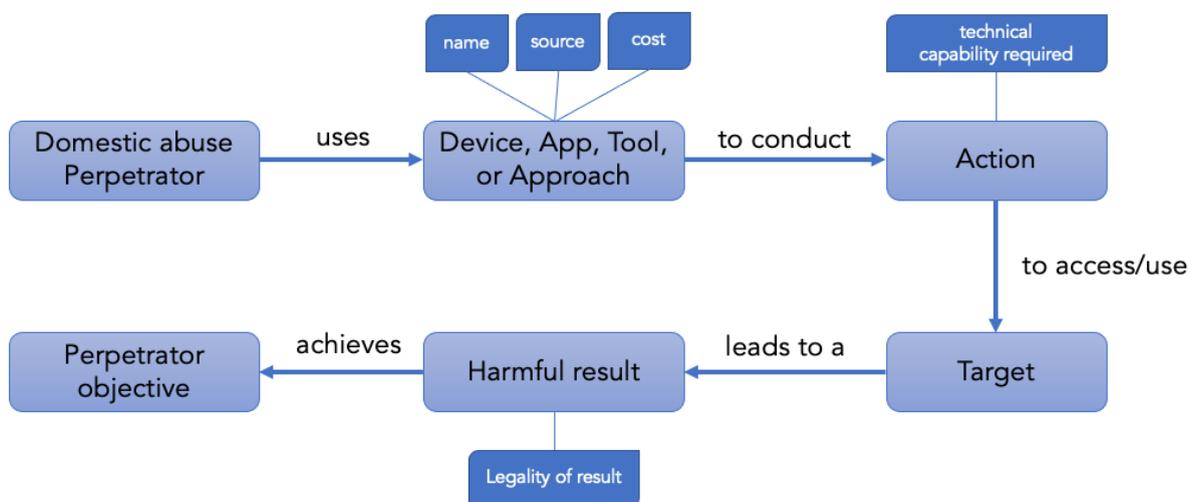
From the execution of these searches within Google, our preliminary findings revealed a wide variety of resources. Some of them aim to help victims and provide information about digital safety. There are also news articles pertaining to domestic violence cases where technology was misused. In addition, there are blogs reviewing different apps or devices. Finally, there are websites of tools, apps or devices. Since the cumulative results would be overwhelming to analyse manually, we defined a research protocol for further investigations where we decided to analyse websites retrieved on the first two pages of Google search results; on average this resulted in 20 search results per query. The complete set of rules that guide our study are given in Table 4.

Table 4: Search Protocol

ID	Rule
1	First 2 pages (unvisited webpages) returned by Google will be analyzed
2	Webpages that have information about technology use will be included
3	Webpages that aim to help people with their digital safety will be excluded (how-to guides, news articles etc)
4	Any information related to legal uses of the discovered technologies will also be extracted if they have the potential to be misused by perpetrators
5	Queries suggested by Google which will not return guidance on how to misuse technologies will be excluded (“Is it legal to monitor my wife’s emails”)
6	Name of the app, device, tool and any associated cost/price will be extracted
7	Source of the app, device, tool will be extracted (Website, App Store, Online sellers etc)
8	Action taken by the perpetrator will be extracted (Using “Forgot my password” functionality of dating apps to see if an account is registered there)
9	Target (Data that can be accessed using the app/tool/device) will be extracted
10	Technical capacity required to use given technology will be extracted.
11	Harmful, illegal results will be determined by the researcher depending on the category of the digital abuse.
12	Objective of the use of the technology will be determined by the researcher based on what is stated on the webpage
13	Technical capabilities required to perform the action will be determined by the researcher based on points 8 & 9

To complement this table, we also define a framework to guide our work and analysis (see Figure 6). This framework is presented below and allows us to consider the main high-level components/aspects within the TFDA domain as it relates to our review.

Figure 6. Framework for analysing TFDA tools, considering perpetrators, actions and results



While reviewing the webpages, we mainly focused on extracting “recommendations” given to readers (we view readers as likely or potential TFDA perpetrators). These recommendations can be categorised into four broad groups: apps suggested to be installed; software programs; devices that can be purchased; or actions that can be taken which do not rely on a specific app, software or device. Throughout this document, we use “recommendation” for all of these groups.

4.3. Interviews with Domestic Abuse Service Providers

We conducted twenty-one semi-structured interviews with domestic abuse service providers and charities in England and Wales in order to yield a body of qualitative data about the experiences of domestic abuse cases involving CMA and related technology offences. The project received full ethical approval from the University of Portsmouth Faculty of Humanities and Social Sciences committee on 23rd February 2021 – Reference Number: FHSS 2021-009. A range of different domestic abuse service providers were interviewed - including those that support any genders or ethnicities, those that predominantly support women and those that specifically support men. We attempted to conduct interviews with organisations that specifically support the LBGTQI+ community, those that specifically support BME women, and those that offer support for women of particular faiths but were unable to do so due to staff unavailability during the time the research was undertaken. The interviews conducted were with domestic abuse service providers, charities, independent domestic violence advisors (IDVA) council workers, and two first response police officers, from the South of England, the Midlands and North England. The majority of the interview participants are women, which is indicative of many domestic abuse service professionals. This information is presented in Table 5 below

Table 5. Interview participant demographics

Interview	Role	Clients	Location	Gender
1	Charity – support worker	All adult victims/ any gender	N England	F
2	Charity – support worker	All adult victims/ any gender	SE England	F
3	Charity – support worker	All adult victims/ any gender	SE England	F
4	Charity – support worker	All adult victims/ any gender	SE England	F
5	Charity – support worker	Victims 16 -25/ any gender	Midlands	M
6	Council - IDVA	All adult victims/ any gender	SE England	F
7	Charity – support worker	All adult victims/ any gender	SE England	F
8	Council - IDVA	All adult victims/ any gender	SE England	F

9	Charity – support worker	Adult male victims	N England	F
10	Charity - Counsellor	All adult victims/ any gender	Midlands	F
11	Charity – support worker	All adult victims/ any gender	SE England	F
12	Council IDVA	All adult victims/ any gender	E Midlands	F
13	Charity - support worker	All adult victims/ any gender	SE England	F
14	Charity - support worker	All adult victims/ any gender	SE England	F
15	Frontline Police Officer	All victims	SE England	M
16	Council community safety officer	All adult victims/ any gender	London	F
17	Council IDVA	All adult victims/ any gender	SE England	F
18	Charity - Counsellor	All adult victims/ any gender	Midlands	F
19	Council IDVA	All adult victims/ any gender	London	M
20	Frontline Police Officer	All victims	SE England	F
21	Crown Prosecutor	All victims	SE England	F

All interviews were conducted synchronously online over Zoom or MS Teams, audio recorded, and were between 45 minutes to 2 hours in length, aside from interviews 20 and 21, which were conducted over email due to time constraints. The interviews were thematically analysed (Braun & Clarke, 2006).

The report now presents the key findings from the research, combining the data from all three phases of the project to inform the following thematic areas: Types of TFDA, Tools of TFDA, Scale of TFDA, Spaces of TFDA, Drivers and motivations of TFDA, Perpetrator profiles, Hidden Groups, Harms of TFDA, Support for victims of TFDA, Criminal Justice System (CJS) responses to TFDA.

5. Types of Technology-Facilitated Domestic Abuse

The starting point of the research was behaviours linked to the Computer Misuse Act 1990 (CMA), such as hacking and malware related attacks. These, however, only account for part of the picture.

“Where somebody’s hacked into your account, for example. Or where they’ve, they’ve pretended to be you and got into the account as you, because they’ve got your password, for example. But for me, the worst thing that perpetrators do to our clients is posting about them on social media. But I guess that doesn’t come under the Computer Misuse Act (Interviewee 3)

The interviews indicated that domestic abuse perpetrators are engaging in a broad range of behaviours involving the use of technology, some of which encompass and combine offences within legislation such as the CMA, Malicious Communications Act (MCA) 1988, the Protection from Harassment Act (PHA) 1997, the Stalking Protection Act (SPA) 2019, the Criminal Justice and Courts Act (CJCA) 2015, and the Fraud Act 2006, but also those not necessarily illegal yet are still harmful activities conducted as part of the wider pattern of coercive control. Behaviours that fall within the CMA are predominantly hacking related (S.1 and S.2), with email and social media accounts targeted the most, however, bank accounts have also been identified.

The assessment of media cases identified a wide range of ways in which technology was used to facilitate and perpetrate abuse during or after intimate relationships and within family relationships. In full the team identified the following types of technology-facilitated abuse, only some of which are covered by the Computer Misuse Act:

- Unauthorised access to accounts, devices, systems etc.
- Installation of spyware for hacking, tracking applications etc.
- Using fake accounts to monitor, communicate with or harass/shame victim or associated persons.
- Impersonating the victim, either through fake accounts or through unauthorised access.
- Disclosing sensitive images/videos.
- Installing tracking devices.
- Installing covert cameras/listening devices.
- Use of drones to monitor/harass persons.
- Excessive and abusive mass communication through text, email, messaging, websites etc.

Some of these behaviours alone are offences, some are not. For example, unauthorised access to an account would be an offence under the Computer Misuse Act but setting up a fake account is not. However, some of the abuses above, taken in the context of the wider range of behaviours by the offender, can lead to them being sanctioned under legislation related to coercive control, stalking and harassment etc. The legislative coverage of such behaviours will be considered later.

In the sample of cases assessed the number of cases by type of abuse are listed below in Table 6. It shows that unauthorised access was the most common form of abuse found. Next was impersonation of the victim, followed by fake accounts and disclosing images – with these combinations often happening together. Tracking and covert devices, as well as spyware, were less commonly found in the sample.

Table 6. Most common technological abuses in media case sample

Type of abuse	N
Unauthorised access	83

Impersonation of victim	40
Fake accounts	36
Disclosing images	35
Tracking	20
Covert devices	19
Unauthorised access and spyware	11
Drones	2

Notes:

1. Number exceeds 146 as frequently multiple abuses were pursued in the same case.
2. Excessive communication was not noted as a separate category but was found in many of the above cases.

Many of the cases alluded to multiple acts of technological and other abuse. In some cases, the technological aspects were the only or most significant part, in some cases there were multiple types of abuse occurring, some of which were not technology related. In some cases, there was much wider abuse, but technology was only a small part. This was frequently the case in controlling and coercive relationships where the technological abuse was dwarfed by the threats, physical and sexual abuse the victim experienced.

5.1. Unauthorised access

The use of unauthorised access as a tool in technological abuse was the most common in the media cases sample. The target of the access, the way it was secured and its role in the wider abuse did vary significantly and these will now be explored.

Below are the different types of accounts and devices that perpetrators secured unauthorised access to. As in some cases multiple accounts and devices were targeted it totals more than 83.

- Social media, Facebook, Instagram, Snapchat, Twitter, Tinder, Whatsapp: 48
- Email: 20
- Mobile phone, laptop, PC: 17
- Smart device: virtual assistant, heating, lights, blinds, music, CCTV, doorbell: 5
- Bank account: 4
- Cloud: Apple, Dropbox: 3
- Work database: 2
- Telephone system: 1

The list shows that social media accounts were the most common target. Given that social media has become one of the most ubiquitous means for people to communicate this is not surprising. Email was next in popularity, closely followed by mobile phone, laptop or PC. The hacking of smart devices such as virtual assistants like Alexa, heating systems, blinds etc., was rare in the sample. However, given such systems are not the norm in the UK this is probably not surprising. However, as they grow examples such as Box 2 may become more common.

Box 2

In a case from the USA a woman shared a house with her partner which had all the latest smart technology. In one particular strained period when he moved out he would wake her in the middle of the night by switching on and off music, televisions and lights (CBC, 2018).

In another example of a smart device being hacked one ex-boyfriend was able to monitor who was visiting his former boyfriend for months as he maintained access and used the remote doorbell "Ring" (The Information, 2018).

The lack of cases of bank accounts being hacked was surprising. This might reflect that such access is just not reported in the media or it could represent the greater security applied by financial institutions to access accounts compared to social media and email accounts. Many also had joint accounts meaning there would be no offence too. There were also a very small number of cases where cloud systems were hacked, such as Dropbox, and a couple of cases where offenders used privileged access to databases in the course of their work to secure information on partners/ex-partners or their new partners. Finally, there was one case of a telephone system that had been hacked (see Box 3).

Box 3

In one case from the USA after the breakup of a nine-year relationship during which the couple had established a successful restaurant, the ex-boyfriend, who had set up the IT and telephone system, hacked into the system and recorded a new voice message stating the restaurant was closed, resulting in a substantial loss of business. He was aware of all the passwords as he had set up the system and they hadn't been changed. He also emptied their joint account of funds among other issues (MailOnline, 2020a).

In the interviews, financial abuse was noted as being conducted, with perpetrators obstructing access to bank accounts or using payment details without authorisation, committing fraud and impersonating their partners for fiscal gains, as part of wider patterns of coercive and controlling behaviour. Perpetrators also access their partner's credit reports to determine what products are available to them, and which the perpetrator can then apply, whilst assuming their partner's identity.

Hacking into online banking is probably one of the most common issues that we see. So we do a lot of work with banks around this as well (Interviewee 1)

It's more the online banking side of things and having their cards stored on their phones to be able to buy things, that tends to be a bit more common (Interviewee 2)

It's fraud, doing online loans, perpetrators taking out loans in their client's names, things like that. So, we've recently had one where they were trying to facilitate an extension of a mortgage and because of COVID everything was done online, and had a phone call but couldn't clarify that person's ID, so luckily that was stopped because there was some weird things that the client had hold of (Interviewee 12)

They [victims] may be falsely accused of having affairs, of being abusive, you're lying to me, you're being abusive to me by not sharing that information, you are the abuser, and you're being financially abusive by not sharing money with me or not sharing finance details with me. They may then remove all of the money from that bank account to teach them a lesson, or withhold funds again to teach them a lesson; well, actually, if you're not responsible, you won't let me have this, you won't share the responsibility, then I will show you how this needs to work. So there'll be financial repercussions. They may be threatened with other actions, like if you can't give me extra money then you're not going to see the children or you won't be able to have money to put fuel in your car to get to work, or you're now responsible, I'm transferring all of the responsibility for the bills over to your bank account. So they'll start changing the names of direct debits or other stuff (Interviewee 9)

5.1.1. Means of unauthorised access

Table 7 below illustrates the means for unauthorised access where this was mentioned in the media report. It is important to note there were many cases where no mention was made of how access was secured. The vast majority of cases where it was noted, was by very low tech means. Most common was knowledge or access to accounts and devices. Many partners share devices using their login details on them (which may also be saved) or tell each other their passwords. Some know where partners keep lists of passwords. This is the most common means of access. For example, in one case, after her boyfriend ended the relationship, which she did not want, a woman wrote a long email to him. He did not respond, so she logged into his account – knowing his password – to see if he had read it. This led to her reading many other emails in his account (Bolde, 2020). In a similar case, after a breakup one ex-girlfriend regularly looked at her ex's emails to see what he was up to for several years, as he did not change his passwords which she knew (Grazia, 2019). Box 4 illustrates another example.

Box 4

A man from the South West of England, after splitting with his girlfriend, took over her social media and bank accounts, which he knew the passwords to. He then started impersonating her posting messages and explicit pictures and videos for several months driving the victim to the brink of suicide among other incidents (Devon News, 2020).

Table 7. Means of Unauthorised Access

Method	Number	%
Knowledge, access	21	41

Control, violence, threat	17	33
Spyware	6	12
Guess	2	4
Hired expert	2	4
Theft	2	4
Partner's finger while asleep	1	2

N=51

The interviews highlighted that perpetrators are able to access their victims accounts through a range of different means. For example, perpetrators may easily guess passwords through intimate knowledge of their partner.

A lot of them [perpetrators] already know or can very easily guess passwords. If you've been with someone for like a couple of years or something, they're going to know roughly what your passwords are, unless you're someone who is really vigilant about it. But I don't think many people are, you trust whoever you're in a relationship with don't you. So it ends up being like your pet's name with a couple of numbers after it. And it's quite easy to guess really. Once that's known, it's really easy to get in, so just stuff like that (Interviewee 4)

Passwords are often manipulated out of victims during the relationship where they are emotionally blackmailed into providing them in a bid to prove their love and trustworthiness:

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? So then that person is brainwashed really and coerced into agreeing to allowing that person to have access to their bank accounts, maybe to their payslips. So the majority of people now don't have a printed off payslip, they have an electronic account or an electronic notification of their earnings. The same with things like benefits and that type of stuff. So the majority of things, whether that's your PayPal account or whatever it is you may have, not just financially but also other electronic accounts that you might have are accessible by a password and perpetrators are very good at trying to justify or give reasoning as to why they should be able to access that, and actually you're being unreasonable then by not allowing them to, so you must have something to hide (Interviewee 9)

Perpetrators were also noted as linking email accounts, so if their partners changed a password, they would receive a notification. Additionally, shared social media profiles were common in coercive and controlling contexts.

I think the biggest thing for me is when I see on social media people who have joint accounts where it says, I don't know, Sally and James Smith or something, for example, my alarm bells start ringing, because actually why is that happening and what are their reasons for having that joint social media account Surely you can have your own accounts. If you want to put in there that you're in a relationship or married or whatever that's absolutely fine, but for what reason are you sharing an account and who is posting for who? I received a message from a joint account once giving information about an abusive situation and I wasn't sure who was sending that. This was on a professional social media account that I had. It made me really cautious as to how I replied and was I actually replying to a genuine victim or was I replying

to a perpetrator who was trying to mask who they were? So that always rings alarm bells for me is if people have joint social media accounts (Interviewee 9)

Simply guessing a password was reported in a couple of cases. Theft was another means and in one case an upset ex-boyfriend turned up at his ex-girlfriend's workplace to meet her and stole her phone, enabling him to access it and the accounts on it, and send an explicit video to friends and family (Echo, 2020). In another case the former partner broke into the house threatening the woman and left with her device (Belfast Live, 2021). The advent of biometric means to access devices has also not stopped some. In one case the partner would use his partner's thumb while asleep to open her phone so he could access her accounts (MailOnline, 2018a). There were also a couple of cases where the perpetrator hired experts to hack accounts. Reading accounts in the media, the authors also found in the chat under one online case, a person offering hacking services to persons.

The next most common means in the media case analysis was control, threats and actual violence to secure access. In some of the cases the victim was involved or had been involved with a coercive and controlling partner who pursued that through a variety of methods ranging from psychological, threats of violence through to actual violence. In some cases, when asked, victims simply handed over devices with accounts open or gave them the passwords or PINs to enable them to access. An example typical of many, was a man convicted of coercive control in Kent who through demands and violence took over his partner's life including her Facebook and bank accounts. Refusals or attempts to leave were met with threats or actual violence (Kent Online, 2020).

Interviewee 9 also described how perpetrators have been able to obtain passwords from service providers by claiming that they are victims of domestic abuse:

So they've [perpetrator] phoned a service provider and said actually, I really need to access this, I'm a victim of domestic abuse and I don't know the passwords and I just need this to be reset and they would believe them and the password was reset so that then they could take over that account. So that's manipulating the services too (Interviewee 9)

In the interviews, victim's email accounts were noted as a primary target for unauthorised access due to the wealth of information available within them:

Predominantly, they try to get through to the email, because when they hack the email and take over that, that gives them access to every other account (Interviewee 1)

Perpetrators are also using spyware in order to gain the knowledge required to access their partners or ex-partners accounts, but also to monitor their movements. Spyware apps, which abusers install on their victim's devices to covertly monitor their communications, location and other information, are among the most concerning tools used in domestic abuse (Dimond et. al, 2011; Freed et.al, 2017). Defining spyware is contentious because whilst some apps are clearly branded to enable surreptitious surveillance such as *'Flexispy, Wife Spy, Girlfriend Spy, Spyera, and ePhoneTracker'* (Levy, 2014), other seemingly innocent apps such as *GPS and Find My Phone apps* (Maher et al., 2017) can also be exploited by abusers to engage in IPS. Chatterjee et.al (2018) refer to these as 'dual-use' apps because although they have been designed for a legitimate purpose such as child or anti-theft protection they are easily repurposed to spy on a partner, as their functionality allows another person remote access to a device's sensors or data, without the knowledge of the owner of the device. Both overt spyware and dual-use apps are harmful in domestic abuse contexts.

Spyware was mentioned in only six media cases. In most of these cases it was also deployed in relatively simple ways. For example, in some cases the partner gave the other a gift of a mobile

phone, which was preloaded with spyware. Some cases involved the partner having access to devices which they were able to place spyware on. In one unusual case a woman forgot to make a payment and when she returned home apologised to her husband only to be told he had taken care of it as he had installed spyware on her phone without her knowledge, to monitor her movements and read her communications, hence he knew she had not made the payment. She was initially angry but then actually embraced the idea (Mirror, 2015). There were few mentions of what software/apps were used in reports, but the few that did listed: *Cerberus monitoring app*, *eBlaster*, and *Find My Friend*.

Hacking or accessing victim’s social media accounts is a common tactic of perpetrators, with Facebook, Instagram and WhatsApp noted targeted platforms, in the interviews, and prevalent in the Google search predictions. In order to explore guidance online for hacking into Facebook accounts, we used the queries given in Table 8 (this essentially allows us to follow the actions that would be likely taken by a perpetrator searching for abuse methods online). Execution of those queries led to 13 unique unvisited websites where we extracted 49 recommendations. Recommendations refers to the actions that sites suggest persons use to conduct their potentially abusive actions.

Table 8: Queries for Facebook

Initial Queries	Google’s search predictions
How to hack my girlfriend’s/boyfirend’s/wife’s/husband’s Facebook’s account	how to log into someone's facebook messenger without them getting a notification

Following apps were recommended;

- Highster Mobile
- mSpy
- Spyera
- uMobix
- Phonty
- NEXSPY
- FlexiSpy
- SpyFone

Using keyloggers to learn credentials is another way given to access Facebook activities. Both the software keyloggers and hardware keyloggers were mentioned as a solution. In addition, a website, *Hyper-Cracker*, is given as a spying tool which claims to hack a Facebook account after entering the target’s Facebook ID.

Other solutions are mainly around resetting passwords which can be done via accessing the email of the victim. For the cases where it is not possible to access email of the victim, following steps are suggested:

“...Next, select “Forgot your password? and type in their email. Select the option tagged: “This is my account.” Facebook will give the option of resetting the password via your target’s email. However, this will only alert them that someone is trying to access their account, and you don’t want that. To avoid getting caught, select the option: “No longer have access to these?” instead.

Once you have done this, you will see a bar titled: “How can we reach you?” Fill your own email address into the blank field provided. However, you have to make sure that the email address isn’t linked to any Facebook account. If you don’t have an email address that isn’t linked to a Facebook account, create a new one.

Once you have provided an email address, Facebook will ask you a secret question. This part is easy if the victim is your child, partner, or a close friend. However, if you don’t know so much about them, you can always try to guess the answer to the question. If you get the answer to the secret question right, you can then reset the password. However, you will need to wait 24 hours before you can log into the account.

If you have no idea about the answer to the secret question, click on the option tagged: “Recover your account with help from friends.” Once you do this, Facebook will let you choose between three and five friends. It then sends passwords/codes to them, which you could ask for and fill into the next page. You could decide to choose between three and five friends who would be willing to send you the codes. However, if you don’t trust anyone to send you the codes without snitching, you may decide to create about three fake accounts beforehand and send your victim a friend request. This way, you can select the fake accounts and have Facebook send the codes to them.”²³

This recommendation highlights the risks of Facebook’s “trusted contacts” strategy designed for the ones who get locked out of their account.²⁴

Performing brute force or the Man-in-the-Middle attacks, SS7 Vulnerability, hiring hackers or performing phishing attacks by creating a fake login page and sending the link to the victim are the options given that require more technical capabilities. For the ones for whom those techniques are complicated, a simple guidance is given regarding guessing passwords where the following items are given as popular weak password combinations:

- Name + date of birth
- Name + year of birth
- 123456789
- 987654321
- Kids’ names
- Significant others’ names
- Anniversary dates
- Pet names
- Other meaningful information/cell phone number/numbers/dates/names

The following way to impersonate a legitimate person who works for Facebook is another particular recommendation given for spying on Facebook accounts:

- “1. Think of a legitimate organization that you’d like to impersonate – in this case, Facebook.*
- 2. Create a fake website with a similar domain name. For example, facebook.com, facebooknetwork.com, or something else that is as similar to the original as possible.*
- 3. Create an email address using the website domain.*

²³

<https://application-partners.com/facebook/how-to-view-someones-facebook-messages-without-knowing-their-password/>, April 2021

²⁴ <https://www.facebook.com/help/204495386254288>, May 2021

4. Find a legitimate person who works at Facebook through LinkedIn and use their name when creating the email address. The website must look legit, and your email account has to have a signature and a Facebook logo.
5. Find the victim's email address and write an email that is titled something along the lines of "Your Facebook account has been hacked," or "Your Facebook account needs URGENT assistance." The whole goal is to make the email seem urgent, to entice the victim into clicking the link to your website.
6. Tell them that they need to log into their account through your link for further assistance.
7. Once they do, you will receive their email address and password."²⁵

Searching for the queries given in Table 9, we extracted 41 recommendations for hacking Instagram accounts out of 18 websites.

Table 9. Queries for Instagram

Initial Queries	Google's search predictions
How to hack my girlfriend's/boyfirend's/wife's/husband's Facebook's account	how to log into someone's facebook messenger without them getting a notification

Similar to our findings for Facebook, majority the apps recommended for spying on Instagram accounts were stalkerware that were covered in the previous section:

- TheTruthSpy
- Spyier
- mSpy
- Spyzie
- FlexiSpy
- Highster Mobile
- KidsGuard
- NexSpy

We identified some new apps that are dedicated to hack Instagram accounts;

- IGHack
- Instaripper
- ArroApp
- Instagram Hacker²⁶ collects the credentials

Those apps' websites, however, looked fraudulent. Instagram Hacker, for instance, asks users to follow some steps which require them to enter their credentials. In addition to the apps, there are websites that claim to be used to hack Instagram accounts. Those websites also seemed fraudulent with a single "start hacking" buttons on their main pages. We also identified two software with the same purposes.

Table 10. Website for hacking Instagram accounts

²⁵ <https://celltrackingapps.com/spy-on-someones-facebook/>, May 2021

²⁶ <https://chrome.google.com/webstore/detail/instagram-hacker/eoanbdkiclbphojpagififelggplocan> May 2021

Tool	Name	Data collected
Website	instaportal ²⁷	UNKNOWN (broken link)
	instahacker ²⁸	UNKNOWN
	instaentry ²⁹	UNKNOWN
	PIRATERCOMPTEINSTAGRAMGRATUIT.COM ³⁰	User name
	Instahax0r ³¹	UNKNOWN
	aa ³²	UNKNOWN
	InstaLeak ³³	UNKNOWN
Software	Password revelator ³⁴	UNKNOWN
	InstaInsane ³⁵	UNKNOWN

Using hidden cameras to see credentials was the only recommendation which includes use of a device for spying on Instagram accounts. Some techniques which require cyber skills were also present including Man-in-the-middle attacks or phishing attacks via creation of a fake Instagram login page and sending it to victims. Some other techniques that do not require cyber skills were given as resetting passwords (accessing the email account of the user) or guessing them where 12345, ABCD, Password, Qwerty were given as common passwords.

Among the types of technology misuse that target digital identity of the individuals, we extracted the maximum number of recommendations for WhatsApp messages. Execution of the queries below returned 59 unvisited web pages out of which we extracted 126 recommendations.

Table 11. Queries for WhatsApp

Initial Queries	Google's search predictions
How to hack my girlfriend's/boyfirend's/wife's/husband's Whatsapp?	how to check my husband whatsapp, can we hack whatsapp without victim mobile, how to read someones whatsapp messages without their phone 2019, how to read

²⁷ <https://www.instaportal.net/>, April 2021

²⁸ <https://instahacker.org/>, April 2021

²⁹ <https://www.instaentry.net/>, April 2021

³⁰ <https://www.piratercompinstagramgratuit.com/en/>, April 2021

³¹ <https://www.instahax0r.com/>, April 2021

³² https://s3.amazonaws.com/external_clips/3715389/hack_instagram_account_2021_hack_insta.pdf, April 2021

³³ <https://instaleak.net/>, 19 April 2021

³⁴ <https://www.passwordrevelator.net/>, April 2021

³⁵

<https://null-byte.wonderhowto.com/forum/to-crack-instagram-passwords-using-instainsane-0194711/>, April 2021

	whatsapp messages from another device, how to hack someone whatsapp using chrome, how to spy on whatsapp messages without target phone, how to hack someone whatsapp using python
--	---

There were 39 apps recommended for monitoring WhatsApp activities; a majority of which can be classified as stalkerware.

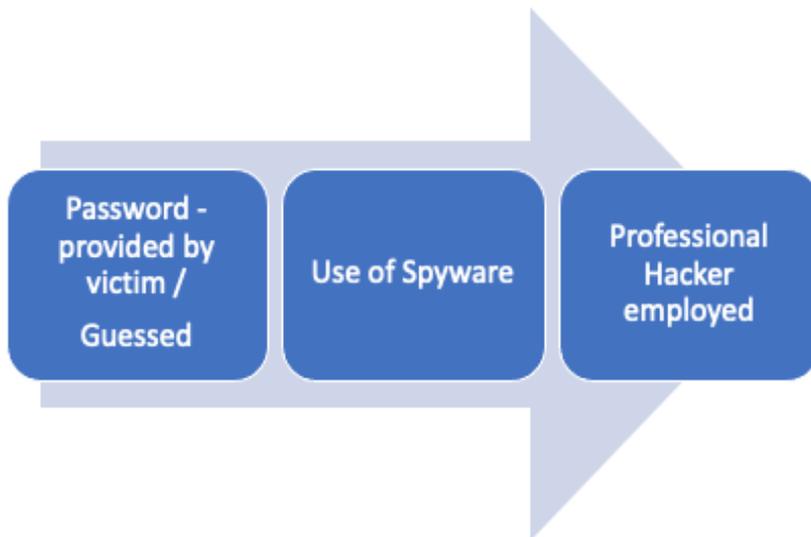
Table 12. Apps for hacking WhatsApp

Names		
Auto Forward	JJSpy	PullOutCorrWhatsApp
Cocospy	Join	SpyActivity
Dr Fone	KidsGuard	Spyera
EvaSpy	KidsPro	SpyFone
Flexispy	Minspy	Spyic
FoneMonitor	Mobile Spy	Spyier
FreePhoneSpy	Mobistealth	Spyine
FreeTracking	MoniMaster	spylive360
GuestSpy	mSpy	SpyMaster Pro
Highster mobile	Neatspy	TheTruthApp
Hoverwatch	NexSpy	TheTruthSpy
iKeyMonitor	OwnSpy	WhatsApp - BlueMesCrack 2.0
iMyFone	Phonty	WhatsApp Scan Pro

WhatsApp Web is the most popular recommendation as already reported before. In addition, WhatsApp's "Export chat" and backup on Google Drive functions are also misused to access messages of the victims. Highly technical strategies given for the same purposes include use of keyloggers and a phishing software, QRJacking, which requests QR code to be used for WhatsApp Web. MAC spoofing, phishing attacks via sending fake WhatsApp login links and sending OTP (one-time-password) which can work if Two-Factor Authentication is disabled are the other options provided for perpetrators with technical capabilities.

Where perpetrators are unsuccessful in their previous attempts to access their partners or ex-partner's accounts, whether from having the password, or by utilising spyware, they can then enlist the help of 'professional' hackers - technically proficient friends/associates or persons who advertise their services online. Figure 7. shows the methods taken by perpetrators in order to have unauthorised access to their partner or ex-partner's accounts.

Figure 7 . Methods used to procure unauthorised access to partner or ex-partner's accounts



5.2. Fake Accounts

The use of fake accounts is a significant method used in abusive relationships. It was the second most common tactic in the media analysis, with 36 cases found involving this. The fake accounts can be fictitious persons, real persons who are known to the victim or impersonating the victim themselves. Box 5 below provides a mix of real cases involving fake accounts. They are used in a wide variety of means, which will be illustrated below.

Covert surveillance – the offender sets up a fake account to enable them to follow them, by friending their victim, which if they used their real account, would probably be blocked from doing so or are perhaps even banned from doing so.

Communication – a common motivation is to use the account to communicate with the victim or associates of them, which would not be possible with their own accounts. The purpose of the communication might be simply to want to engage with the person. It is common for this to occur in relationships which have ended, and the ex no longer wishes to communicate and reconciliation has been sought. Communication such as emails and messaging might also be used via false accounts to distribute intimate images of the victim for more revengeful acts. It might be used to simply send abusive messages to the victim. It can also be to frighten the victim or test them. For example, in one case a man set up a fake account to stalk his partner, where he would send her abusive and threatening messages. She became so scared she slept with a knife under her pillow (WalesOnline, 2020).

Impersonate the victim – fake accounts can also be used to impersonate the victim via actual accounts or messaging. Many perpetrators do not have the skills or knowledge to hack the victim's account, so this is a simpler means. It is also a greyer area legally. Hacking a person's account is a clear criminal offence, creating a fake account impersonating someone is not. Although used with other activities it can then form the basis of offences under stalking/harassment, malicious communication etc. Impersonation of the victim is commonly used to try and shame them, such as publishing intimate images (as discussed above) or to facilitate harassment. In some cases, the victim was impersonated in order to create abuse by them, which could then be used to report to official agencies as a means of revenge or some other motive. In another case the female victim's images were used on a dating website to enable the male partner to engage in sexual talk with men.

Impersonate another: sometimes offenders impersonate persons other than their victims to facilitate their aims. This might be the new lover in the ex's life or some other person. For example, in one

case the daughter of UK comedian Lenny Henry impersonated him with a fake account offering her ex-partner loans to try and lure him back into a relationship (BBC News, 2020a). Other examples of fake accounts are provided below.

Box 5

A man who had been convicted of coercive control of his former partner and banned from communicating with her, after release from prison, attempted to contact her using multiple fake accounts (LeicestershireLive, 2020).

A woman who had a restraining order against her regarding contact with her ex used numerous fake accounts to contact him/her to abuse and threaten him/her (gender not identified in article) (LancsLive, 2020).

A woman set up a fake account purporting to be her ex which she used to send abusive messages to herself, which she then reported to the police to try and discredit him, among other acts (SomersetLive, 2018).

One man after his girlfriend left him he set up accounts on swingers and dating accounts in her name and with her workplace listed to discredit her (Echo, 2021b).

An ex boyfriend set up fake accounts on Grindr in the name of his ex with various falsehoods, resulting in over 1000 men turning up at his house and work looking for sex (OutSmart, 2017).

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).

An American state level politician used his girlfriend's images, both during and after the relationship ended, to set up a dating website profile which he then used to engage in explicit sexual chat with men (PinkNews, 2018).

Fake accounts were discussed in the interviews. Domestic abuse service providers expressed their frustration about how perpetrators are able to continually create falsified profiles without any criminal sanctions to deter them. 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 have been set up on dating sites, Interviewee 7 highlighted that the victim is not only dealing with the false representations of herself she is also having to contend with other men trying to talk to her and contacting her on WhatsApp or text, because her mobile phone number has also been publicly divulged. Fake profiles are also used to try and re engage with partners after separation has occurred, whilst during ongoing relationships, perpetrators also use them to try and prove if their partner will cheat or to prove that their partner was cheating all along.

5.3. Online Harassment

Perpetrators are also engaging in behaviours that could contravene the MCA, such as posting harassing and derogatory content about their victim on social media. Often this is not undertaken from the perpetrator's own accounts, rather anonymous profiles have been created in order to perpetuate the abuse. In some cases, perpetrators have hacked into their victim's social media

account and posted content from there, which presents the victim in a pejorative way, potentially alienating them from friends and family, who can then become embroiled in the facilitation of the abuse. Perpetrators have also signed their victims up to hate groups to embroil them in criminal activity. On other occasions, perpetrators have created fake profiles of their victims, which in itself is not a criminal act, however this is usually undertaken with a view to humiliate or disparage the victim and can lead to other acts that are illegal, such as the posting of intimate images of the victim.

Repeated messages, just kind of like constant harassment through different messages and different media accounts, so Facebook, Instagram, the whole lot of the social media platforms now that are easier to access. And create lots of...some perps will create lots of fake accounts in order to gain access when they've been blocked by certain people. I mean, other peoples' accounts will be used by perpetrators to get in touch with some people, or they'll just keep creating fake accounts and harassing the ladies until they get, you know...I suppose pretending to be friends of friends or putting fake contact request through, creating fake profiles that they're not themselves but somebody else just to try and act as if they're a friend to contact them sort of thing (Interviewee 13)

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)

5.4. Stalking and Installing Trackers

Many of the methods undertaken by domestic abuse perpetrators involve stalking and controlling their victims, with technology providing easy and accessible means to further this form of abuse. Location apps that serve a legitimate purpose, such as *Find my phone*, are being utilised to monitor activities for obnoxious reasons, often without the knowledge of victims. Stalkers also draw on geo-location on social media as the following quotation highlights:

For instance, apps that you have that people don't always necessarily think of, like your locations on things like Snapchat. So unless you turn that off people can see whereabouts you're located and could stalk you on there. When people do their updates on social media about where they're going and tagging themselves in places, people can know those places then and things like that. So we have a lot of issues there. And obviously hacking into emails to see what they're doing.We had a case recently where an offender got hold of their ex partner's phone by breaking into their property, saw an email saying that they were going on holiday, that client ended up taking our advice and not going on that holiday which was within the UK. This was last year. The offender did turn up there (Interviewee 12)

Perpetrators are also tracking victims by installing software on their phones, without their knowledge:

I've had a case recently where one of my clients, their ex-partner had put software on my client's phone and he was tracking her this way. And she just couldn't work it out, he was turning up while she was walking down the road, while she was in...places that he just wouldn't know. And she'd say, she'd be driving and then he'd be driving next to her (Interviewee 7)

In this instance the interviewee highlights how victims can be manipulated into having trackers put on their devices for 'safety' reasons:

I know I've got one client at the moment who 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 (Interviewee 3)

Combining activities that may not be illegal but also depending on the context could come within both the CMA and the MCA, as well as the PHA or SPA (if a relationship has ended) as perpetrators subject their victims to a barrage of communication, including texts, emails, social media messages and posts. They might also have hacked into accounts, spyware or physical trackers to be able to follow their victim's every movement. This enables them to pursue their victim physically but also maintain an omni-present control over everything their victim does.

It's coercive control, the stalking element and the harassment I tend to find is where primarily the technology is being misused and abused against victims... Phone tracking is an absolute common one. I've got experiences, multiple experiences, of women having their mobile phones cloned... The obvious other ones that we have a lot of experience with, trackers; trackers on phones, trackers on cars. I've had women put their cars into garages two or three times, and the trackers have been so far, like, embedded in car engines, things like that. So their every movement obviously is recorded (Interviewee 6)

Things like tracking, GPS tracking, hidden cameras, accessing devices. So I know previously when I was in a frontline supporting role when I suppose iPads and iPhones were fairly new that somebody I was working with, their ex-partner had activated the camera and the microphone on an iPad that was in her home, well the place that she'd fled to, and that obviously enabled that person to record what she was saying, what she was doing and that type of stuff. I think it was probably the first instance of tech abuse that I became aware of where I thought crikey, I need to be a little bit more vigilant when I'm talking to somebody or I'm offering them advice. Since then obviously it's happened a lot more (Interviewee 9)

Box 6 further illustrates the combination of stalking and harassment behaviours using digital technologies, and how these can be used to circumnavigate the criminal justice system (CJS).

Box 6

On the day of her marriage, a woman was told by her husband that he now "owned her." She then found out that she had two restraining orders against previous victims and had served a suspended sentence for being violent against a former partner. Throughout the relationship the victim was subjected to coercive and controlling behaviour, as well as physical violence.

Upon ending the relationship, the woman secured two non-molestation orders against her ex-husband. He was able to navigate these by including her in group WhatsApp messages, which he claimed were sent in error. He would constantly look at her other online accounts, such as LinkedIn, so she would be aware of his presence. He also placed a tracker on to her

The media cases also highlighted the use of trackers to monitor the movements of partners/ex-partners. In some of these cases it involved triggering existing software on mobile phones that enables such activities to occur, some offenders downloaded software to enable this, and, in some cases, physical vehicle trackers were attached to cars. Such software and devices enable the offender to monitor very accurately the location of the victim. Placing software on a person's mobile phone without their permission would clearly be an offence under the Computer Misuse Act. This is not as clear when it comes to placing physical tracking devices to another person's car. There is not a clear criminal offence, although combined with other behaviours could be dealt with under the stalking and harassment legislation or coercive control, which is where examples in this sample were derived from.

The eight cases that involved trackers were all perpetrated by men. In one case from Australia a woman sought help from an ex-boyfriend in purchasing a Land Rover. He helped but also downloaded software which could enable him to track her movements. The app he placed on the car would also enable him to take control of the car, stopping and starting it (ABC News, 2020). The offender pleaded guilty to stalking, which included this and other incidents. The other cases of vehicle tracking were less sophisticated involving the attachment of physical devices to cars. In one example from Somerset a husband thought his wife was having an affair so installed a tracker device on her car and a covert camera in the television at home. He also accessed her email and sent messages from her Facebook account to the person he thought she was having an affair with. He was found guilty of stalking (Somerset Live, 2017).

5.5. Image-based Sexual Abuse

Domestic abuse perpetrators are also engaging in so-called revenge pornography, or what is more accurately termed image-based sexual abuse (McGlynn & Rackley, 2016). This can involve situations where perpetrators threaten to release intimate pictures or videos in order to retain control over their victim. Currently, this would not be an offence under the CJCA, however within the forthcoming Domestic Abuse bill, the legislation targeting revenge porn will also be expanded to include threats to disclose intimate images with the intention to cause distress. In other instances, perpetrators, in setting up fake social media profiles of their victims, have used these to disseminate indecent images of their victims. Other means of distributing these materials have been to send them directly to friends, family, and employers, as well as publishing them publicly online.

So people, you know, if someone sends intimate photos and then they're posted online or any videos or anything or posting any kind of personal information online so that other

people can see. Any kind of threatening behaviour. And even – well, even with the physical abuse side of things, like documenting these photos and putting them up into public places without anyone’s consent or doing it in a really nasty way with nasty, malicious intent. Getting family and friends involved and publicising things that aren’t wanted by both parties (Interviewee 2)

Some cases of image-based sexual abuse involve the creation of fake profiles and digitally altered pictures:

We get a lot of cases where there are threats to share images or they have shared images. I’ve had cases where the victim wasn’t sure if the perpetrator had videos or pictures, at all, because she wasn’t aware of them being taken. But there have been threats around that, so there’s been a lot of perpetrators taking pictures, not telling victims, and then threatening to release them if they don’t do certain things. And I’ve also had a recent client, actually, where she has no idea who’s doing it, but they are creating profiles on porn websites of her, and sharing. So, none of the pictures are explicit, but they’re, kind of, like, photo-shopping pictures of penises and stuff on her, and they’re also sharing all of her contact details and where she lives (Interviewee 7)

In one media case of image-based sexual abuse, a man had secretly recorded him and his girlfriend having sex. When the relationship ended, he engaged in a campaign of harassment which included many acts, culminating in publicising and sending the video of them having sex he had secretly recorded (Cheshire Live, 2020). In another example a husband thought his wife was having an affair so installed listening devices behind the television and in her car, among other activities. The relationship ended and he moved out and continued to use them to monitor her, among other stalking activities (MailOnline, 2020b).

The media review excluded the most basic forms of this crime from the case analysis i.e. where both parties agree to take pictures or record video and then one party releases those images or recordings on their own account without the permission of the other. However, there were many other cases which involved other technological aspects, which warranted inclusion and 35 cases were found involving the disclosure of images. These fell into the following categories with the number of cases found next to each (note some involved both, so numbers exceed 35).

- Hacking of another person’s account to secure images/footage which is then released or to publicise images held - 17
- Creation of fake accounts to publicise images/footage -15
- Use of covert camera to record images/footage which is then publicised - 4

Some of these examples will now be explored, beginning with those that involved unauthorised access, which broadly fell into two categories: unauthorised access to secure images or unauthorised access to share images. In an example of the first, a woman received a tip her partner was not faithful so accessed his phone and found he was using gay dating sites. She obtained the naked pictures he used, including those of his penis and screenshots of his sex chat and published them on her Facebook account (The News, 2021). In an example of the second type the perpetrator used the victim’s account to share intimate images. For example, in one case from Liverpool an ex-boyfriend hacked his former partner’s Instagram and Snapchat accounts and shared images of them engaging in sexual activity. He also changed the passwords so she could not get into the accounts to take them down (Echo, 2021a). Both hacking to secure images and then using the victim’s account can also be used, although no cases of this were found.

Another common means is the use of fake accounts to publicise images. These can be fake accounts that are purported to be the victim or a close associate of them, or a seemingly unconnected person. For example, in one case from Plymouth a woman set up a fake Facebook account to send images of her former boyfriend's penis to friends and work colleagues (Mirror, 2019). Such behaviours can be more expansive than the creation of a simple social media/email account to communicate with specific targeted persons close to the victim. For example, in one case a man set up an Instagram account of his ex with intimate pictures of her on it, which were also recorded without her knowledge or permission (East London and Essex Guardian, 2017). Other cases were illustrated above of the use of covert devices in this type of behaviour too.

6. Tools of Technology-Facilitated Domestic Abuse

Abuse involves common technologies, not just purpose-built spyware. Our findings revealed technologies targeting the physical identity of individuals (voice, image, location); technologies that target digital data (whatsapp messages, app usage, existence on dating sites etc.); and finally, the

ones which target both physical and digital identities of individuals. Stalkerware and parental monitoring apps belong to the third group whose monitoring capabilities are efficient to abuse both digital and physical worlds of the victims. Identical devices, applications and behaviours can be both used to abuse and protect. Everyday mainstream devices and services are most commonly used to perpetrate abuse. Context is significant in establishing TFDA in personal, intimate and familial contexts, distinct from healthy relationships and interactions.

6.1. Physical covert devices

A form of technological abuse is the use of covert devices. Technology has advanced the ability for a much wider availability of covert devices, which were once the preserve of spies. First, mobile phones can be used to record conversations and video activities (either by being covertly placed to do so or recording communications secretly). Second, there are ordinary CCTV systems which can be deployed domestically and used as part of abuse. Finally, there are a wide array of gadgets, which can now be easily purchased in specialist shops and online that enable both audio and video recording. Some of these gadgets are disguised such that only experts or the inquisitive would spot, such as cameras hidden in smoke alarms, clocks and plug sockets. Twenty years ago, such devices would have been hard to get hold of and expensive, but now they are cheap and a click away on outlets such as Amazon. The legality of these devices is also complicated. If a person is using them in their own home, in most cases this would not be illegal. If they no longer live there or never have, an offence is clearer and even more so if recordings from such covert devices are published.

There were only five cases in the media sample where covert listening devices (bugs) were used – one case in a TV, another in a car, fake smoke detectors, and plug sockets. Sometimes these were used alongside CCTV (covert and non-covert). Covert cameras were more common. There were 19 media cases overall where covert devices were used, but as well as CCTV related, perpetrators could also be placing a phone on record in a hidden place.

6.1.1. GPS trackers

In order to explore the GPS Trackers available on the web, we used the query “Devices to monitor partners children” and included the ones predicted by Google (see Table 13).

Table 13. Queries for GPS Trackers

Initial Query	Google’s search predictions
Devices to monitor partners children	child tracking device hidden, child tracking device hidden uk, gps tracker for autistic child uk, best gps tracker for kids, gps child tracking pendant, personal gps tracker

Those queries returned 72 unique websites and we extracted 292 recommendations reviewing the main page of them. Among the recommendations, the majority of them (217 out of 292) were tracking devices. There was only one website (<https://helpmobi.io/en>) which claimed to allow persons to track targeted individuals via a provided phone number. Finally, we extracted 74 app recommendations about 39 unique apps in total. Unsurprisingly the data primarily targeted in this group of technology was GPS data. However, apps which can function as GPS trackers can also provide several other information as summarised in the Stalkerware section.

Table 14. Apps for GPS Tracking

	FoneMonitor	Qustodio
--	-------------	----------

BrickHouse Phone Tracker App		
Aispyer	FoneTracker	Securafone
All Tracker Family App	FreePhoneSpy	SpyEra
Auto Forward	GEO TRACKS	SpyHuman
Avocado	Highster Mobile	SpyMug
Cocospy	Hoverwatch	Spyzie
Couple Tracker App	KidsGuard Pro	SurePoint Spy
CoupleMonitor	Life360	TeenSafe
couples monitor device tracker	mCouple	TheSpyBubble
Family locator	MoniMaster	TheTruthSpy
Family Tracker	mSpy	uboro Tracker
Find My Friends	PathShare	Web Watcher
Flexispy	PhoneSheriff	XySpy

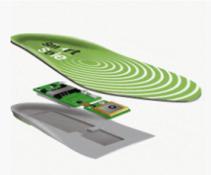
GPS trackers can be advertised in a manipulative way. For instance, PathShare is mentioned on a website as follows;

“The application assists you in enhancing the trust level in your relationship. This happens when your partner decides to install PathShare. If your dear one did not agree to install it, it could be an intrusion of privacy. So, if you are looking for apps for couples with trust issues, then you need to try this one. Furthermore, it tracks your spouse’s honest level. It offers updates on your partner’s safety level. The application also empowers your loved ones and you for spilling up one another’s location. Remember that PathShare works only when your partner allows tracking of their location.”³⁶

Similar to the other technologies, GPS tracking devices available on the web can be divided into legitimate ones which are generally not hidden and used for kids, pets or older people, and the others which are used for stalking. Their cost ranges from £49 to £299 pounds depending on their battery life. It is also possible to categorise this group of technology as the ones used for people and the ones attached to vehicles.

Table 15. Devices for GPS Tracking

³⁶ <https://www.fonetips.com/apps-for-couples-with-trust-issues/>, May 2021

Examples of hidden trackers	 <p>37</p>	 <p>38</p>	 <p>39</p>
Examples of not hidden trackers			

With the aim of exploring the options that can easily be accessed via well-known and universal online sellers, we listed the links Google returned from those platforms (accessed in April 2021). Even though the majority of those products are not advertised for illegitimate purposes, the variety of them and their ease of access are still worrying. Besides, Amazon and Ebay also provide products which are targeted to be used on “cheaters.” Here, it is important to note that we did not execute searches on these platforms and the list given below only includes the ones returned by Google during our searches.

Table 16. Online Sellers for GPS Trackers

Online Seller	Links
	https://www.alibaba.com/showroom/hidden-gps-tracker-for-kids.html

Alibaba

³⁷ <https://www.wearable.com/wearable-tech/the-best-kids-trackers>, April 2021

³⁸ <http://www.possum.co.uk/products/smart-sole/>, April 2021

³⁹

https://www.amazon.co.uk/dp/B08T7C1KW6/ref=as_li_ss_tl?SubscriptionId=AKIAJO7E5OLQ67NVPFZA&ascu_btag=501647360-311-2017352469.1619002021&tag=best_reviews_uk_1-21, April 2021

	https://www.alibaba.com/showroom/mini-gps-tracker-child-tracking-pendant.html
Aliexpress	https://www.aliexpress.com/w/wholesale-hidden-gps-tracker-for-kids.html
Amazon	https://www.amazon.co.uk/AngelSense-Dementia-Nationwide-Speakerphone-Auto-Answer/dp/B08211HC64
	https://www.amazon.co.uk/Children-Positioning-Anti-Lost-Necklace-Tracking-Black/dp/B07LG671WV
	https://www.amazon.co.uk/Personal-GPS-Tracker/s?k=Personal+GPS+Tracker
	https://www.amazon.co.uk/Pueri-Tracker-Necklace-Positioning-Tracking-Blue/dp/B075KGS58T
	https://www.amazon.co.uk/s?k=best+gps+tracker+for+kids&adgrpid=118089481888&gclid=Cj0KCQiAst2BBhDJARIsAGo2ldU1YjYWHKyzqIlg_KSD3lIP4hHUPEHWu0Ee5-4q73IUIUOVIZFYJcgaAhDSEALw_wcB&hvadid=477096100035&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=e&hvrnd=9727722966849010769&hvtargid=kwd-32307675788&hydacr=4207_1795004&tag=googhydr-21&ref=pd_sl_7hpeg504w9_e
	https://www.amazon.co.uk/s?k=gps+child+tracker+bracelet&adgrpid=76205247285&gclid=EAlaIqobChMlvMGxz9yE7wIVj77tCh3EmwBkEAMyAIAAEgIyP_D_BwE&hvadid=381631432073&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=b&hvrnd=12757275601637624548&hvtargid=kwd-295008812067&hydacr=4208_1795006&tag=googhydr-21&ref=pd_sl_61ez9i1czc_b
	https://www.amazon.co.uk/s?k=kids+fitbit+with+gps&adgrpid=63416973250&gclid=Cj0KCQiAst2BBhDJARIsAGo2ldVOSUEWeBfxEblQPfxZPID8E7dDH9YUrNJKrVSwlpe4dlmvpJ3-c7EaArSSEALw_wcB&hvadid=338399628630&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=b&hvrnd=4587607489724245873&hvtargid=kwd-303521645510&hydacr=13251_1819383&tag=googhydr-21&ref=pd_sl_7fyk0sb546_b
	https://www.amazon.co.uk/Tracking-Device-Children/s?k=Tracking+Device+for+Children
	https://www.amazon.com/Cheater-Camera-Photo-Electronics/s?k=The+Cheater&rh=n%3A502394
	https://www.amazon.com/GPS-Bracelet-Kids/s?k=GPS+Bracelet+for+Kids
	https://www.amazon.com/GPS-Kid-Tracker/s?k=GPS+Kid+Tracker
https://www.amazon.com/Personal-GPS-Tracker/s?k=Personal+GPS+Tracker	
Ebay	https://www.ebay.co.uk/b/Car-Personal-GPS-Trackers/139838/bn_7114048185
	https://www.ebay.co.uk/b/Gps-Tracker/139838/bn_7023477420
	https://www.ebay.co.uk/c/1013439567
	https://www.ebay.co.uk/itm/Catch-Cheating-Spouse-w-NEW-iTrack-GPS-Tracker-Cheaters-Spy-Equipment-/163470874531
	https://www.ebay.co.uk/itm/Find-A-Cheating-Spouse-Easily-With-This-Tracking-Device-Track-Your-Husbands-Car-/152670136582
	https://www.ebay.co.uk/itm/Mini-Magnetic-GPS-Tracker-Locator-Spy-Track-Nano-Covert-Hidden-Pay-As-You-Go-UK-/322918047003
	https://www.ebay.com/p/1913441510

6.1.2. Covert Cameras

Covert cameras are other types of devices misused for covert surveillance and surreptitious recording of individuals. In this part of our analysis, we used “covert camera” as a query (due to overlapping results with Google’s predictions) and reviewed nine websites that were not visited before within our study. We extracted 151 products whose cost spanned from £23.98 to £550.80. The most remarkable finding at this stage is the variety of ways in which these devices can be hidden. Sunglasses, USB chargers, cups or water bottles are common examples (see Table 17 for others).

Table 17. Covert Cameras

Table 16: Covert Cameras

		
<p>Save £60.95</p>  <p>£249.00 £309.95 Lawmate HD Spy Headphones 1080p Camera with WiFi MicroSD Storage</p>	 <p>PIR Alarm Sensor With Built In Camera WiFi 50 days Battery Life</p>	 <p>USB Charger With Built In WiFi Camera</p>
 <p>Smoke Alarm WiFi Camera, 6 months Battery Life</p>	 <p>Wall Clock Camera Video Recorder</p>	 <p>Picture Frame WiFi Camera, 6 months Battery Life</p>
 <p>Router WiFi Camera</p>	 <p>Table Lamp Camera Video Recorder</p>	 <p>Pen Hidden Camera Video Recorder</p>
 <p>Coffee Cup Camera</p>	 <p>Keyfob With Built In Camera</p>	 <p>Sports Water Bottle with Built in Camera</p>

As done for the GPS trackers, we noted the links from well-known online sellers retrieved by Google (accessed in April 2021) for covert cameras. It is noteworthy that some products on these links are advertised as spy cams or nanny cams.

Table 18. Online Sellers for Covert Cameras

Online Seller	Links
Amazon	https://www.amazon.co.uk/Covert-CCTV-Camera/s?k=Covert+CCTV+Camera https://www.amazon.co.uk/s?k=covert+cameras&adgrpid=52942805477&gclid=CjwKCAjwmv-DBhAMEiwA7xYrd6f_XTUuVSH45PKUpHy0Hh_S3bDKftACHuDF64QduNzMKq5yleofMRoCDUMQAvD_BwE&hvadid=2

59046895723&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=e&hvrnd=224262794549722235&hvtar
 gid=kwd-45552021&hydadcr=28149_1752716&tag=googhydr-21&ref=pd_sl_l28pmhmsa_e

6.1.3. Covert Microphones

In this part of our analysis, we used “covert microphone” and the predictions of Google as queries (see Table 19 for the whole list). Execution of those queries yielded 21 unvisited webpages and 254 products whose cost differed from £4 to £2,337 depending on the distance at which they allowed one to listen. As can be expected, even though all the search queries include the keywords microphone or listening, we retrieved several recommendations for covert cameras. Wall listening devices were also in the list of Google’s predictions.

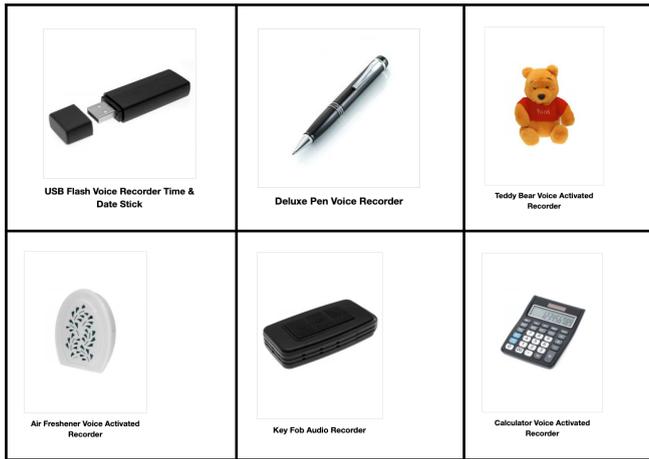
Table 19. Queries for Covert Microphones

Initial Query	Google’s search predictions
Covert microphone	spy microphone, surveillance microphone, covert listening devices, spy microphone uk, secret recording devices uk, wall listening device uk, mini spy microphone, spy microphone long distance

Some examples of covert microphones can be seen in Table 20.

Table 20. Examples of Covert Microphones





Similar to other devices, covert microphones are also sold by well-known online sellers. We present some examples below in Table 21.

Table 21. Online Sellers for Covert Microphones

Online Seller	Links
Amazon	https://www.amazon.co.uk/Listen-Through-Walls-Device/dp/B00FOE94K

	https://www.amazon.co.uk/s?k=covert+microphone&adgrpid=54210562958&gclid=Cj0KCOjwmluDBhDXARIsAFITC_49_pShxIRrRgLfGwThkrxvF0Lyj6TN82WNRu12aj_WkrtsHYIe6_4aAs2pEALw_wcB&hvadid=259051775666&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=e&hvrnd=18044108368665453314&hvtargid=kwd-296399515334&hydadcr=5058_1827823&tag=googhhydr-21&ref=pd_sl_7_rnfxjntbn_e
	https://www.amazon.co.uk/s?k=listen+through+walls+device+pro&adgrpid=118621727684&gclid=Cj0KCOjw6-SDBhCMARIsAGbl7UisPBL_3L_bX_CsK2k9mpKSvj5FR19ZK9F0YCOlcf1qZ8ulU8CnaLQaAmWtEALw_wcB&hvadid=494079194286&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=b&hvrnd=6108653073716674266&hvtargid=kwd-987212348574&hydadcr=4234_1795016&tag=googhhydr-21&ref=pd_sl_9r20scmcsb_b
	https://www.amazon.co.uk/s?k=parabolic+listening+device&adgrpid=58616198572&gclid=Cj0KCOjw6-SDBhCMARIsAGbl7UivAed2LsbtX9wJa5OlvNieTAg6_usw40CKwJ_XRMRtPWsVA4gwU8aApGiEALw_wcB&hvadid=259068905928&hvdev=c&hvlocphy=1006602&hvnetw=g&hvqmt=b&hvrnd=6824185420491675789&hvtargid=kwd-298589992297&hydadcr=28182_1821136&tag=googhhydr-21&ref=pd_sl_3lthy01d8g_b
	https://www.amazon.co.uk/Sensitive-Thru-wall-Contact-Microphone-Amplifier-silver/dp/B01CU4P9FE
	https://www.amazon.co.uk/Spy-Devices/s?k=Spy+Devices
	https://www.amazon.co.uk/spy-microphone/s?k=spy+microphone
	https://www.amazon.com/spy-microphone/s?k=spy+microphone&page=2
Ebay	https://www.ebay.co.uk/itm/Covert-Spy-Voice-Recorder-In-Car-Key-Hidden-Microphone-High-Quality-192KBPS-WAV-/283469347502
	https://www.ebay.co.uk/itm/Professional-Wireless-GSM-Spy-Audio-Listening-Device-Hidden-Body-Worn-Microphone-/302717990956
	https://www.ebay.co.uk/p/5011456805
	https://www.ebay.co.uk/sch/i.html?nkw=Wall%20Listening%20Device&norover=1&mkevt=1&mkr_id=710-154084-941154-2&mkcid=2&keyword=wall%20listening%20device&crp=432905382685_&MT_ID=584416&geo_id=32251&rlsarget=kwd-2030353696&adpos=&device=c&mktype=&loc=1006602&poi=&abclid=1139906&cmpgn=1538464005&sitelnk=&adgroupid=59792236958&network=g&matchtype=p&gclid=Cj0KCOjw6-SDBhCMARIsAGbl7Uh2fgP5KI1JqS6kUSZB9aWM5cY3h_kGUA0dLsKs611jd6jz8MQmVqsaAqXIEALw_wcB

Appendix 2 provides a list of the online retailers based in the UK which sell devices that are apparently used to monitor or spy on others.

Perpetrators are adept at adjusting to new technology and exploiting legitimate tools. The Internet of Things (IOT) and smart devices such as Alexa, Hive and Ring doorbell are being used within domestic abuse contexts⁴⁰. For example, if there is a joint account for Alexa, then if this is not removed after a victim has ended the relationship (which as acknowledged is the riskiest point in the relationship), the perpetrator will be able to know everything that is being delivered to the property and even the details of a new address. If a victim is planning to leave, then the perpetrator can work out the behaviour of the victim. With Hive, the perpetrator is able to emotionally abuse, gaslight and inconvenience their victim by changing the heating in the house, whilst the Ring app could be accessed by perpetrators to see who is visiting.

⁴⁰ <https://www.bbc.co.uk/news/technology-54554408>

In order to explore online discussions regarding use of smart home technologies in TFDA, we used a generic query and the search predictions Google made for it. There was no website dedicated to selling smart home technologies or reviewing them in our list, nor were they advertised as a facilitator to spy on others. However, we identified articles explaining how this technology is misused from 12 websites.

Table 22. Queries for Smart Home technologies

Initial Queries	Google’s search predictions
Remote control smart technologies abuse violence	smart abuse, smart home domestic abuse, technology and domestic violence

Smart home technology is a broad concept and includes several devices. In our analysis the ones that we identified to be misused are Internet-connected video doorbells, sensors on doors, smart lights, internet connected locks, built-in cameras and audio facilities. Data targeted via those technologies are mainly movements of the individuals at home which include both the people living in the house and the visitors. Visiting times are also easily accessed via those technologies and can introduce risks for the privacy and the safety of the targeted people.

For this specific technology group, the main misuse is not only about accessing the information of others but also taking actions with the aim of abusing and controlling them. Locking people at home, turning on the television or music, setting the thermostat on to very high degrees, controlling lights and alarm systems or ringing the doorbells are examples experienced by victims. We found that the internet-connected video doorbells and cameras make it possible to monitor what someone is doing from anywhere in the world. On the other hand, sensors on doors can reveal when someone leaves the house or the use of lights with smart bulbs can show their movements between rooms.

We identified very limited information about the misuse of voice assistants and, therefore, we executed a further query where we used Amazon’s Alexa as an example. Predictions made by Google provided a proof for use of this technology as a facilitator to domestic abuse. Executing those queries, we extracted four recommendations from two websites.

Table 23. Queries for Voice Assistants

Initial Queries	Google’s search predictions
How to use Alexa to spy on my wife	how to eavesdrop with alexa, how to use alexa to listen remotely, what is track my girlfriend on alexa, can you drop in on alexa without them knowing

Searching through recordings is the main advice which allows a perpetrator to learn the instructions, voices and the time of those instructions. Timing also would enable them to discover when the individual or others who interacted with the voice assistant were present in the home.

“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?”⁴¹

Using activation words to record conversations is another way of monitoring potential victims via voice assistants. Activation words are used to bring the device out of sleep mode and to start recording audio. If a perpetrator sets an activation word as a common word therefore, that would allow them to use the assistant to record random dialogs within the domestic environment.

“If you suspect your partner of cheating, is it beyond the realms of possibility to consider changing the activation word to something different? Something that your partner is likely to use in conversation? The aim is, to then get your partner to unwittingly activate the smart speaker, thus allowing it to record their private conversations and catch them in the act.”⁴²

Finally, the “Drop In” feature which was designed to connect instantly to supported Alexa-enabled devices with the aim of hearing sound of the alarms or accidents within the house can be misused to monitor individuals in the home environment.

“These Smart Alerts also include the ability to “Drop In” on the sounds of your home, via the Echo to listen in remotely. Privacy alert! Amazon's stated reason is to hear the sounds of the alarm, but for the first time, via this feature, one could now use Alexa remotely to also snoop in on the sounds from home – a cheating spouse or a misbehaving teen, perhaps.”⁴³

A wealth of physical technological tools used by perpetrators during the facilitation of their abuse, were noted in the interviews highlighting that perpetrators are using the tools readily available to them to facilitate their abuses. These are outlined below but it is noted that this is not an exhaustive list:

- Mobile phones
- Laptop, PCs, Tablets
- Ring doorbells
- Hive
- Smart TVs
- Home hubs - Alexa, Google
- Children’s electric scooters
- Kindles
- Drones
- Fitbits/ fitness tracker
- Plug adaptors (with hidden cameras)
- Car trackers
- Children’s toys (with hidden cameras)
- Air Fresheners
- Pet trackers

Box 7 presents a case described in the interviews, where a covert device was used.

Box 7

A perpetrator purchased a listening device that was disguised as a four-way extension lead, from the internet for £100. He had offered to help his ex-partner install her television at her new property and brought along the extension lead, which had a radius of 50 metres, and put that into the flat as well. After this he started phoning her and making comments such as “I know you’ve got someone in the flat with you” and other things, which showed that he knew everything that was going on in his ex-partner’s property. The victim ended up being so traumatised that she would not get undressed, have a bath, or speak about intimate things in her own home

The use of technological tools to track and monitor behaviours was further emphasised in the interviews:

I've actually had a couple of clients that have unplugged their Amazon Alexas because they found that ex-partners just seem to know stuff that they shouldn't know. And they've got no idea how, and after unplugging the Alexas, not so many problems. So, it tends to be where the perpetrator has bought it and set it up, or they know your log in details for your Amazon account, that kind of stuff (Interviewee 7)

CCTV is another big one that's used, where, and like the Hive Doorbell, where they can monitor who's coming and going, and when the victim is leaving, and who they're having in the home. And kind of we frequently hear about listening devices as well, the kind of, they seem to know information. There's not any way of knowing how, but victims frequently say, I don't know how they're getting this information, but they seem to know, and I don't know how they know, is what we hear a lot. Because, yeah, because they're so ahead of the game, the use of technology is, like I said, it's frequently around keeping track of, or monitoring, rather than trying to find information, so much. And then they will also use direct behaviours, so they, once they've found out where someone's going through some method of knowing, kind of where they are, like, whether it's Google Maps, you know, saying your car has been parked (Interviewee 14)

What surprises me is that if you go on the internet and Google, for example, like the listening devices, the extension leads, they're just readily available. And they're disguised in air fresheners, fake Alexas; it's yeah, beyond me. Most of it, in my experience, trackers and cloning (Interviewee 6)

Pets have even been exploited to facilitate abuse, through the use of devices designed to monitor their physical activity:

This woman whose ex-partner was stalking her because he'd hacked into the dog's fit-bit. So, the dog's fit-bit was connected to his phone, so he was able to see when she was taking the dog on a walk, the, kind of, time she was taking the dog. And he could just intercept her (Interviewee 7)

6.2. Apps

To differentiate 'spyware' from other software that assists employers and parents in keeping track of employees and their children respectively, we adopt the definition from Harkin et al. (2019) who consider a programme to be 'spyware' if the following conditions are satisfied;

- “(a) Data is gathered remotely from a target device that would not otherwise be shared unless foreign code or software were introduced or permitted access by an operator.*
- (b) Data is gathered from the target device with the credible possibility that the user of the target device would not be aware of the exfiltrated information, the on-going presence of the foreign code or software, or any permissions to disclose information.*
- (c) The code or software is to be deployed in the context of targeting a specific individual or group of individuals for the purposes of monitoring, tracking, and surveillance. It therefore does not include firmware updates, native operating system functions, or applications that collect large amounts of data from multiple users in the user-approved course of its ‘normal’ functioning (e.g. Facebook or other social networking services and platforms, as well as internet-of-things devices).*
- (d) The data being disclosed to operators about the target can be reasonably understood to include private, confidential, and otherwise intimate personal information (such as location data, private correspondence, personal photos, passwords etc.).”*

Even though we take this difference into consideration and report our findings accordingly, at the beginning of the technology review search process we followed an inclusive approach and we used queries for both technologies; spyware and dual-use apps. It is known in the literature that dual-use apps, which have a legitimate purpose, such as tracking children or stolen devices, can also be easily repurposed to abuse victims (Chatterjee et al., 2018). Therefore, in this study, we also included queries to retrieve apps with ‘legitimate’ uses such as child monitoring.

The initial queries searched on Google and the additional suggestions/predictions it provided are given in Table 24 .

Table 24. Queries for Stalkerware

Initial Query	Google’s Search Predictions
Stalkerware	stalkerware iphone, stalkerware app, stalkerware download, best stalkerware, stalkerware software, stalkerware android, spouseware

Technology to monitor partners or children	using icloud to spy on spouse, mspy
Apps to monitor partners or children	best monitoring apps, how to track your child's android phone, how to see, what my kid is doing online, best free child tracking app, apps for parents to monitor social media, best parental control app for iphone, best free child tracking app for iphone, how can i monitor my child's text messages for free
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
Spy on cheating partner	spy devices for cheating spouses, cheaters spy app free, what is the best way to catch a cheating spouse who is very clever?, how to catch cheaters on iphone 2020, read cheating spouse text messages free, how to find out if your spouse is cheating for free, cheaters spy app free iphone, how to catch a cheating husband on whatsapp
Stealth monitoring apps / devices	nspy, mspy, flexispy, spyic, how can i spy on a cell phone without, installing software on the target phone?, best free phone monitoring app, cocospy
Couple tracker apps / devices	monimaster, apps for couples with trust issues, accountability apps for couples, couple tracker premium apk, couple tracker download, couples monitor device tracker, couple tracker apk, couple tracker review

It is noteworthy that some app names regularly emerge in the search predictions, for instance, *mspy*, *nspy*, *flexispy*, *monimaster* and *spyic*. More interestingly, “using icloud to spy on spouse” is also presented as a predicted query by Google when we search for “Technology to monitor partners or children”. This finding is valuable on its own as it highlights the role of Cloud technologies in TFDA which is, therefore, examined within this study.

Execution of the queries given in the table above returned 135 unique websites. We extracted 530 recommendations reviewing the first web pages of those websites. The recommendations mainly took the form of apps and websites that can be used to spy on individuals. In total we have identified 124 apps. We counted the number of webpages which mention those apps to give us a rough idea about the popularity of them. Those findings reveal that *mSpy* is the most popular app advertised on the web, which was followed by *FlexiSpy*, *Spyic*, *Highster Mobile* and *Cocospy*.

Here, it is important to note that due to our queries which target dual-use apps, we discovered apps with legitimate uses. In order to differentiate them from the remainder of the apps we wrote dual apps in italics. Our judgement is based on the explanations given in the webpages. Dual-use apps in our list can be divided into three groups; family monitoring apps, employee monitoring apps, and apps dedicated for couples which work based on mutual consent.

In order to understand how spyware, which are not obviously dual-use apps, are promoted on the web, we extracted the motivations given on the websites. Those texts are mainly around parental control and employee monitoring. However, enhancing the trust level in relationships, protecting partners (against physical harm, rape, cyberbullying etc), and gathering evidence from cheating spouse's mobile phone, are some other motivations stated on the websites. In order to clarify those issues, we present some of the following quotes from the reviewed websites:

*"Over a million parents, employers, and people in relationships use Spyier to protect their interests. Track locations, calls, messages, and apps. It's web-based, stealthy, and 100% secure"*⁴⁴

*"Our youth and children have either been a subject of cyberbullying or catfishing online. The digital dangers coupled with the new dimension of technology has led to the development of smartphone spying apps. Our youth and children have been the subject of numerous online crimes, like cyberbullying or catfishing, body shaming, frauds, etc. The digital dangers coupled with the new unscrupulous dimension of technology has led to the development of undetectable spy apps for iPhone. The purpose of these apps is to defend and protect our loved ones from the rampant digital vulnerability. Businesses are harnessing them to monitor their employees and people are using them for location tracking."*⁴⁵

*"Parental Control: Protect your child from potential threats such as rape, harassment, privacy violation and child abuse in this contemporary world"*⁴⁶

*"The technology is growing fast, where almost everyone has access to a smartphone. Kids to adults use applications and other mobile services to transact day to day activities. To keep your kids safe from cyberbullying, gather evidence from your cheating spouse's mobile phone, or improve the productivity of your employees, these are the needs to spy on an Android device of a particular individual automatically and discretely"*⁴⁷

Table 25. Stalkerware Apps

⁴⁴ <https://spyier.com/>, May 2021

⁴⁵ <https://xnspy.com/top-10-iphone-spy-apps.html>, April 2021

⁴⁶ <https://nosecretspy.com/>, April 2021

⁴⁷

https://www.clevguard.com/spy/undetectable-spy-apps-for-android/?gclid=CjwKCAiAyc2BBhAaEiwA44-wW5BnGauCUz1guu0Q2Kd90toP_IIPch-P1aTsPymRv6fFB-6UxPvEEhoCFxYQAvD_BwE, April 2021

Name of App	Number of Mentions	Name of App	Number of Mentions	Name of App	Number of Mentions
mSpy	33	BlurSpy	2	LetMeSpy	1
FlexiSpy	24	Bust a Cheater boyfriend, girlfriend spy app	2	LogsKit	1
Spyic	20	Cerberus	2	MamaBear	1
Highster Mobile	17	ClickFree	2	<i>MMGuardian</i>	1
Cocospy	16	<i>Couple Monitor App</i>	2	Mobile Spy Agent	1
SpyEra	15	<i>ESET Parental control</i>	2	Mobile Tracker Free	1
Spyier	13	<i>Family locator</i>	2	MobiPast	1
KidsGuard Pro	12	FoneMonitor	2	Monitor Minor	1
XNSPY	12	JJSpy	2	Monqi Phone	1
Hoverwatch	11	<i>Kaspersky Safe Kids</i>	2	My Mobile Watchdog	1
Minspy	11	Mobile Spy	2	MySpy	1
Spyzie	11	MoniMaster	2	NoSecretSpy	1
AppMia	8	MxSpy	2	OEM Find My Phone	1
iKeyMonitor	8	PhoneSpector	2	PanSpy	1
SpyBubble	8	<i>Screen Time</i>	2	PathShare	1
Spyine	8	SpyStealth	2	Phone Tracker	1
AutoForward	7	StealthGenie	2	Photo Stream	1
Mobistealth	7	TiSPY	2	Prey Anti Theft	1
<i>Net Nanny</i>	6	Truth spy	2	Quester	1

PhoneSheriff	6	uMobix	2	SafeToNet	1
TheTruthSpy	6	XPSY	2	SecureTeen	1
WhatsApp Web	6	AccuTracking	1	SMS Peeper	1
Couple Tracker App	5	Android007	1	spouseware	1
Guestspy	5	Avocado	1	SpyAdvice	1
Norton Family	5	Boomerang	1	SpyBunker	1
SpyHuman	5	Carrier family locator apps	1	SpyMug	1
Spymaster Pro	5	Circle	1	Spytech SpyAgent	1
Find My Friends	4	ClevGuard	1	SpyWare	1
Google Family Link	4	Connect	1	SpyZee	1
mCouple	4	Copy	1	SurePoint Spy	1
All Tracker Family App	3	DDI Utilities	1	TeenSafe	1
Bark	3	Family Time	1	Text Message Spy	1
Fami360	3	Family Tracker	1	TheOneSpy	1
FamiSafe Phone Monitoring	3	Find My Device by Google	1	TheSpyBubble	1
iSpyoo	3	Find My Kids	1	Track Any Phone	1
Life360	3	FoneTracker	1	Trick or Tracker 3.0	1
NeatSpy	3	FreeForward	1	uboro Tracker	1
OurPact	3	FreePhoneSpy	1	Web Watcher	1
pcTattletlae	3	Google+	1	WhatsEye	1

SpyFone	3	Hellospy	1	XySpy	1
Spy to Mobile	3	iMessage	1		
Aispyer	2	iOS 12	1		

Even though the majority of the popular stalkerware share a range of common capabilities, they are not identical. Next, we present the capabilities of the most popular apps identified in the previous sections. We followed a similar approach while selecting the types of personal data targeted and considered the top 11 data frequently accessed via those apps. Those apps may have different features for different products depending on their cost. Features may also differ from IOS to Android apps. In Table 26, we present the largest set of features for each brand.

Table 26: Apps and their features

App	GPS	Text	Call logs	Browser History	Instant Messages	Social Media Details	Photos	Contacts	Apps	Video	Emails
mSpy ⁴⁸	X	X	X	X	X	X	X	X	X	X	X
FlexiSpy ⁴⁹	X	X	X	X	X	X	X	X	X	X	X
Spyic ⁵⁰	X	X	X	X	X	X	X	X	X	X	
Highster Mobile ⁵¹	X	X	X	X	X	X	X	X	X	X	X
Cocospy ⁵²	X		X	X	X	X	X	X	X	X	
SpyEra ⁵³	X	X	X	X	X	X	X			X	X
Spyier ⁵⁴	X	X	X	X	X	X		X			
Kids Guard Pro ⁵⁵	X	X	X	X	X	X	X	X		X	
XNSPY ⁵⁶	X	X	X	X	X	X	X	X	X	X	X
Hoverwatch ⁵⁷	X	X	X		X	X	X	X		X	
Minspy ⁵⁸	X	X	X	X	X	X	X	X	X	X	
Spyzie ⁵⁹	X	X	X	X	X	X	X	X		X	

It is concerning that *WhatsApp Web* is very commonly recommended as a spying tool to monitor WhatsApp messages of victims. This service enables perpetrators to monitor text messages of their

⁴⁸ <https://mspy.org/>, May 2021

⁴⁹ <https://www.flexispy.com/en/features-overview.htm>, May 2021

⁵⁰ <https://spyic.com/>, May 2021

⁵¹ <https://highstermobile.com/>, May 2021

⁵² <https://www.cocospy.com/>, May 2021

⁵³ <https://spyera.co/>, May 2021

⁵⁴ <https://spyier.com/>, May 2021

⁵⁵ <https://www.clevguard.com/>, May 2021

⁵⁶ <https://xns Spy.com/>, May 2021

⁵⁷ <https://www.hoverwatch.com/>, May 2021

⁵⁸ <https://minspy.com/>, May 2021

⁵⁹ <https://spyzie.io/>, May 2021

victims once they access the [WhatsApp web](#) service site by entering the QR Code with the phone of the victim. Perpetrators can monitor the messages unless the victim takes the phone away from the area and the connection can get interrupted.

Of the aforementioned apps, the location finder apps, *WhatsApp*, *Find my phone* and *Life 360* were noted in the interviews. Participants highlighted that the everyday apps that people use are being exploited by perpetrators to monitor, harass, and intimidate victims.

The following apps were also highlighted in the interviews:

- Food delivery apps - Just Eat, Deliveroo
- Location finder apps - Find my phone, Live 360
- Strava app
- Spyware software

Food delivery apps, which can involve linked accounts and shared details such as passwords, were mentioned in the interviews as a method to uncover victims' new addresses after they have ended the relationship with their perpetrators.

He used her JustEat account to find her address because she didn't think to change that password...so if they know the password they can log in and there is your address details all set out nicely for them...imagine the impact on a victim when they get a message from a perpetrator saying, oh, did you enjoy your pizza last night, that extra topping? That's going to scare the living daylights out of them (Interviewee 11)

Apps designed to protect and empower people are also inadvertently putting them at risk of TFDA because they are also able to be misused by perpetrators to stalk and control.

Hollie Guard is an app which is a brilliant app for those who are experiencing domestic abuse. But again you can add people on who can know your locations and you can get them to track your journeys, but again in the wrong hands that can be very dangerous and very controlling (Interviewee 12)

Service providers spoke frustratingly about how the mechanisms, including apps, that they use to protect and support victims are being publicly divulged, which inadvertently informs perpetrators, ultimately putting the safety of victims at risk.

6.3. Parental monitoring tools

With the aim of exploring apps that are used by families, we used the query: "Family tracking apps/mutual tracking". Google's search predictions for this query were either irrelevant or about stalkerware which were already covered in the earlier phases of our study. Consequently, in this part of our analysis, we limited our reviews to two unvisited webpages that Google returned for this single query. We extracted 15 recommendations which mention 11 unique apps given in Table 27.

Table 27. Parental Monitoring Apps

Name	Data Targeted
------	---------------

FamiSafe	GPS, Apps, Screen time, Browser history, Social media activities,
Life360	GPS
Sygy Family	GPS
Glympse	GPS
Foursquare Swarm	GPS
FamiGuard	GPS, Programs, Apps, Search Engine Use
Safe365	GPS, Battery level
Sprint Family Locator	GPS
GPSWOX Family Locator	GPS
Verizon Family Locator	GPS
ZoeMob Family Locator	GPS

As seen above, it is mainly the GPS data that can be monitored via these apps. In this context, capabilities of these apps are much more limited compared to ones identified during the searches for stalkerware.

6.4. Keyloggers

Keyloggers are other types of apps and devices used for stalking. Their major feature is to collect the passwords of the victim, which can subsequently be used to gain access to several online accounts including social media, email and even financial accounts. Therefore, this specific type of technology allows not only the monitoring of victims but also their impersonation for malevolent purposes.

In this part of the study, we have used the query “How to monitor my partner using keyloggers?” in order to access relevant websites. We eliminated Google’s predictions since they mainly overlapped with the ones that were already covered for stalkerware. Execution of our query resulted in three new websites that were not reviewed before. We extracted 18 recommendations which include some spy apps (*KidsGuard Pro, FlexiSPY, uMobix, Spycic, iKeyMonitor, mSpy, Cocospy, Spytech*), and software programmes as listed in Table 28.

Table 28. Software Keyloggers

Name	Data targeted
------	---------------

Iwantsoft Free Keylogger	keystrokes, browser history
Spyrix Keylogger Free	keystroke, screenshot, audio, camera
Kidlogger Free	keystroke, screenshot, audio, camera, GPS, text, browser history
Revealer Keylogger Free	keystroke, instant messages
Refog Personal Monitor	keystroke, instant messages, browser history, text, screenshots
Ardamax Keylogger	keystroke, screenshot, audio, camera, GPS, text, browser history, email
Spytector	keystroke, email, passwords on browsers,
Best Free Keylogger	keystroke, browser history, passwords on browsers, application monitoring, screenshots
Windows Keylogger	keystroke, application monitoring
Actual Keylogger	keystroke, application monitoring, browser history, screenshot

6.5. Dating sites

Accounts on dating sites or apps can be considered as a type of sensitive information that is being targeted by partners in abusive relationships. With the aim of understanding options provided to perpetrators online to explore accounts of their victims, in this part of the study we used “How to catch my cheating spouse on dating sites?” as a query and also included Google’s predictions that are listed in Table 29.

Table 29. Queries for Dating Sites

Initial Queries	Google’s search predictions
How to catch my cheating spouse on dating sites?	how to find out if someone is registered on a dating site for free, find someone on dating sites by email, how to find out if your husband is on dating websites for free

We extracted 65 recommendations from 19 different websites, the majority of which were website services dedicated to detect accounts of a given name on dating apps. Those websites are not only concerning because of the information they provide, but also due to the personal information they collect. As given in the table below, data requested about the targeted person includes several personal identifiers.

Table 30. Software to explore accounts on dating sites

Tool	Name	Data collected	Data claimed to be provided
Software	OurSecret	Images	Images embedded into an audio or picture file secretly
	QuickStego	Images	Images embedded into an audio or picture file secretly
	Tinder API	None	Public accounts
Website	Spokeo ⁶⁰	Name, email, address, phone number	Contact information, personal details, location history, wealth data, family and associates, criminal records, social media accounts, accounts on dating apps
	<u>Profilesearcher</u> ⁶¹	Email, first age, age, gender, race, zodiac, zip code, address	Tinder account
	Lookupc ⁶²	Name	Tinder account
	ctsearchonline ⁶³	Email	social media accounts, accounts on dating apps
	<u>BeenVerified</u> ⁶⁴	First name, last name	Criminal records, accounts on dating apps
	<u>PeopleLooker</u> ⁶⁵	First name, last name, phone number, email, address	accounts on dating apps
	Craigslist ⁶⁶	Email	Personal details
	Social Catfish ⁶⁷	Image, email, name, address, phone, user name	Contact information, accounts on dating apps (blocked in EU due to GDPR)
	<u>Truthfinder</u> ⁶⁸	First name, last name, city, state (US based)	contact information, social presence, and police records
	Instant Checkmate ⁶⁹	First name, last name, city, state (US based)	public information ranging from criminal records, past or current relationships,

⁶⁰ <https://www.spokeo.com/>, April 2021

⁶¹ <https://profilesearcher.com/>, April 2021

⁶² <https://lookupc.site/#/>, April 2021

⁶³ <https://ctsearch.online/>, April 2021

⁶⁴ <https://www.beenverified.com/>, April 2021

⁶⁵ <https://www.peoplelooker.com/>, April 2021

⁶⁶ <https://geo.craigslist.org/iso/gb> April 2021

⁶⁷ <https://socialcatfish.com/>, April 2021

⁶⁸ <https://www.truthfinder.com/>, April 2021

⁶⁹ <https://www.instantcheckmate.com/>, April 2021

	Intelius ⁷⁰	First name, last name, city, state (US based)	criminal record
	usersearch ⁷¹	User name	accounts on dating apps, social media accounts, email, phone number
	cheaterbuster ⁷²	First name, age, address	Tinder account

In addition to those software and website services, following apps were recommended with the same purposes; Dating.ai⁷³ and *Find My Friends*.

There are also some actions among the recommendations which do not require installation of any app or software. For instance, people are recommended to check browser history to look out for popular dating website names or apps such as *Tinder*, *Coffee Meets Bagel*, *Match*, *OkCupid*, *Bumble*, and *Zoosk*. If the browser history is clean, a further option is suggested which is based on beginning with the first letter of the alphabet and typing each letter into the Google search bar to see what the targeted person has been Googling recently. This is possible by monitoring what appears in the autofill section.

Checking installed apps to look out for dating apps is recommended with the same purposes. It is also underlined that those apps can be hidden, and it is encouraged to check purchased or downloaded apps on App stores or checking for apps that have “disable” toggled on an android device by opening up “settings” and clicking “application manager”.

Google is another option that could be used to uncover hidden accounts on social media or dating sites. Running a Google search using the target's email address, name, phone number and image is given as a way to discover those accounts. In order to get more accurate results, Google Advanced Search is given as a solution where it is recommended to type in the email address that is looked up in “exact word or phrase” and popular dating websites like *Match.com* *pof.com* or *zoosk.com* in the domain name field. Checking previous destinations on Google Maps is another recommendation we identified on the web pages analysed at this part of the analysis. Similarly, Google’s “*Find My Phone*” is also suggested with the aim of location tracking. For iPhone users, checking iPhone's *Significant Locations* is given as an alternative.

Visiting Facebook’s search page to search for email address, creating fake profiles to search for or access target’s account, monitoring emails or messaging apps looking out for the ones from dating apps, hotels or about suspicious money transfers, recording phone conversations with a secret second phone (if using landline) are other uncommon strategies given to monitor private lives of targeted people. Checking battery usage is also given as a way to see what apps are used and for how long.

It is worrying that there are also some websites where “cheaters” are disclosed by their partners;

⁷⁰ <https://www.intelius.com/>, April 2021

⁷¹ <https://usersearch.org/index.php>, April 2021

⁷² <https://www.cheaterbuster.net/>, April 2021

⁷³ <http://dating.ai/>, April 2021

“Check name on websites designed specifically to find cheaters and warn others about them. Some of the best ones are “Liars, cheats and bastards”⁷⁴, “Cheaterville”⁷⁵ “Playerblock”⁷⁶ and “Spokeo.com”⁷⁷ People post stories on these websites about how they were betrayed and why others need to steer clear of certain people. They also post the real names of cheaters who hurt them, and some of their stories are heartbreaking. “Don’t Date Him, Girl” is a site for women only featuring the profiles of male cheaters.”⁷⁸

Online documents, Cloud-based storage options like Keepsafe, Vault and Hide It Pro and finally deleted digital items are other digital types of data that are told to be monitored.

6.6. Use of drones

Drones have become much more common in the last decade and can be used for leisure, work and criminal purposes. It would be no surprise to find them being used in the context of relationships. In one UK case a man used a drone to monitor his former partner and her friend, among other acts of harassment (BBC News, 2020b). Another example from the US involved a man using a drone to monitor his wife, who he suspected of having an affair. He uploaded the footage of his discovery to YouTube alongside his commentary describing how she had thrown 18 years of marriage away (MailOnline, 2016). Although drones were not specifically mentioned within the interviews, their potential to be used within TFDA should not be underestimated as perpetrators seek to use any tools available to conduct their abuses.

6.7. Excessive and abusive mass communication

One of the benefits of the new technologies that have emerged over the last 20 years is the ability to undertake communication by text, voice and picture/video easily and cheaply. Return to the 1980s and communication would have been largely done via letters, telephone or in-person. The ability to send several hundred messages in a day would have been more difficult, time-consuming and costly. Fast-forward to today and it is very cheap and easy to contact a person hundreds of times or more a day. Lots of the media cases assessed as part of the wider scheme of the abuse involved excessive communication. Excessive email can form part of a Distributed Denial of Service Attack (DDoS). No cases were found of such attacks occurring in relationships, but the sheer amount of communication in some cases could be considered as equivalent. Indeed, it was common to find examples of hundreds of emails, texts, messages, calls having been made in relatively short periods of time. For example, in one case a man regularly contacted his former partner, received an order prohibiting it, but continued and in one instance made 37 video calls in 15 minutes among other acts (The Herts Advertiser, 2020).

Another angle to this is the ease with which it is possible to set up accounts, profiles and websites and use those to abuse a person. Aspects of this have already been covered with fake accounts, but sometimes the perpetrator doesn’t even seek to use a fake profile or the victims. In one case a wife discovered her husband was having a gay affair with their gardener, so she set up a website, and also hired a PR company to publicise it, denouncing him. It stated, among other things, *“This website is*

⁷⁴ <https://sites.google.com/site/liarscheatersandbastards/>, April 2021

⁷⁵ <https://www.bullyville.com/?page=articles&id=994>, April 2021

⁷⁶ <http://playerblock.hipnosisprofesional.org/>, April 2021

⁷⁷ <https://www.spokeo.com/>, April 2021

⁷⁸ <https://www.itscheating.com/cheating/nine-highly-effective-ways-to-catch-your-partner-cheating-online/>, April 2021

dedicated to my cheating husband Egill Antonsson. A man who had it all but decided to throw it all away for a quick romp,” the website reads. “We had it all. A nice house, a loving relationship, beautiful kids, a dog and enough joint income to make our living comfortable. What more could you want?” (PinkNews, 2016).

The relentlessness of excessive and mass communication was brought to the forefront in the interviews:

I’ve had clients that have had hundreds of messages an hour, you know, so, my client that was in court this week, with the really good outcome, I think one of the phone numbers that he admitted to, there were over 7,500 calls in a month. That’s not taking into account the other multiple numbers he was using, the contact she was getting on social media from the fake profiles. And I remember one day I rang her and she ended up having two phones, and I rang her and all you could hear in the background was her other phone that he was contacting, constantly beeping and ringing. And she was just crying on the phone to me. She was, like, I don’t know what to do. And we’ve got people that are scared to turn their phone on (Interviewee 7)

In some instances, there is a lack of realisation that excessive and mass communication equates with harassment as this quote from the interviews demonstrates:

Some of our victims don’t perceive it as abuse, they just see it, oh, we just had an argument. It’s a perception, oh, God, he used to drive me mad, he’s, you know, it’s undermining me. And it’s not until they sit down with someone, say, like me, when I sit down, now let’s have a look at these messages, that’s 600 messages in a day, of excessive emotional abuse or threats to kill. Yeah, but he’s got a mental health problem. No, it’s criminal and it’s harassment (Interviewee 6)

7. Scale of Technology-Facilitated Domestic Abuse

The indication is that technology does feature in the majority of domestic abuse cases that are dealt with by service providers, in particular activities that fall within the CMA. Interview participants have stated that in nearly every case they see, there is some form of a hacked account, or attempts to hack into accounts.

I think what we see most commonly, in absolutely every case, there is some form of hacked account. There isn't any case that's come through to us in the thousands of cases we've had, that there hasn't been a hacked account (Interviewee 1)

As such, many domestic abuse service providers will raise concerns about the likelihood of accounts being hacked with victims, even if victims themselves had not considered this previously. Additionally, harassment using technology, involving abusive comments, fake profiles and image-based sexual abuse are common.

I hold roughly 25, 30 cases at any one time; so it is about 800 cases a year, if we go by numbers. I would suggest that technology is involved in any form probably 70 per cent of the cases, if not more. In some cases we could almost say it's involved 100 per cent because of the social media abuse. I would suggest probably in every single case that I work with we have to address our clients' social media usage and security settings, because at some point in our discussions social media is the primary – and I am going to use the brand name Facebook, okay, because that has some notoriety to it – I'm going to stick neck out, I reckon probably 95 per cent of the cases I take have some element of Facebook misuse in them: whether it's nasty comments being posted; fake profiles being set up; comments about confidential information being shared. Allegations of, I hate the phrase revenge porn, I really do, because it's just inappropriate, but the whole it's the trust of intimate photographs and the distribution of them, and the publication of them. That is regular in a lot of cases (Interviewee 6)

The use of digital tools to stalk victims are also all too prevalent.

Particularly in stalking cases, it's very rare to have cases, as well, like, ex-partner cases, where there isn't some kind of, like, online element to it, digital element to it. Whether that's creating the fake profiles online, threatening to post images, putting software on phone, listening devices, that kind of stuff (Interviewee 7)

Excessive and mass communication was also noted as featuring prominently in cases of domestic abuse.

In some capacity, whether it's from the, this is the way that I contact you to send you verbal abuse, I will send you 100 text messages a day, I will call you all the time (Interviewee 17)

Interviewee 15 also highlighted that the police are expecting technology to feature in some respect when they respond to domestic abuse cases.

I think most officers are aware that it's likely that any domestic will involve technology to some extent. I mean, you know there's always some sort of argument that's happened over a text message, or social media, in addition to whatever arguments may have happened face to face. You know, it's that prevalent, you know, that I would say the vast majority of domestics are going to involve technology to some extent, without a doubt (Interviewee 15)

The interviewees also noted that TFDA is likely to be part of an ongoing pattern of coercive and controlling behaviour throughout such relationships, where access to victim's accounts is expected along with monitoring of their movements, as outlined in the earlier discussion on unauthorised access. The indication is that where there is coercion and control present in a relationship, technology will also feature as a means to conduct that abuse too.

I mean, it's all the way through. So it's when they're in a relationship, he's going to want to hack her accounts. And sometimes it's really obvious. They'll say, we have to sync accounts, you know, wanting everything, take the phone off them. Other times, they're hacking in, to check to see if she's liaising with any agencies, planning on leaving, who she's speaking to, hacking into the WhatsApp accounts to read messages (Interviewee 1)

The researchers also assessed the length of abuse in the media cases. This was difficult to assess for a number of reasons. First, many reports did not specify the length. Second, technology was often a small part of a larger scheme of abuse. In such cases it was not clear how long the technological aspect lasted. In these cases the broader abuse was taken as the measure, which means the technological aspect is lengthened in some cases, but to do otherwise would have involved guessing and speculation. In 88 of the cases the length of abuse was determined. The numbers where it was possible to determine meant for some categories it was not possible to do further analysis. Only for unauthorised access/spyware, impersonation, fake accounts and disclosing images. Table 31 provides the full analysis. Some key findings, baring the caveats in mind:

- In unauthorised access/spyware cases the abuse lasted the longest with two thirds of the cases having abuse that lasted at least in the months; and
- Disclosing images generally had the shortest, with almost 70% lasting in the days or weeks.

Part of the reason for the above is that unauthorised access was often part of wider abuse in controlling relationships, which went on for some time. Although disclosing images tended to be short, i.e. the offender published images and a few days later they were taken down, it is likely the psychological impact on the victims lasted much longer.

Table 31. Length of technological abuse

	All	%	Unauthorised access/spyware	%	Impersonation	%	Fake accounts		Disclosing images	%
Days	20	23	14	29	11	37	5	19	11	58
Weeks	9	10	2	4	4	13	5	19	2	11
Months	44	50	24	49	12	40	12	46	6	32
Years	15	17	9	18	3	10	4	15	0	0

8. Spaces of Technology-Facilitated Domestic Abuse

In addition to apps used to spy on individuals, our analysis revealed some websites that are also used to monitor individuals with relatively more limited functionalities. GPS is the main information proposed to be provided by those services which mostly require the phone number of the targeted person to be given to the system. We have identified two websites which collect email addresses and usernames of targeted people to provide online pictures, social media profiles and accounts on dating apps or websites.

Table 32: Websites for Stalking

Website	Personal data asked	Output claimed to be provided
CellTrack ⁷⁹	Phone number	GPS
Cell Phone Tracking mobi ⁸⁰	Country, Phone number	GPS
Spokeo	Email address / User name	Online pictures, Social profiles
Find my Iphone ⁸¹	Apple ID	GPS
Device Tracker Plus ⁸²	Phone number	GPS
CheaterTest ⁸³	Email address	Dating profiles
Helpmobi.io ⁸⁴	Phone number	GPS

An interviewee noted that they had dealt with cases where perpetrators have accessed illegal content on the dark web so that their victim would have appeared to have engaged in criminal activity:

I've come across a few cases where people have said that perpetrators are accessing things like the dark web and the fear of that type of thing going on and if they've accessed that on a computer within the home, the criminal side of stuff they've accessed or deliberately accessed, illegal content from a computer or a device that's within the victim's home so then the victim can be accused of accessing that (Interviewee 9)

Specific online spaces enabling TFDA were mentioned during the interviews, these are:

- Social media platforms - Facebook, Whatsapp, Instagram, Snapchat, Twitter

⁷⁹ <https://www.celltrack.co.uk/>, April 2021

⁸⁰ <https://cell-phone-tracking.mobi/index.php>, April 2021

⁸¹ <https://www.icloud.com/find>, April 2021

⁸² <https://www.devicetrackerplus.com/>, April 2021

⁸³ <https://ctsearch.online/>?, April 2021

⁸⁴ <https://helpmobi.io/en>, April 2021

- Netflix
- Spotify
- Dating sites - Tinder, Grinder
- Anonymous messages sent through Pandora Jewellery

Companies that enable anonymous messaging have also been used by perpetrators to harass and stalk their victims, with the jurisdiction of companies creating further challenges for victims and the authorities. Box 8 illustrates a case example that was discussed in the interviews.

Box 8

The jewellery company Pandora provides an online service in which anonymous love messages can be sent to the object of your affections. A woman began receiving messages from this site, several times a day, which she believed to be from her ex-partner, but was unable to prove it. Despite compiling a report with the police, logging all the messages, the case could not be pursued further because Pandora, as a US company, did not provide details of the IP address sending the messages.

9. Drivers and Motivations of Technology-Facilitated Domestic Abuse

Technology as a facilitator of domestic abuse, is generally acknowledged to occur throughout a coercive and controlling relationship. In many cases a perpetrator will have demanded access to their partner's accounts or are already infiltrating them, without their partner knowing. They might have also installed spyware or hidden cameras to constantly monitor their partner's activities. The technological abuse, however, increases when a relationship ends, or the perpetrator becomes aware that the victim is planning to leave them. In these situations, the surveillance involving these tools escalates as the perpetrator attempts to uncover information that will win them back or prevent them from leaving.

Generally when they lose control is when they start behaving more challenging in different ways. So they do everything they can but they never quite...it's like they don't quite satisfy that itch, so they look for more and more things to scratch it, so any kind of where they can gain that control, they will do it (Interviewee 2)

It's just, I think to control. They don't want to lose that control, particularly if the relationship is breaking up or has broken up. They've lost that power of control that they had when they were together. And they'll do anything they can to get anything really, any of it back (Interviewee 4)

And so while they're in a relationship, it's an issue, when they're leaving it's an issue, because they suspect something's happening, they're really on it and they want to check everything to see someone's movements. And when they're left, it really ups the ante then, because then they're hacking into absolutely everything (Interviewee 1)

It is here that perpetrators might employ more severe forms of technological abuses such as the dissemination or threats to disseminate intimate images of their partner, and/or harassment and stalking, particularly to discover where they have gone or are planning to go.

Interviewees also spoke about relationships where abuse did not feature prior to them ending, however the break-up led to an ex-partner engaging in methods of TFDA:

We have ones where the relationship was fine. And as soon as they break up, that's when the person thinks, oh my god I need to control them. So they do just do anything that they can get information on them (Interviewee 4)

Core motivations for technology-facilitated domestic abuse can broadly be understood via the relationship status and type of abuse, as shown in Table 33.

Table 33. Perpetrator motivations in relation to relationship status and type of abuse

Relationship Status	Type of abuse	Perpetrator Motivation
Relationship ongoing	Unauthorised access to accounts Use of covert spyware Creation of fake accounts	Control, monitoring Financial gain Check for infidelity, impersonate the victim
Relationship ending	Unauthorised access to accounts Use of covert spyware Creation of fake accounts Harassment Stalking Image-based sexual abuse	Control, monitoring Financial gain Uncover information to prevent victim leaving/ victim's plans Check for infidelity Communication Impersonate the victim/another Ruin victim's reputation, get family friends on side Blackmail
Relationship ended	Unauthorised access to accounts Use of covert spyware Creation of fake accounts Harassment Stalking Image-based sexual abuse	Control, monitoring Communication Impersonate the victim/another Ruin victim's reputation, get family friends on side Blackmail Uncover victim's location Evidence to use in child custody case

Some media reports offered insight on the purpose and motivation for the offender. The quality and quantity in the reports did make assessment more difficult in some cases and ultimately one is relying on the reporter's assessment. For that reason, the actual numbers will not be set out, but rather some of the different motivations, of which often there was more than one, will be presented. Some of these do overlap, but the following were felt to be the most common motivations in the sample. These motivations also apply in the cases discussed during the interviews.

Revenge: this was probably the most common motivation. Offenders upset at the ending of a relationship or the conduct of the other pursued behaviours to punish them, which often involved technology, such as disclosing private images, seeking to discredit them, to name some.

Control: another common motivation was to control the partner and technology provided a means to do so, from controlling who they communicated with and what they did (because of the surveillance they knew they were under). In some cases, this involved creating fake situations to make the partner vulnerable, so they needed the offender even more.

Surveillance: underpinning some of the others was the pursuit of surveillance to find out what the other person was up to, what they were doing, who they meet, talk to, what they say etc. In some there was also possibly a sexual element to this too.

Attempted reconciliation: another common motive was reconciliation. Some did not accept the end of the relationship and used technology as a means to communicate when their former partner had blocked them or if there were legal prohibitions.

Secure evidence of infidelity: in several cases there was fear of infidelity in the other partner, and technology along with other means was pursued to find evidence of this.

Secure evidence for divorce: a small number of cases found evidence of the use of technology to try and secure evidence for an advantage in divorce proceedings.

Financial gain: in a small number of cases part of the motive involved a financial aspect, to secure access to the finances of the partner.

Curiosity: in some cases the partner was interested to find out what the other was doing, thinking, engaged in.

Perverf justice: a couple of cases were found where one partner was seeking to implicate the other, by using technology to create evidence to support that, such as creating a false account with abuse coming from it that implicates another.

Sexual: there was evidence in some cases that the motive was sexual, where technology was utilised to help secure sexual gratification.

From the above motivations it was possible to develop a typology of abusers set out in Table 34.. They include **the curious, the investigator, the deviant, the controller and the avenger.**

Table 34. A typology of abusers

	The curious	The investigator	The deviant	The controller	The avenger
Aim	Just want to know what partner or former partner is doing	Want to secure information for a purpose such as to secure evidence of infidelity or other information which might aid a divorce case	Want to observe, secure data or use person for sexual gratification	Want to control partner and prepared to use means to aid compliance.	Want to cause damage to current or former partner
Technique/ Action/ Method	Could involve searching clothes, looking at bank statements through to technological based hacking, tracking, covert devices etc.	Could involve following a person, asking people, hiring an investigator through to technological based hacking, tracking, covert devices etc.	Could involve watching a person from secret location through to technology based covert devices, use of private images etc.	Technology such as hacking, covert devices, trackers etc is used to control a person (which may be alongside more traditional psychological, physical and sexual forms of abuse).	Desire for revenge could be through violence, sexual assault to murder, but through technology could be via disclosing private images, harassment. Technology could be used to facilitate the traditional, such as to locate a person so they can be attacked

9.1. Purpose of Unauthorised Access

The reasons for unauthorised access were varied in the media cases. At the base level for some it was just curiosity. Another frequent rationale was suspected infidelity and the desire to secure evidence of such behaviour. Some divorce cases involved perpetrators using hacking to try and secure evidence to aid their case. A very common reason was related to controlling partners seeking to see who was communicating with the victim and in some cases communicate on their behalf. These cases move hacking from information gathering to pursuing a secondary act. Indeed, impersonation was common in hacking cases. This could be to simply send out messages from the person’s account about their status or related to a particular issue. Several cases were found of women who had discovered their partner was cheating, who then hacked into their accounts and changed their status. For example, one wife who discovered her husband was cheating on her using Tinder, accessed his profile and changed it to the following:

*Hey my name is Mike and I'm married with two kids. I have a tiny d*** that is STI infested. My wife found my profile if you can't tell and I don't know let that [sic] she's talking on the phone right now with one of my girls and is leaving me. I'm a piece of s*** who doesn't give*

*a flying f*** about anyone but myself. I have been talking and cheating so long, don't be sad if I don't remember your name because I send the same generic s*** to all you girls. Feel free to blow me up with hate mail* (The Sun, 2016).

In another case, it was found that a girlfriend who shared a laptop with her boyfriend, and therefore had access to his email, discovered he had won a scholarship which would have meant him moving away. She declined the offer without him knowing and then set up a fake account to communicate with him impersonating the organisation, offering him a lesser scholarship she knew he would not take (MailOnline, 2018b). Some unauthorised access cases were the base for committing more serious acts such as theft or disclosing explicit images/videos, see Box 9.

Box 9

In one case from Wales an ex-partner hacked his former girlfriend's social media accounts and uploaded pictures of her naked. He changed the passwords so she couldn't access them and also communicated with men (impersonating her) suggesting they come round to the house for sex (WalesOnline, 2020a).

In another case a former model experienced an 18-month campaign of harassment, which included her former boyfriend hacking her bank account and spending enough money to send her into overdraft, among numerous other acts (MailOnline, 2021).

In the interviews, one of the main reasons provided for unauthorised access was about uncovering the new location of the ex-partner (and children) after a relationship has ended. In these instances, perpetrators could be either the investigator or avenger (or both) on the typology, depending on what they intend to do once they have obtained the desired information.

Predominantly, we find that people are mainly hacking online to find out someone's location, where they've moved to, if someone's fled. So, they've fled with their children for safety, either to a refuge or a safe location. They're using all their accounts online; they're hacking into them to try and find the movements of where they've gone (Interviewee 1)

9.2. Involvement of Children and Custody Proceedings

It is during the break-down of the relationship that another key driver for technological abuse develops - child contact/custody cases. Interviewees spoke about the increased involvement of children in technology-facilitated domestic abuse contexts, especially as a means for perpetrators to further control in post-separation shared parental situations. Children are used to abuse the other parent, their devices such as phones, tablets and games consoles, are exploited by perpetrators to monitor and maintain control over victims. Post-separation contact around parenting enables abuse. In some instances, technology-facilitated contact is used in lieu of physical meetings to decrease risk, yet instead it allows persistent harm.

In this example the perpetrator has hacked into their ex-partner's accounts in order to find information that would give them the upper hand during their child custody case:

It's...in nearly...most child contact cases, they're printing off information from social media especially, you know, to try and make her look like a bad mother, or question her whereabouts (Interviewee 1)

In some instances, perpetrators have fabricated communication from their ex-partner after hacking into their accounts, so that it appears as if the ex-partner is the abusive party. In other cases, perpetrators have accessed their ex-partners accounts and printed off information to use in court against them. Children's devices have had listening/tracking apps installed on them and instructed to always have them on and keep them close, so that perpetrators are able to know everything that is happening at their ex-partner's new house. Children's devices are also used as a conduit to send abuse to the ex-partner as this quotation demonstrates:

There's a lot of manipulation through the kids, I mean, I've seen people send abusive messages to the children that's for their parent, so there'll be some really quite severe allegations, you know, like paedophilic allegations, sexual assault allegations that are being sent to the child, but that's for their parent (Interviewee 2)

Children being used to spread harmful messages is further demonstrated in the case example in Box 10

Box 10

In a case described in an interview, an estranged father was using video conferencing calls with his seven-year-old child to make threats of suicide. During these calls, the father also tried to coerce the child to take a side and subjected them to conversations of an adult nature. The father's defence was that as he had bought the phone and it was his contract, he can use it however he likes.

Where perpetrators have access to children, they have used this claim to stalk and harass their former partners. FaceTime was mentioned in many of the interviews as a way to listen in to conversations and check on ex-partner's homes – children are instructed to have their videos on whilst moving around the house. The reliance on technology during COVID has exacerbated the ability to engage in TFDA involving children:

I mean, the whole thing of child contact is a big thing. So during lockdown, child contact has gone quite, Facetime with the kids, and electronic, and all of that. And then, abusers using that as an opportunity, because they know it's on loudspeaker, they know mummy will be listening in to make sure the child is protected. But they can say all sorts of things that, you know, are abusive, and cause fear, and part of controlling another person. So the thing with ex-partners, particularly during lockdown, has been the use of computers for child contact, has been quite a big issue that we've seen. It's often linked to stalking, stalking and harassment, I think, the relentlessness of it. So, stalking and harassment, and tech abuse, and using devices as part of the abuse, it's the relentlessness of it. Yeah, it's a bombardment, often. And yeah, so those often go together. So it's more around the controlling behaviour, than the violence, usually (Interviewee 8)

Children may unwittingly be used as conduits for abuse via their technological devices, and this can occur not just after the breakdown of a relationship, but during the relationship. In the technology review the ambiguity and difficulty of differentiating between dual-use and spyware apps was highlighted. This enables perpetrators to exploit technology designed to help parents monitor their children's devices and online activity, to stalk and abuse their partners/ex-partners. Some apps, however, are blatant about the potential for abuse in their advertising. Statements such as, "A complete parental monitoring software, *MobiPast*, helps parents carefully keep vigilance on their children's smartphone activities but also can be used to catch a cheating spouse." confirm the role of dual apps in TFDA reported in the literature. Similarly, *iKeyMonitor* requires jailbreaking a device even though it is given as a dual use app for parents.⁸⁵ *KidsGuardPro* is particularly interesting since it pretends to be a legitimate app on the main page of its website, however, it includes explanations about using the app to gather evidence from cheating spouses on other webpages. It is also given as a spyware on the blogs that list the best spyware to use.⁸⁶

Children are exploited to record what is going on in the home, see Box 11

Box 11

In one case described in an interview, a primary school child had her own tablet. The tablet went everywhere with the child, including when she was with her respective estranged parents. The father instructed her that the tablet must always be on and charged 24 hours day, whilst she is 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.

⁸⁵ <https://ikeymonitor.com/>, April 2021

⁸⁶ <https://www.clevguard.com/monitor/how-to-catch-a-cheating-husband-on-whatsapp/>, May 2021

10. Perpetrator Profiles

Table 35 below provides some data on the demographics of the offenders derived from the media case analysis. The spyware related cases were not assessed as 11 cases were not considered enough. As each type of offence is considered, more discussion will be provided. However, a brief commentary here:

- Men are the dominant offenders (circa 70%+ in all categories), but some categories such as tracking and covert devices were very dominant (circa 90% +);
- Women are much more involved in fake accounts and impersonation, than other forms of technology assisted abuse (circa 25%), but generally are engaged in such activities much less, compared to men;
- Mean and median age for most categories in low 30s, with tracking and covert devices the exception with late 30s the most common;
- Ages did cover the full spectrum, ranging from 20 to 71, with 6 cases over 60.

Table 37 sets out the relationship context for the abuse. The vast majority of the sample were in (or had been) in straight relationships at 94%, with 6% LGBT. Cases were grouped on a number of criteria. If husband or wife were listed those terms were used, if boyfriend, partner etc., intimate partner was used. The majority of cases involved ex-partners, husbands, wives (55.5%). If the abuse occurred before and after they were classed as ex. We also looked for niche areas of abuse in relationships beyond intimate partners where technology featured, such as families. Very little was found other than some cases involving a son on father and daughter on parents. We also found one case where the female partner impersonated a man, deceiving the female victim. Part of the scheme involved fake accounts, but ultimately the victim was sexually assaulted (See Box 12).

Box 12

A woman set up a bogus Facebook account as a man and developed a relationship with another woman, which evolved to a sexual relationship. She also communicated with the victim impersonating fake relatives. The victim was blindfolded during sex where she used a prophetic penis. Eventually the victim removed the blindfold and discovered she was a woman. The offender was convicted of sexual assault (The Guardian, 2015).

Table 35. Demographics of offenders in the sample

Demographics	All (N)	%	Unauthorised access/spyware cases (N)	%	Impersonation cases (N)	%	Fake accounts (N)	%	Disclosing images (N)	%	Tracking (N)	%	Covert devices (N)	%
Male	120	82	69	83	29	73	26	72	29	83	20	100	17	89
Female	26	18	14	17	11	27	10	28	6	17	0	0	2	11
Mean age	35		33		33		34		32		39		37	
Median age	34		32		31		29		31		43		38	
Mean occupational status	3.4		3.6		-		-		-		-		-	

Median occupational status	3		3		-		-		-		-		-	
----------------------------	---	--	---	--	---	--	---	--	---	--	---	--	---	--

Notes:

1. Male and female based upon reporting, not how the person may identify.

Table 37. Relationship status where abuse occurred

	All	
Intimate male partner on female	32	21.9
Intimate female partner on male	5	3.4
Husband on wife	20	13.7
Wife on husband	5	3.4
Son on father	1	0.7
Daughter on parents	1	0.7
Fake intimate male partner on female	1	0.7
Ex intimate male partner on female	51	34.9
Ex intimate female partner on male partner	9	6.2
Ex intimate male partner on male partner	5	3.4
Ex intimate female partner on female partner	2	1.4
Ex intimate female partner on unknown	1	0.7
Ex husband on ex wife	11	7.5
Ex wife on ex Husband	1	0.7
Ex wife on ex wife	1	0.7

Some reports also note the occupational status of the offender, sometimes in a sensational way such as when a police officer or teacher is involved. Where the occupation was listed this was added to the database and an assessment was made using the ONS Occupational Status Tool. This ranks occupations in nine broad categories and these headline numbers: 1 to 9 were used. Generally, the lower the number the higher the status and skill in the job. The tool does not include unemployed, retired and students which were also listed. It is important to note many cases did not have the occupation of the offender and given the context, the offender was probably likely to be either unemployed or in a low status job. So the sample is highly likely to over-represent higher status occupations and these figures should be treated with caution. But perhaps what they best illustrate is all echelons of society are involved in using technology for abuse in relationships. Box 13 illustrates this with some of the names of occupations.

Table 38. Occupational status of offenders by occupational status

ONS Category	N	%
1	12	23.1
2	10	19.2
3	13	25.0
5	5	9.6
6	2	3.8
8	1	1.9
9	5	9.6
Students	2	3.8
Retired	1	1.9
Unemployed	1	1.9

N=52

Table 39. Mean occupational status

	All	Unauthorised access/spyware
Mean occupational status	3.4	3.6
Median occupational status	3	3

Box 13 Occupations of offenders listed in abuse

Politician, actor, flight attendant, builder, commercial pilot, soldier, teacher, police officer, road sweeper, businessman, restaurant owner, astronaut, banker, researcher, retail manager, mortgage broker, scaffolder, construction site manager, production manager, medical doctor, surgeon, security guard, carpenter, nanny, gas engineer, mechanic, IT expert, photographer, forestry worker, electrician, property developer, management consultant and hairdresser.

Most of the acts of technological abuse in the media cases found were low skill. Figure 9 divides levels in three categories. At the base level are acts that any ICT user could do. Setting up a fake account, guessing a password or physically intimidating someone to provide access, all require little

skill. The vast majority of cases in this sample fitted this category. Some acts require more skills such as further research or basic training. The use of some apps that enable spyware fit this category. Installing covert devices may involve some basic research to do so effectively, although if it is just placing a mobile phone covertly this would also be low skill. Tracking devices/apps similarly fit this same category and could be both depending upon the device or app. Anyone who has flown a drone knows it is not as simple as one might think, and to use to monitor/harass a person would require some additional skills. In the sample of cases there were a small number that fitted this category. The final category, where extensive research and training would be required, such as hacking a person's account via social engineering, requires much more skill. Such technological skills were rarely found in the sample.

Figure 9. The sophistication of technological abuse

Low Skill Technological Abuse Any person who uses ICT could do	Medium Skill Technological Abuse Research and small amount of training would be required to do	High Skill Technological Abuse Extensive research, training and a high degree of skill to do
<i>Hacking based on Force/threat</i> <i>Theft</i> <i>Control</i> <i>Multiple access to devices</i> <i>Guess</i> <i>Sharing passwords</i> <i>Knowledge of where passwords kept</i> <i>Gifting devices with spyware</i> False accounts Impersonation Installation of covert devices and tracking	Hacking based upon spyware Use of drones Installation of covert devices, tracking devices	Hacking based upon social engineering, spyware, sophisticated tools

In order to explore ease of access and use of the popular apps on the Web, we considered five main criteria: existence of available versions working on both IOS and Android markets; possibility of remote installation without physically access to the victim's phone; whether the app requires

jailbreaking⁸⁷ or rooting⁸⁸ before installation; and finally, the cost of the apps at the time of the study (April 2021). Our findings can be found in Table 40.

Table 40. Apps and their ease of use

App	IOS	Android	Remote Installation	Needs jailbreaking/ root	Invisible/ Undetectable/ Stealth mood	Cost
mSpy	X	X	Yes ⁸⁹	No	Yes	Less than \$1 per day
FlexiSpy	X	X	Yes	Yes	Yes	\$29.95 per month - \$349 per year
Spyic	X	X	No	No	Yes	\$99.99 - \$399.99 per year
Highster Mobile	X	X	No	No	Yes	\$80- \$110 per year
Cocospy	X	X	No	No	Yes	\$99.99 a month - \$3999.99 a month
SpyEra	X	X	No		Yes	\$389 per year
Spyier	X	X	Yes ⁹⁰	No	Yes	\$39.99 per month
Kids Guard Pro	X	X	No ⁹¹	No	Yes	\$29.95 per month
XNSPY	X	X	No	No	Yes	\$4.99 per month
Hoverwatch	Only Mac OS X	X	No	No	Yes	€24.95 per month

⁸⁷ Jailbreaking is the process of modifying iOS system kernels to remove the limitations and security features built by the manufacturer Apple (the "jail") through the use of custom kernels. This process allows unauthorised modifications to the operating system.

⁸⁸ Rooting is the process of gaining administrative or privileged access for the Android OS by gaining unauthorised access or elevated privileges.

⁸⁹ Physical access is required for installation for android phones but remote installation is possible once the iCloud credentials are known.

⁹⁰ Remote installation is possible only for IOS solutions.

⁹¹ Not necessary for iCloud monitoring if the credentials are known.

Minspy	X	X	No	No	Yes	\$39.99 per month
Spyzie	X	X	No	Yes	Yes	\$39.99 per month

Our findings reveal that popular apps work on both iOS and Android, and more importantly some of them support remote installation. Only one of them needs jailbreaking or rooting which makes the installation process much more feasible for perpetrators with low IT skills. It is also important to emphasise here that those apps can work in stealth mode which makes those apps invisible to the victims. Finally, the costs can be reported as affordable with a minimum cost of \$4.99 per month.

The interview data indicates that there is no specific profile for perpetrators of technology-facilitated domestic abuse. Any person already being abusive to or having the potential to be abusive to their partner or family member, is also likely to use technology to further the mistreatment. In addition, technical skills do not appear to be necessary in order to perpetuate most forms of technological abuse, particularly as there is a wealth of information and tools readily accessible and available online for would-be TFDA perpetrators.

I think the more that people realise that devices are so readily available online I can see it becoming more of a problem. I mean, if you go on YouTube, you can find videos about how to fit trackers on cars without being caught. So, it's things like apps and, kind of, websites that you can connect phones to and stuff, that you can watch where they're going and what they're doing, you could argue that you are doing that to keep your child safe or to keep your wife safe. You're not doing it to track them and to control them, you're doing it to keep them safe, I've got consent for this. So, it's one of those things, they're marketing all of these products which, I mean, really, you and I know that they're not the best things in the world and it's easily accessible to perpetrators. But they can get away with it under the guise of, oh, we're keeping people safe (Interviewee 7)

Some indicative distinctions, however, have been made in the forms of abuse and the educational level and professional status of perpetrators. Perpetrators who are less educated (have not attended university) and are unemployed or in minimum wage jobs appear to engage in more overt technological abuse - the abusive commentary on social media and/or the accessing of accounts to disparage their partners/ex-partners (this applies to both male and female perpetrators)

Perpetrators who have greater levels of education (have attended university) and are in professional roles, seem to conduct more covert means of technological abuse, utilising spyware and physical tracking devices to monitor and control their partners/ex-partners. This also could be due to a disparity in socio-economic status and the means to afford and access such tools.

Social media abuse is less academic, more overt. The more educated the more insidious...[they] have to the tools to manipulate IT (Interviewee 6)

Perpetrators who work in IT, such as software developers, have been referred to, as well as those who have a personal interest in technology, suggesting that these persons could be more inclined to use technology within the broader pattern of their abuse.

I also find that the more technical software and things like hacking of the wifi and things like that, it tends to be where the perpetrator has a job in technology. And knows how to evade

everything, you know, they can cover their tracks, they know where to get things from (Interviewee 7)

Box 14 illustrates a case of a perpetrator who was an IT consultant

Box 14

An IT consultant working at a University, presented 'abusive' messages from his former partner to the police. The police investigation revealed that the consultant had bought a second mobile phone, engaged in a conversation between his left hand and his right hand, to his ex-partner's number on the phone – in order to fabricate that she was threatening violence against him. He would then download those messages using the university's technology and manipulate them to show her correct telephone number on them.

In another case discussed in the interviews, a perpetrator who is a security professional, installed dedicated surveillance apps and devices, such as bugs, car trackers and tracking on his children's phones, to monitor his ex-partner.

This guy is super dangerous. I think he's quite unusual to have that level of access and that level of knowledge to be able to set that up, because what the victim has said is that since having her phone like cleared and debugged and completely reset and everything, she can now hear clearly, there's always been like a faint buzz that she's never really noticed on her phones, ever, but now we've done that she's like, oh God, like... (Interviewee 17)

Age was noted as potentially impacting upon the types of apps or software used in TFDA perpetration, with younger persons (30's and under) engaging in authorised access to accounts and the creation of fake profiles, whilst older people (40+) employed physical covert devices. This could be linked with the educational and professional status of perpetrators as above, as well as the socio-economic means. Social media use is ordinarily more prevalent with younger people and part of their daily activities, which are then drawn on to perpetuate abuses.

In cases where the victim and perpetrator are younger, I would say it's a lot more hacking Facebook, making the fake profiles, using things such as Snapchat or Strava. In the cases where the perpetrators and victims are a little bit older, I've actually noticed it's more the listening devices and cameras. I find definitely in the under 30s it's more using social media to get what they want (Interviewee 7)

11. Hidden Groups

Domestic abuse is generally considered a gendered phenomenon, with women perceived to be the victims and men the perpetrators due to the overwhelming evidence supporting this, as a result other victims and indeed perpetrators are often overlooked. Consequently, research has been dedicated to examining this gender asymmetry, concentrating on the historical and socially constructed influence of the patriarchy in enabling men to control and subjugate their female partners (Fisher, 2003; Walsh et al., 2015). This has led to a gap in knowledge about the domestic abuse experiences of hidden groups such as men as victims, women as perpetrators, persons within the LGBTQI+ community, BME individuals, and disabled victims.

Due to the nature of the majority of organisations which took part in the research, interview participants have primarily spoken about heterosexual relationships, whereby the male is the perpetrator, and the female is the victim. However, some cases have been discussed which involve same sex couples - both male and male, and female and female, as well as child to parent abuse. Further, due to the type of support provided by one particular charity interviewed, there is also insight into females as perpetrators and males as victims. Gendered roles and stereotypes are significant in these domestic abuse contexts.

According to this charity, men have reported that they've been victims of image-based sexual abuse, as they have had images taken of them when they've been asleep or under the influence of drugs or alcohol, which they have either consciously or unconsciously taken. Sexual acts have also been committed upon men when they've not been in a conscious state, which have been recorded or photographed, and those images shared with other people. Box 15 illustrates a particular case example.

Box 15

A man in his late 40s who was well known within his community, was drugged and coerced into having sex with his then partner. When he was asleep, she then committed acts of sexual abuse upon him and took photos and filmed it. He did not know about this until the relationship ran into problems later, and his ex-partner then used the images to blackmail him. The man was unaware that any illegality had occurred until he sought advice from a men's domestic abuse service. He was reluctant, however, to report the abuse, because as a professional with an established reputation, he didn't want to lose his credibility. He also didn't want other men to perceive him to be weak and so he did not want to speak out or disclose what had happened to him.

Other organisations, however, that support any adult victims, of any gender, indicate that where the perpetrator is female and the victim is male, women use lower levels of IT, and usually exert verbal abuse towards their victim via social media and will try to access their accounts to monitor what they are doing.

Although heterosexual and LGBTQI+ people may experience similar patterns of domestic abuse, national UK LGBTQI+ anti-violence charity Galop⁹² highlights the specific issues unique to the experiences of LGBTQI+ people, such as the threat of disclosure of sexual orientation and gender identity to family, friends, or work colleagues. Other issues include an increased isolation due to a lack of family support, undermining someone's sense of gender or sexual identity, limiting or controlling access to spaces and networks relevant to coming out and coming to terms with gender and sexual identity. The abused may also internalise the abuse, believing they deserve it due to negative beliefs about themselves; the abused may believe that no help is available due to perceived and/or experienced homo/bi/trans phobia of support services and the criminal justice system.

Furthermore, drawing on society's heterosexist myths about aggression and violence, abusers may convince their partners that others will not believe the abuse is real, some abusers may manipulate their partners into believing abuse is a 'normal' part of same-sex relationships, and/or abusers may pressure their victims to minimise abuse to protect the image of the LGBTQI+ community.

In some same-sex cases, discussed by interviewee 1 involving female partners there was active recruitment of others to join in with the abuse and selling of data. The perpetrators allowed others online - access to their victim's accounts and encouraged them to harass the victims. This suggests that having a public aspect to the abuse was important to the perpetrators in these situations.

What I noticed was, they were including and recruiting other individuals. So while it seemed like it was really hi-tech and there were lots of accounts hacked, lots of damage, impact was massive for the victims, which it was, it wasn't because the woman had done it on her own. She had sold data, she'd allowed other people to have access in and harass, and coerce the person as well. So other people were recruited in that process. There's at least three that I can think of, that were all so similar to the point where I thought they all had the same perpetrator. And they didn't. They never knew each other. They lived in different parts of the country, but their examples mirrored each other....It was completely different people and they didn't know each other. There was no connection, but everything that happened, the pattern of behaviour was exactly the same. Friends, associates. You know, sometimes you can sell the data on third party websites as well, so, you know, you get £100 if you sell someone's email and password, and then, you know, they can do the rest. So sometimes it isn't someone they know necessarily, but sometimes it's associates, that they've portrayed, that they're the victims, so let's get back at this person and hack into their account to try and find evidence of abuse. And then people are recruited in that process, trying to help, and giving that perpetrator the information that they need. (Interviewee 1)

In a same-sex case involving male partners, the victim also had disabilities, which the perpetrator exploited to facilitate their technological abuse and harassment against them see Box 16

Box 16

A man in his 60s who suffered with neurological deficiencies, separated from his younger abusive husband. Due to his condition, the man would have to go to bed at nine o'clock and would not be able to get up without carers. He had to keep his phone on and nearby because it was linked to his telecare monitor, safety network, and the hospital because he would have seizures. The ex-husband, knowing this, would ring the phone all night, from unknown withheld numbers constantly – blocking access to it. The man was unable to sleep and endured this for eight months.

⁹² <http://www.galop.org.uk/wp-content/uploads/DV-A-LGBT.pdf>

In terms of ethnicity, some cases described have involved perpetrators and victims from Eastern Europe, in which cultural differences and a lack of legislation recognising coercive control as domestic abuse in their home countries, were suggested as factors influencing the abuse.

In one case involving a Polish heterosexual couple, the perpetrator fits with the typology of the avenger, as his motivation was to destroy his former partner's life. His strategy was to involve others, obtain custody of their child, gaslight and isolate her, using her religious beliefs to present her as insane, see Box 17.

Box 17

A woman was maintaining a parenting relationship with her ex-partner and believed they were on friendly terms. Her ex, though, planned to get his revenge on her for ending the relationship. He planned and organised, including recruiting a neighbour to watch her and her and record what they were doing in the park opposite. The ex would then send text messages describing what she had been wearing on a particular day.

The ex was also able to listen to everything that was going on in her flat. There was an occasion where her benefits had been delayed. The ex then contacted children's services, stating that his child had no food, they were being starved. She would then receive contacts and calls from children's services. She also had police turn up in the middle of the night after her child had fallen and cut themselves. Within about an hour of her having that conversation with someone on the phone she had the police at her door with a child abuse allegation. She would also get contact from health visitors that she was having a mental breakdown, because she had been recorded on the telephone talking to her mum in a different country – and she had expressed to her mum "I'm going crazy, I don't know what's going on here, he seems to know everything what's going on". The ex suggested that she was mentally unwell and was religiously controlled, as she was a practising Catholic. This abuse continued through a custody battle over the child, in which the ex was producing information procured from his monitoring of the victim's flat, as evidence to support his case. Eventually, it transpired during the court proceedings that he had used a covert listening device and so he was prosecuted for this despite his defence that he was just looking out for his child and a lack of appreciation for UK law being different to that of Poland.

12. Harms of Technology-Facilitated Domestic Abuse

Technology-facilitated domestic abuse has serious impacts upon victims, both psychologically and physically. For many victims, there is not domestic abuse and then technology-facilitated domestic abuse; rather, in varying degrees, in different ways, and with very real impacts – digital technologies simply feature in a constellation of violations by an abusive partner or ex-partner. Perpetrators online and their motivations are not different from those offline. Victims have always experienced both contact (physical violence) and non-contact (coercive and controlling) abuses. Digital technologies merely provide new tools and opportunities to extend the repertoire of non-contact forms of harm.

Comparisons are made with sexual assault to the intrusive nature of these abuses, which are facilitated as part of a broader pattern of coercive and controlling behaviour.

I'd say that when we've spoken to women, they say it's intrusive as being assaulted sexually assaulted. And quite often, there's visual cameras in the property. They suspect there is, they're trying to find them. And they know they're being watched; their every movement is being watched. They can't...there's no safe way to speak to somebody, communicate, get help, you're never left alone. Imagine what that does to somebody's mental health. It really, really makes somebody, it helps that facilitation of gas lighting, making somebody think they're going crazy (Interviewee 1)

The feeling of constantly being monitored, not having secure means to communicate with others, and questioning one's sanity through being gaslighted, affects the mental and physical health of victims. Technology is utilised to further control victims and remove what little autonomy and independence they have from the perpetrator.

Interviewee 6 stated that all the women they have supported have made comments such as *I'd rather be punched, because I can see a punch coming, I know how to deal with a bruise*, in regard to the impact that TFDA has upon them.

Interview participants have highlighted how the knowledge or suspicion that their perpetrators are accessing their accounts, have installed or using monitoring trackers/devices in their homes or on their vehicles, are disseminating malicious content about them online, fuels increased feelings of anxiety, panic and paranoia in victims, to the extent that their lives are consumed by fear.

The indication thus far, is that the severity of the harms caused through technology-facilitated domestic abuse are minimised by the authorities when compared with physical violence, suggesting that greater awareness and understanding about coercive control in general, is still required, despite the introduction of national training programmes aimed specifically at criminal justice professionals (Brennan, Muhill, Tagliaferri and Tapley, 2021).

The fear arising from TFDA can also be a barrier to victims reporting, along with the reluctance to part with their devices, which need to be investigated for evidence

linked with the fear is the strength to report it, because they've been so coerced and undermined and frightened, that they do need that empowerment, or, putting it politely, that

hand to hold, that actually says, let's get you to the police station, you can live without your phone for three months, we'll give you a temporary phone. But it is that barrier (Interviewee 6)

Digital devices, especially mobile phones, constitute people's lifelines and to be without them would be more than merely inconvenient in some cases, as they could be the only means of communication and work. Further, victims might want to monitor their abuser's social media accounts so that they know what they are up to, and what the victim in turn can expect from them.

The impact of TFDA can become a constant feature and the majority of victims just want it to stop:

Mainly, they just want to be left alone. They just want to move on. They just want to be able to live without looking over their shoulder, constantly questioning everything. And just to feel safe (Interviewee 4)

12.1. Personal data most commonly targeted for stalking

In order to further understand the risks that technology misuse can cause to victims, we identified the personal information that is targeted by the stalking apps and the websites. Location (GPS), text messages and call logs are the most commonly targeted personal data. It is also apparent that online activities of the victims are monitored, and browser history, instant messages and social media activities are the most frequently targeted by the technologies for stalking. In addition to accessing personal information, we also found suggestions related to recording data via monitoring keystrokes and activating the microphone or camera on the victim's data.

Table 41. Personal data most commonly targeted for stalking

Type of Misuse	Data	#Apps	Definition
Access	GPS	119	GPS location
	Text	81	Text messages (the ones given as text messages and do not include instant messages WhatsApp, Facebook etc)
	Call logs	63	Details of the calls including date, duration, name of caller
	Browser History	53	List of websites that you have visited recently
	Instant messages	42	Messages on a range of instant messaging applications, including Facebook, Instagram, Skype, WhatsApp, Viber, Kik, LINE, and others.
	Social media details	34	Activities on Social media including Facebook, Instagram, Twitter, and others
	Photos	33	Photos both taken and received
	Contacts	26	Contact details on the phone
	Apps	22	Apps installed on the phone
	Video	22	Videos on the phone

	Emails	10	Emails sent or received
	Calendar events	6	Calendar
	Screenshots	6	Taking screenshots of the phone remotely
	Youtube	5	Youtube history
	Device usage	3	Active times on the phone
	Files	3	Files on computers
	Notes	3	Notes on the phone
	Data on iCloud	2	Data stored on iCloud accounts
	Porn	2	Porn websites accessed
	Wi-Fi	2	Nearby Wi-Fi hotspots
	Battery level	1	Battery level of the phone
	Chrome saved logins	1	Login credentials saved at Chrome
	Dating profiles	1	Accounts at dating apps
	Programs	1	Program usage history
	Reminders	1	Reminders on the phone
Record	Camera	39	The remote access to the camera of target phone that allows you to see take photos remotely
	Audio	25	Ambient recording
	Keystrokes	10	Recording (logging) the keys struck on the keyboard
Limit	App locking	11	Restricting use of some apps remotely
	Internet time limits	9	Setting time limits for internet use
	Block websites	7	Blocking specific websites
	Limit calls	6	Limiting calls coming from specific people or setting time limits
	Limit text	6	Limiting text (no further definition provided)
	Lock device	6	Locking device remotely
	Access to Facebook	1	Limiting access to Facebook
	Access to Fortnite	1	Limiting access to Fortnite
	Access to Youtube	1	Limiting access to Youtube

13. Support for Victims of Technology-Facilitated Domestic Abuse

Some solutions for TFDA are overly simplistic and/or have victim blaming connotations, for example expecting victims to refrain from using technology. Douglas et al. (2019) state that a 'technology detox' or disconnect is unfair because it is the abuser who has misused technology rather than the victim who has been abused, and yet they pay the price. It is also impractical because increasingly even routine services and activities require a connection to technology and is potentially unhealthy because it increases isolation and may obstruct the victim's ability to engage in work, education and social life (Douglas et al., 2019).

One of the first steps in mitigating TFDA is recognising when and how it is occurring. Victims are often disbelieved or not taken seriously when they have suspicions that their partner or ex-partner is engaging in TFDA against them. They are aware that their abuser is privy to information and knowledge about them that they ordinarily should not have access to, and so victims have concerns that their accounts have been breached and they are being spied on. With little evidence to support their apprehensions, because they do not have the means to obtain it, victims may be disbelieved and considered paranoid by family, friends and the authorities. This may form part of the broader pattern of abuse and gaslighting tactics of the perpetrator.

They [victims] suspect something's happening, so they'll come to us and say, I think that he's been in my accounts, because he's mentioning to me that he knows contents of emails from solicitors. Or sometimes they go to court and he produces bundles of information that he's taken from her online accounts, banking accounts, email accounts, social media, because he's hacked into them. And he produces that in court and they don't think anything of it. I mean, if you need more evidence that someone's abusing you, tracking you, monitoring you, you can't get more evidence than an 8,000 document, which shows someone's every waking movement. And the Judge just wouldn't have it, he was like, that's not, you know...that's not domestic abuse. So what can you do in that situation, when the evidence is in front of somebody and they're refusing to acknowledge it? (Interviewee 1)

It is recognised that a one-size-fits all approach is not feasible in domestic abuse contexts. The circumstances of each case and the individuals involved need to be taken into consideration. There is, nevertheless, general guidance that can be offered to victims who are experiencing TFDA, which could be implemented if they are able and safe to do so. In providing any advice, service providers have to be careful about alerting the perpetrator and putting the victim at risk of increased harm. For example, the removal of spyware or tracking devices could escalate perpetrator's behaviours, as they would be aware that their victim knows they have been monitoring them, and the perpetrator no longer has that control over the victim. In situations where victims are planning to leave their abuser, it is pertinent to consider all the protections necessary and be ready to implement them immediately upon ending the relationship.

As the onus is usually and unfairly placed with the victim to collate evidence of the abuse, practical support is necessary to protect the safety of the victim. Ensuring the safety and security of the victim is paramount. In the following quotation, advice about securing evidence from Snapchat, which is favoured by perpetrators due to its instantaneous deletion of messages, is provided:

If you screenshot in Snapchat it tells the other person you've taken a screenshot, so we always advise if things like that are potentially happening, use another device to take the picture so you can see it on the phone (Interviewee 11)

Snapchat along with other platforms such as secret conversations on Facebook and the timer function on WhatsApp, enable perpetrators to send abusive messages to their victims, which will automatically disappear after having been read, instantaneously removing all traces of their harassment.

Some service providers described how instead of advising victims to block perpetrators, which will remove the opportunity to collect evidence, is an insight into the mindset of the perpetrator and can also be a forewarning about their escalating behaviours. Instead, they recommend using features such as archive or mute. This means that messages are still received, however, perpetrators would not know when they are being read, they would only be aware that the messages are being delivered.

We've moved on from it used to be block them, because if you block, you've removed the access point, whereas now we can use features like archive or mute...we use that because that's the evidence and usually if a perpetrator's coming to do serious harm, they seem to tell us first (Interviewee 11)

Overall, the interviews highlighted that although service providers are aware of the significant role that technology is playing within the facilitation of domestic abuse, and are attempting to support victims appropriately, there is still a great deal of knowledge and training required to fully appreciate how technology is changing the nature of domestic abuse.

Right now, no, a lot of our services tend to be very much in the physical space or tend to deal with domestic violence as a physical crime, and I'd say that is where the public sector hasn't really kept pace. We know that domestic violence takes place online as well, like cyber bullying, but our service provisions tend to be very much shelters, workers keyworkers, support officers, social workers who deal with the physical act and taking people out of a situation. But when you talk about a phone and other digital devices, I don't think we're there yet. I think it's just beginning to change the landscape in terms of what we consider to be domestic abuse. (Interviewee 19)

Nevertheless, there are some key UK organisations that provide helpful guidance to victims of TFDA, Appendix 3 provides details of these.

14. Criminal Justice System Responses to Technology-Facilitated Domestic Abuse

We also collected data on the offences the offender was prosecuted for and the sentence they received in the media cases. Some were prosecuted for multiple offences. For the sentence received the principal sentence was recorded, where multiple sanctions were applied. However, because the vast majority of cases involved multiple charges and/or utilised offences such as stalking/harassment and coercive control, of which technology was only a small part, further analysis of sentences was not felt appropriate. Therefore, only the offences used for prosecution are assessed here. Table 42 below begins with the cases for England and Wales where there was a criminal case, illustrating the prosecution offences used. In some instances, in the sample of 108 cases, there was no prosecution, or it was linked to a divorce and therefore a civil case.

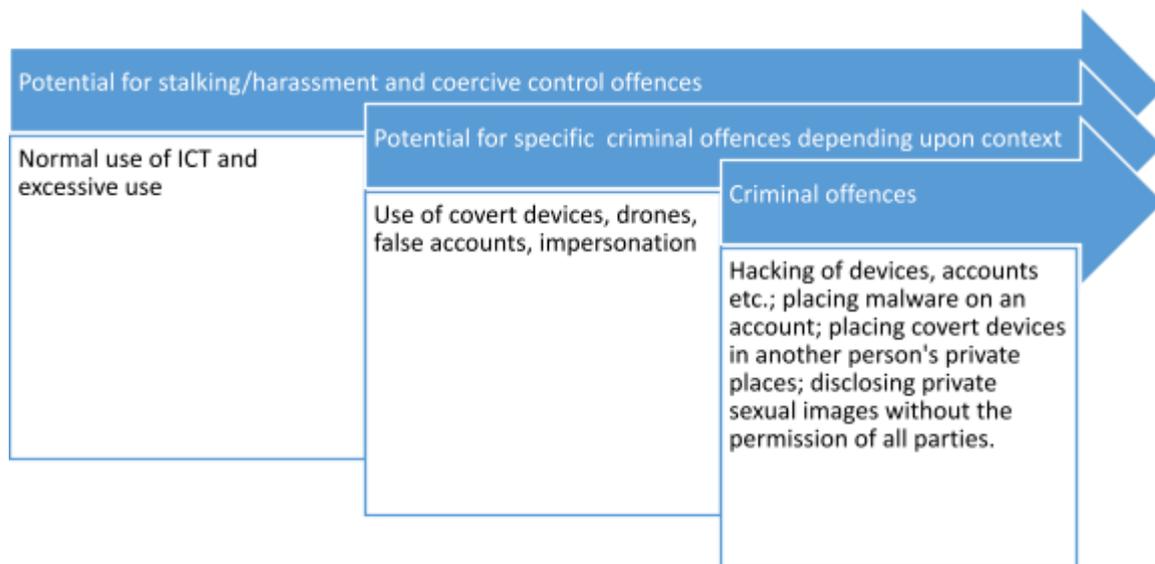
Table 42. Prosecution offences used

Prosecution offence	N
Stalking and harassment	45
Cases where coercive control used	26
Cases where disclosing private sexual images used	22
Cases where serious offences of murder, sexual assault, GBH, firearms etc were used	9
Cases where Computer Misuse Act used	4
Cases where Malicious Communication used	3
Cases where perverting the course of justice used	3
Cases involving telecommunications offences used	1
No prosecution or civil case	5

Note: 1 All cases above are where the offence was listed and, in many cases, more than one charge was made meaning cases exceed 108.

The most significant finding from this table is that the Computer Misuse Act offences are rarely used for prosecution. Only 4 cases were found in this sample of cases in England and Wales and 55 cases in the 108 involved unauthorised access. Clearly prosecutors prefer to use the stalking/harassment legislation or coercive control. Figure 10 below illustrates further how different types of technological abuse can be captured under different types of criminal legislation.

Figure 10. Technological abuse and the potential for criminal legislation



In the interviews, however, service providers spoke about how perpetrators were able to evade criminal justice sanctions whilst engaging in TFDA. This was often due to an inability to collect the requisite evidence, perpetrator’s savviness in using technology to cover their tracks (such as using Snapchat, which automatically deletes messages; or using WhatsApp with automatic removal timers) and a general lack of understanding within the CJS about how technology is utilised within an ongoing pattern of domestic abuse.

Delays impeding investigations also impact upon TFDA perpetrators being brought to justice.

A lot of perpetrators are getting clued in to how long it takes the police to access things like WhatsApp and Snapchat...because of the length of time it's taken to get those permissions, it's not worth the crime going forward, which is something we are seeing an awful lot, the length of time from the crime to the trial it's not worth the trial anymore, it's not worth the cost of the crime...because once that's gone, it's not gone forever but it is, from the point of application to get access to the WhatsApp messages, Snapchat and Facebook, it's 13 months because it goes through the American process (Interviewee 11)

The lack of applicable legislation to tackle distinct forms of TFDA was also noted as problematic. The following quote highlights the necessity for the forthcoming Online Harms legislation to consider this in the context of domestic abuse.

What I've noticed, that there is a gap in terms of provision of keeping people safe from say online harms. And I think the law is still catching up with where technology is, it's only recently in England that we've made say sharing of images by ex-partners or I guess husbands illegal, while in Wales they had that come into force. think I guess the judicial system, the police are somewhat behind in terms of where technology is, and law and regulations have to keep up, but for every legislative measure, technology precedes it, there's something new out there, there's a new piece of software which the law doesn't quite cater to just yet and the new crime that's committed. (Interview 19)

Often, the issue is that coercive and controlling abuses, of which technology is part of, are treated as isolated incidents rather than part of a larger pattern of abuse. This can also mean that unless something serious occurs there is limited recourse via the CJS. In this study, interviewees advised that victims were literally told by responding police officers that nothing could be done until the perpetrator had actually committed an offence (as perceived by the officers), which in some cases would be too late to protect the victim. Where coercive and controlling behaviour is recognised and legislation can be applied, service providers stated that it would be prudent to combine it with computer misuse offences *because that's what it is , to enable them to exert that control, they are misusing electronic devices...another charge of coercive controlling behaviour using computer misuse, that technology, that kind of needs to be a link* (Interviewee 11)

Although there is some evidence that initial police responses are improving, this remains inconsistent and this has a negative impact on victims' confidence and their willingness to remain engaged with the criminal justice process:

On the whole, I'd say it's [police response] fairly positive. Obviously, you do get the odd ones where they'll ring up to report and have a bad experience. Someone on the other end won't be very understanding. And then that sets the tone for the rest of it really. I think it's easy for trust to be broken. And I think it's hard to gain back once it's been broken.' (Interviewee 4)

Evidence from the interviews undertaken with specialist services demonstrates the key role of specialist advocates in improving the safety and protection of victims, providing ongoing support and assisting victims through the often, slow, complex and confusing stages of the criminal justice process:

Every safety plan I do has got a big bit on online safety, thinking about the devices, thinking about the passwords, thinking about everything because it's all there. It's all around the things we are noticing and what we do as best practice is when we come across something that we don't think is out there it's shared across the board, like the Just Eat thing. As soon as that happened, it was shared with everyone, be alert, be aware... we need to keep ahead of it, we don't sit on anything we've seen, because that's the best way for us to always be ahead of the game (Interviewee 11)

It's the linking in as well. Sometimes the police like for some reason, it will get lost in the system, it won't be picked up... and that's where I come in and highlight it. And then they actually go...that is quite bad, we should look into that. And then it will get picked up again. So it's just to help to keep it all linked together (Interviewee 4)

Wife battering and domestic violence was once referred to as a hidden crime, but our knowledge and understanding of the nature and impact of domestic abuse has changed significantly, as has the criminal justice response. But ways of perpetrating domestic abuse continually evolves along with the development of technology, so it is essential that our knowledge and understanding continues to evolve, so that victims can have confidence that the criminal justice system is there to support them and that the harms they suffer will be seen:

The impact is just complete deterioration of their mental wellbeing, isolation, there's the financial abuse because of the access to the online banking, and the fear of nobody's ever going to finally find out what went on, and there has been a few lately that say know one will ever know,, see if he kills me, no one will ever know what he did to me because he's hidden it so well, and that just destroys me, but it's true (Interviewee 11)

15. Conclusions and Recommendations

As technology becomes ever more ingrained into our everyday lives, hastened further by the Covid pandemic, which has driven many more human interactions and tasks online, technology-facilitated domestic abuse is undoubtedly a harmful behaviour that is only going to escalate and increase further the risk of harm, unless appropriate interventions in prevention and enforcement occur.

Below we set out our key conclusions arising from this research.

- Technology-facilitated domestic abuse (TFDA) very rarely occurs in isolation, it is usually part of a wider continuum of abuse, which is not separate from other coercive and controlling behaviours. Offline and online abuse is interconnected and within the context of domestic abuse, often co-occurring. Therefore, TFDA might be better understood as different tactics of patterns of perpetrator behaviour rather than distinct types of harm. However, it is necessary to highlight the specific instances and tactics of TFDA in order to ensure that policy, legislative and support responses appropriately consider these rapidly developing practices of abuse.
- Computer misuse offences, especially unauthorised access, feature within domestic abuse contexts, however, these only account for part of the issue. Domestic abuse perpetrators are engaging in a broad range of behaviours involving the use of technology – including use of spyware, creating fake accounts, online harassment, stalking and installing trackers, and image-based sexual abuse, some of which encompass and combine offences within legislation such as the Computer Misuse Act (1990) CMA, Malicious Communications Act (MCA) 1988, the Protection from Harassment Act (PHA) 1997, the Stalking Protection Act (SPA) 2019, the Criminal Justice and Courts Act (CJCA) 2015, and the Fraud Act 2006, but also those not necessarily illegal yet are still harmful activities conducted as part of a wider pattern of coercive control.
- The problem of TFDA is, however, normalised and often considered unremarkable due to societal challenges towards privacy and the right to keep aspects of (digital) life separate. Context is therefore significant in recognising unhealthy behaviours; therefore, relationship-based understandings of domestic abuse and technology use are critical. There is a need to avoid reinforcing the limited public narrative of domestic abuse, where coercion and control are not viewed as significantly harmful as physical violence. Without discouraging healthy relationships, more awareness needs to be publicly available about abusive relationships and unhealthy behaviours, as well as education about independence and online safety.
- The information available to perpetrators on the web enables individuals to find, source and apply such technologies to harm others in their domestic environment. In particular, stalkerware apps are marketed to information seekers who want to abuse or control their victims via technology. These products are generally advertised on their official webpages as parental tools or employee trackers. This ambiguity is concerning since legitimate statements have the potential to normalise the use of these apps and encourage people to install them, providing motivations such as protecting their families.
- Devices used to monitor physical identity of individuals such as location, image or sound are also accessible via websites. Covert cameras and microphones or GPS trackers are easily obtainable from popular online retailers such as Ebay and Amazon. The wide range of forms that these devices can be hidden in is concerning, especially when the ones in toy shapes are considered. These devices enable perpetrators to access victims via their children and the gifts given to children become more of an issue. It is important to note here that the variety of options is much higher in local retailers in the UK compared to global ones.

- Within coercive and controlling relationships, the use of technology to further that abuse is likely. Perpetrators may already have manipulated access to their partner's accounts or are already accessing them or spying on them without their partner knowing. When a victim is considering leaving or has left their perpetrator, the extent of TFDA will probably increase, or where it has not already occurred, it is likely to be implemented. This is because the perpetrator is seeking to regain/gain control, or due to other motivations, which may overlap, such as revenge, surveillance, attempted reconciliation, to secure evidence of infidelity, secure evidence for divorce/child custody proceedings, financial gain, curiosity, to pervert justice, or obtain sexual gratification. From these motivations it was possible to develop a typology of abusers. They include **the curious, the investigator, the deviant, the controller and the avenger**.
- Children are increasingly being involved in technology-facilitated domestic abuse contexts, especially as a means for perpetrators to exert control in post-separation shared parental situations. Children are being used to facilitate the abuse of the other parent, their devices such as phones, tablets and games consoles, are exploited by perpetrators to monitor and maintain control over victims. It is also during the break-down of the relationship that another key driver for technological abuse develops - child contact/custody cases.
- There is no specific profile for perpetrators of technology-facilitated domestic abuse. Any person already being abusive to or having the potential to be abusive to their partner or family member, is also likely to use technology to further the mistreatment. Technology-facilitated domestic abuse does not require technical proficiency. The majority of the tools used by perpetrators are everyday technologies, readily available, accessible and familiar. Apps are affordable. The majority of them do not need jailbreaking or rooting, which makes them usable for people with average IT skills. There are, however, indications that those with higher levels of education and/or in IT professions are conducting more covert means of technological abuse. There are also potential differences in regard to methods perpetrated by age, with younger persons (30's and under) engaging in authorised access to accounts and the creation of fake profiles, whilst older people (40+) use physical covert devices.
- An Intersectional approach appreciating the converging lived experiences, causes and realities of TFDA is necessary, particularly as the experiences of those suffering TFDA who are not cisgender heterosexual, from the UK, or able-bodied are often missing from the public discussions, rendering the invisibility of these marginalised groups.
- For many victims, there is not domestic abuse and then technology-facilitated domestic abuse; rather, in varying degrees, in different ways, and with very real impacts – digital technologies simply feature in a constellation of violations by an abusive partner or ex-partner. The harms from TFDA, therefore, are no less serious than those arising from other forms of coercive and controlling behaviours and physical violence.
- Solutions to TFDA often involve advising victims to disengage from technology, which is not only unfair to victims, but often infeasible given our increasing reliance on digital technologies. It could also heighten their risk of harm, isolating them from family, friends and professional and social networks, and reducing their ability to request and receive support. Therefore, a one-size-fits-all approach in supporting victims is not possible.
- Perpetrators who are committing computer misuse offences as part of their pattern of abusive behaviour are rarely being charged with these crimes. These offences are often being overlooked in the context of stalking and harassment or control and coercion.
- The ongoing use of technology increases the long term traumatic and psychological impacts on the victim, perpetuating feelings of being trapped and unable to escape the abuse. The use of technology to facilitate abuse should be recognised as an aggravating feature and result in an increased sentence.

Preventative Lessons

This research has identified some key findings that can be utilised to develop improved prevention strategies to tackle some of the technology-facilitated behaviours uncovered in this analysis. Many of these overlap with cyber hygiene advice that is already well publicised, although the research indicates a need for an increase in both public and CJ professional awareness and understanding.

For individuals

Change of all passwords when a relationship ends. It would seem prudent for intimate partners to change all passwords on accounts and devices when a relationship ends. Even if there is no evidence of technology-facilitated abuse, the other party might not know this would seem to be a common risk.

Avoid passwords an intimate partner might guess. If a relationship ends or in a current relationship where the partner does not want the other to have access to their accounts, it would seem prudent not to use passwords that could be guessed.

Be aware of privacy settings on your device: some settings can reveal where you are and if you do not want people to know this, these should be switched off.

Check any devices with internet connectivity given as gifts or which the partner may have access to: Any device which can be linked to the internet which is given as a gift should be checked for any spyware trackers pre-installed (mobile phones, laptops, fitbits, etc). Cookies should be deleted, and the browser history cleaned. Some devices where it is not easy to check might be better discarded or switched off. In some cases, it might be prudent to secure an IT expert's advice to check devices, particularly as spyware apps work in stealth mode and notify the perpetrator as they are uninstalled.

Be aware of app's remote installation capabilities: Installation becomes easy once cloud credentials are known and, therefore, it is important to check for new apps appearing on devices if your cloud details are known, or you think they might have been uncovered.

Check the privacy and use of facial images and email addresses on social media accounts: These are personal identifiers that can be tracked back easily with Google's different search facilities.

Regularly sweep private residence and vehicle for trackers, covert devices. Persons who have partner's or ex partners who are a concern should regularly check where they live and their vehicle for any devices which might have been placed there for surveillance purposes.

Private images and recordings: Encrypt any files holding such images/recordings. If a relationship ends, destroy images.

Friending: Be careful to check any person seeking to 'friend' you on a social networking website.

Communication: Do not assume a person you know communicating with you is who they say they are. If suspicious, use other means to check.

For government and enforcement

Domestic Abuse Bill: Specific inclusion of the recognition of the role that technologies can play in facilitating and exacerbating domestic abuse within the Domestic Abuse Bill

Fake accounts: There would seem to be a gap in legislation relating to impersonating another person online. Given impersonation seems to be a significant aspect of this type of abuse further research should be undertaken as to whether current legal provisions are appropriate for this and reflect the significant harm that can be caused.

Covert devices and apps: Covert cameras, listening devices and vehicle trackers would seem to be used negatively in many cases. Clearly, they have uses for legitimate purposes, such as for safety, parental controls, and private investigators investigating workplace crime, for example. However, further research into controls on the advertising, sale of such items or regulation of their use should be considered, particularly via the forthcoming Online Harms Bill.

Spyware: Given that spyware are designed and implemented purely for abusive purposes, urgent research into controls on the advertising, sale of such items or regulation of their use should be considered, particularly via the forthcoming Online Harms Bill. Platforms that allow access to technologies that are clearly abusive, such as Google, Amazon and Ebay require stricter controls. For example, Google's policy on stalkerware is inadequate given the fact that those apps are advertised as parental tools⁹³.

Risk assessment, repeat offences and serial offenders: Many cases involve repeated acts and, in some cases, regular behaviours that have subsequently escalated. There needs to be a greater understanding and recognition of the indicators of high risk when perpetrators are using technology to facilitate abuse. It needs to be incorporated within the risk assessment models being used. If risks can be identified earlier there will be opportunities to intervene earlier and perhaps prevent behaviours from being repeated or escalating further. Using civil injunctions and criminal behaviour orders earlier could impact upon repeat offending and reduce future serial offending.

Police training: Training policing staff in the full range of potential criminal offences which can be used. Some offences seem to be under-utilised (Computer Misuse Offences), which could often be used earlier in cases against offenders.

Victim centred responses: In responding to victims, responsibility for the abuse must be placed firmly with the perpetrator and there must not be an expectation that the victim change their behaviour in order for the abuse to stop. A thorough risk assessment must be undertaken in order to identify wider patterns of abusive behaviour and to ensure the behaviour is not identified and responded to as a one off incident, which by itself does not constitute a criminal act.

Children: Children's voices are significant. They are being used to perpetrate abuses, whether overtly or covertly and are victims of technological abuse too. It is important to listen to childrens' accounts. The forthcoming Domestic Abuse Act will recognise children who witness/live with domestic abuse as victims, regardless of whether they are experiencing physical violence. Where TFDA is occurring, it should be recognised that children are also being victimised.

For tech companies

Fake accounts: More effort to prevent the creation of fake accounts, and removal of those who repeatedly do so.

⁹³ https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265

Algorithms: Algorithms need to be adapted so as to not encourage the sales of spyware and covert devices for abusive purposes, and avoid directing perpetrators to guidance informing them as to how to hack into their partner’s accounts/ stalk partners. Google’s current advertising policy⁹⁴ 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 domestic abuse service providers

Updated training: Technological aspects to be included in domestic abuse training – Domestic Abuse Matters (DA Matters) run by SafeLives

Specialist advocates: The development of specialist advocates with the relevant knowledge and skills. Many services are already developing this specialism, but it must be supported further with sustainable funding.

Further research

This research was predominantly focused on the methods, tools and motivations of perpetrators and though some insight has been provided into the harms experienced by victims, further research could centre upon victims experiences and utilise their voices to fully appreciate the impact that TFDA is having on people’s lives. The inclusion of children and the effects of TFDA upon them also requires more research.

There continues to be gaps in knowledge as to the experiences of underrepresented groups, therefore future research should focus on working with specialist domestic abuse service providers as well as TFDA victims and perpetrators who are BME/ LGBTQI+ / have disabilities.

We hope our findings inform studies that provide digital safety guidelines for individuals, empower and protect victims, and also provide guidance for government and platforms on how to limit the access of these technologies to perpetrators.

⁹⁴ https://support.google.com/adspolicy/answer/9726908?hl=en&ref_topic=29265

References

- Almond, L., McManus, M., Brian, D., & Merrington, D. P. (2017). Exploration of the risk factors contained within the UK's existing domestic abuse risk assessment tool (DASH): do these risk factors have individual predictive validity regarding recidivism?. *Journal of aggression, conflict and peace research*.
- Belknap, J, Chu, A.T, and DePrince, A.P. (2012). Roles of phones and computers in threatening and abusing women victims of male intimate partner abuse. *Duke Journal of Gender Law & Policy*, 19, 373-406
- Brennan, I., Myhill, A., Tagliaferri, G., & Tapley, J. (2021). Policing a new domestic abuse crime: Effects of force-wide training on arrests for coercive control. *Policing and Society*, 1-15.
- Button, M. & Cross, C. (2017) *Cyber Frauds, Scams and their Victims*. London: Routledge
- Button, M., Lewis, C., & Tapley, J. (2009). A better deal for fraud victims: research into victims' needs and experiences.
- 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.
- Chayn, SafeLives, and Snook (2017). *Tech vs. Abuse: Research Findings, Comic Relief*, London. <https://www.techvsabuse.info/research-findings>
- Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187-204.
- Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends & Issues in Crime and Criminal Justice*, 474.
- 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.
- 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.
- Fisher, C. (2013). Changed and changing gender and family roles and domestic violence in African refugee background communities post-settlement in Perth, Australia. *Violence Against Women*, 19, 833–847.
- Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010) "The new age of stalking: Technological implications for stalking," *Juvenile and family court journal*, vol. 61, no. 4, pp. 39–55.
- 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.

GOV.UK (2013) *Definition of domestic violence and abuse: guide for local areas* Retrieved from <https://www.gov.uk/government/publications/definition-of-domestic-violence-and-abuse-guide-for-local-areas>

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.

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.

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.

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/>

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

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.

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.

Monckton Smith, J. (2019). Intimate partner femicide: Using Foucauldian analysis to track an eight stage progression to homicide. *Violence against women*, 26(11), 1267-1285.

Monckton-Smith, J. (2021). *In Control: Dangerous Relationships and How They End in Murder*. Bloomsbury Publishing.

ONS (2020) *Domestic abuse in England and Wales overview: November 2020*. Retrieved from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwalesoverview/november2020>

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: November 2020*. Retrieved from <https://post.parliament.uk/technology-and-domestic-abuse/>

Refuge (2019). *Tech abuse and empowerment service*. Retrieved from <https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/>

Rempel, E, Donelle, L, Hall, J, & Rodger, S (2019). Intimate partner violence: A review of online interventions. *Informatics for Health and Social Care*, 44(2), 204-219.

Slakoff, D. C., Aujla, W., & PenzeyMoog, E. (2020). The role of service providers, technology, and mass media when home isn't safe for intimate partner violence victims: best practices and recommendations in the era of CoViD-19 and beyond. *Archives of sexual behavior*, 49(8), 2779-2788.

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.

Walsh, J., Spangaro, J., & Soldatic, K. (2015). Global understandings of domestic violence. *Nursing & Health Sciences*, 17, 1–4.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims—both financial and non-financial. *Criminology & Criminal Justice*, 16(2), 176- 194.

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.

World Health Organisation (WHO) (2017) *Violence against women* Retrieved from <https://www.who.int/news-room/fact-sheets/detail/violence-against-women>

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

Appendices

Appendix 1 Media cases

ABC News (2020) Man pleads guilty to stalking and controlling ex-girlfriend's car with his computer. Retrieved from <https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980>

Alice Ruggles Trust (2020) Putting an End to Stalking. Retrieved from <https://www.alicerugglestrust.org/events/default>

BBC News (2020a) Lenny Henry's daughter sentenced for harassing ex-boyfriend. Retrieved from <https://www.bbc.co.uk/news/uk-england-cornwall-52560939#:~:text=The%20daughter%20of%20Sir%20Lenny,King%20to%20to%20%C2%A340%2C000.>

BBC News (2020b) Drone stalker jailed for spying on ex-girlfriend. Retrieved from <https://www.bbc.co.uk/news/uk-wales-55018682>

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>

Bolde (2020) I Hacked My Ex's Email After Our Breakup & I Totally Regret It Retrieved from <https://www.bolde.com/hacked-exs-email-after-breakup-regret/>

Cheshire Live (2020) 'One of us will die today' Single mum on how her ex-boyfriend held a knife to her throat before posting revenge porn pictures online. Retrieved from <https://www.cheshire-live.co.uk/news/uk-world-news/one-die-today-single-mum-17748318>

CBC (2018) 'Stalked within your own home': Woman says abusive ex used smart home technology against her. Retrieved from <https://www.cbc.ca/news/technology/tech-abuse-domestic-abuse-technology-marketplace-1.4864443>

ChronicleLive (2017) How fallen hero Trimaan Dhillon went from guarding Royals to life in prison after Alice Ruggles murder. Retrieved from <https://www.chroniclelive.co.uk/news/north-east-news/how-fallen-hero-trimaan-dhillon-12942389>

Devon News (2020). Revenge porn stalker who 'hijacked' ex-girlfriend's life jailed. Retrieved from <https://www.devonlive.com/news/devon-news/revenge-porn-stalker-who-hijacked-4649711>

East London and Essex Guardian (2017) Cem Kucukbalaban of Highams Park, Waltham Forest who subjected ex-girlfriend to 'spiteful' revenge porn campaign on Instagram. Retrieved from <https://www.guardian-series.co.uk/news/15690223.jailed-cem-kucukbalaban-of-highams-park-waltham-forest-who-subjected-ex-girlfriend-to-spiteful-revenge-porn-campaign-on-instagram/>

Echo (2021a) Ex boyfriend sent revenge porn to three year old's iPad. Retrieved from <https://www.liverpoolecho.co.uk/news/liverpool-news/ex-boyfriend-sent-revenge-porn-19805334>

Echo (2021b) Dumped boyfriend created fake swinger profiles of ex in revenge. Retrieved from <https://www.liverpoolecho.co.uk/news/liverpool-news/dumped-boyfriend-created-fake-swingers-19591442>

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>

Grazia (2019) Two Years After Our Break-Up, I Still Read My Ex's Emails. Retrieved from <https://graziadaily.co.uk/life/in-the-news/hacking-exes-social-media-emails/>

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/>

LancsLive (2020) Lostock Hall woman sent threats to kill and messages about his mum's death to ex. Retrieved from <https://www.lancs.live/news/lancashire-news/lostock-hall-woman-sent-threats-17911335>

LeicestershireLive (2020) Leicester woman bravely speaks out after abusive ex-boyfriend is sent back to prison. Retrieved from <https://www.leicestermercury.co.uk/news/local-news/leicester-woman-bravely-speaks-out-4250142>

MailOnline (2021) Model, 25, flees her home and says she will change her appearance after jilted ex-boyfriend vandalised her car, hacked her bank account and sent threatening messages telling her: 'I have your life in my hands'. Retrieved from <https://www.dailymail.co.uk/news/article-9171447/Model-25-considered-changing-looks-ex-left-terrified.html>

MailOnline (2020a) No reservations: Bitter ex-boyfriend of restaurant owner featured on Guy Fieri's Food Network TV show tries to sabotage her business with customer voicemail message saying it has CLOSED down. Retrieved from <https://www.dailymail.co.uk/news/article-7865285/Ex-boyfriend-restaurant-owner-sabotages-business-telling-customers-closed.html>

MailOnline (2020b) The TV set spy: Husband is convicted of stalking after bugging his estranged wife's living room and texting her about the shows she watched. Retrieved from <https://www.dailymail.co.uk/news/article-8951637/The-TV-set-spy-Husband-convicted-stalking-bugging-estranged-wifes-living-room.html>

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>

MailOnline (2018b) Clarinetist wins \$260,000 damages from ex-girlfriend who deleted email offering lucrative scholarship because she didn't want them to be apart. Retrieved from <https://www.dailymail.co.uk/news/article-5848205/Clarinetist-wins-damages-ex-girlfriend-deleted-email-offering-lucrative-scholarship.html>

MailOnline (2016) 'Watch carefully, you can see 18 years go down the drain': Husband 'catches his wife cheating' by using a DRONE. Retrieved from <https://www.dailymail.co.uk/news/article-3936934/Watch-carefully-18-years-drain-Husband-catches-wife-cheating-spying-using-DRONE.html>

Mirror (2019) Woman convicted of revenge porn after sending images of ex's penis to his daughter. Retrieved from <https://www.mirror.co.uk/news/uk-news/woman-convicted-revenge-porn-after-20935604>

Mirror (2015) 'My husband spies on me with a smartphone app - and I don't care at all'. Retrieved from <https://www.mirror.co.uk/news/real-life-stories/my-husband-spies-smartphone-app-5011718>

OutSmart (2017) Man Sues Grindr After 1,100 Men Show Up At Home Thanks To Ex's Revenge Scheme. Retrieved from <http://www.outsmartmagazine.com/2017/04/man-sues-grindr-after-1100-men-show-up-at-home-thanks-to-exs-revenge-scheme/>

PinkNews (2018) Republican legislator accused of sharing ex-girlfriend's naked photos to 'catfish' men on Instagram. Retrieved from <https://www.pinknews.co.uk/2018/08/01/republican-legislator-accused-of-sharing-ex-girlfriends-naked-photos-to-catfish-men-on-instagram/>

PinkNews (2016) This wife took the ultimate online revenge after her husband slept with their gardener. Retrieved from <https://www.pinknews.co.uk/2016/05/26/this-wife-took-the-ultimate-online-revenge-after-her-husband-slept-with-their-gardener/>

SomersetLive (2018) Scorned mum Jorja Davies tried to frame her ex for stalking and threatening her. Retrieved from <https://www.somersetlive.co.uk/news/somerset-news/scorned-mum-jorja-davies-tried-1032829>

Somerset Live (2017) Taunton supply teacher found guilty of spying on his wife. Retrieved from <https://www.somersetlive.co.uk/news/somerset-news/taunton-supply-teacher-found-guilty-257927>

The Guardian (2015) Woman who pretended to be man to trick friend into sex jailed for eight years. Retrieved from <https://www.theguardian.com/uk-news/2015/nov/12/gayle-newland-sentenced-eight-years-prison-duping-friend-having-sex>

The Information (2018) How Amazon's Latest Security Device Let People Spy on You. Retrieved from <https://www.theinformation.com/articles/how-amazons-latest-security-device-let-people-spy-on-you>

The Herts Advertiser (2020) St Albans man jailed for persistent harassment of former partner. Retrieved from <https://www.hertsad.co.uk/news/st-albans-man-jailed-for-harassment-5215354>

The News (2021) Fareham mum posted naked images of partner after finding out he sent naked selfies to men. Retrieved from <https://www.portsmouth.co.uk/news/crime/fareham-mum-posted-naked-images-partner-after-finding-out-he-sent-naked-selfies-men-3113542>

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/>

The Sun (2016) Wife ruthlessly rewrites her cheating husband's Tinder bio. Retrieved from <https://www.thesun.co.uk/living/2309304/wife-rewrites-cheating-husbands-tinder/>

Wales Online (2020a) Teenager posted naked photos of ex-girlfriend on her social media accounts. Retrieved from <https://www.walesonline.co.uk/news/wales-news/crime-courts-revenge-porn-naked-18539119>

WalesOnline (2020b) Man posed as a stalker to 'test the fidelity' of his partner. Retrieved from <https://www.walesonline.co.uk/news/wales-news/rhodri-harries-court-sentenced-jailed-19399950>

Appendix 2 Online Retailers in the UK

Below we list the online retailers which are based in the UK and sell devices that are apparently used to monitor or spy on others. The ones that seem to sell for legitimate purposes (employee tracking, security etc.) are given in italics.

Table 23: Online Retailer in the UK

Online Retailer	Link
<i>CCTV Direct Online</i>	https://cctvdirectonline.co.uk/ (seems legitimate)
<i>CCTV Kits</i>	https://www.cctvkits.co.uk/ (seems legitimate)
<i>CUCCTV</i>	https://cucctv.co.uk/
<i>Dealsan</i>	https://www.dealsan.uk/buy/spy-microphone links to Amazon, Ebay, Etsy
<i>Euspyshop</i>	https://www.euspyshop.com/ (Spy Shop Is UK Based Company, Retail Store In Central London)
<i>Eyetek</i>	https://www.eyetek.co.uk/product-category/spy-equipment/
<i>Micronic</i>	https://micronic.co.uk/
<i>Mscspytek</i>	https://www.msccspytek.com/
<i>Net View CCTV</i>	https://netviewcctv.co.uk/ (seems legitimate)
<i>Online Security Products</i>	https://www.onlinesecurityproducts.co.uk/ (seems legitimate)
<i>Online Spy Shop</i>	https://www.onlinespyshop.co.uk/
<i>Online Spy Shop</i>	https://www.onlinespyshop.co.uk/
<i>Pakatak</i>	https://pakatak.co.uk/
<i>Rewire Security</i>	https://www.rewiresecurity.co.uk/
<i>Spy Camera CCTV</i>	https://www.spycameracctv.com/ (registered in UK)
<i>Spy Cather Online</i>	https://www.spycatcheronline.co.uk/
<i>Spy Equipment</i>	https://www.spyequipmentuk.co.uk/
<i>Spy Gadgets4u</i>	https://www.spygadgets4u.co.uk/
<i>Sure24</i>	https://www.sure24.co.uk/
<i>Talking Head Sets</i>	https://www.talkingheadsets.co.uk/ (seems legitimate)
<i>Tech Silver</i>	https://www.techsilver.co.uk/
<i>Tracker Shop-UK</i>	https://www.trackershop-uk.com/ (seems legitimate)
<i>Tracking Center</i>	https://www.trackingcentre.co.uk/ (seems legitimate)
<i>UK Spy Gear</i>	https://ukspygear.com/
<i>Wi-LTD</i>	https://www.wi-ltd.com/ (seems legitimate)
<i>York Survey</i>	https://www.yorksurvey.co.uk/ (seems legitimate)

DetectiveStore⁹⁵ was returned by Google for several queries but it is not covered in the table above since it is based in Poland.

⁹⁵ <https://www.detective-store.com/>, April 2021

Appendix 3 Guidance for Victims of TFDA

The National Cyber Security Centre (NCSC) with input from the Department of Digital Culture Media and Sport (DCMS) encourage manufacturers of IoT smart devices to create and maintain the security of their products and have developed a code of practice to protect consumers⁹⁶. Furthermore, the NCSC has published advice regarding the safe use of smart devices within the home⁹⁷, useful to thwart domestic abuse perpetrators' use of such tools. Guidance is provided as to how to set up devices, checking the default settings, managing accounts, keeping devices updated, as well as what to do and where to report to in the event of someone having malicious control or access to a device. Additionally, there is advice regarding what to do when getting rid of a device.

The charity Refuge, which supports women and children who have experienced domestic abuse, provide guidance about tech abuse and tech safety resources on their website⁹⁸. They note that abusers are increasingly using technology to facilitate their abuse and have gained access to women's personal and home devices, online accounts as well as children's toys and devices, especially iPads and games consoles such as Xboxes and Playstations. These enable the perpetrator to trace information such as location and who is being spoken with and when. Comprehensive information to help with recognising the signs of tech abuse is also displayed on the website, along with dedicated guides and tips including, iPhone privacy and security, staying safe on Facebook/ Twitter, online gaming: privacy risks and strategies, spyware, surveillance and safety, choosing and using apps, and IoT.

The domestic abuse charity Safelives provide digital and online safety resources⁹⁹, including a staying safe online guide, a toolkit for survivors, links to social media privacy settings for Facebook, Snapchat, Instagram and Twitter, and links to sector organisations working on tech safety including Chayn, Refuge, EndTechAbuse.org and Cyber safety plan. There are also resources provided by the National Resource Centre on Domestic Violence, hosted on the VAWnet,¹⁰⁰ which include case studies and tech safety and privacy guidance for survivors. Furthermore, researchers at University College London have created a list of available resources for technology-facilitated abuse victims and support workers¹⁰¹, which includes details of organisations who have produced advice and guidelines, as well as highlighting the most common methods of tech abuse.

The charity 'End the Fear - Greater Manchester Against Domestic Abuse' has a same sex domestic abuse page¹⁰² with a downloadable safety plan that includes advice on how to manage home computers/devices/social media. Whilst the LGBT Foundation also has a dedicated page for domestic abuse but no specific technology-related advice.

⁹⁶

<https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>

⁹⁷ <https://www.ncsc.gov.uk/pdfs/guidance/smart-devices-in-the-home.pdf>

⁹⁸ <https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/>

⁹⁹ <https://safelives.org.uk/tech-vs-abuse>

¹⁰⁰ <https://vawnet.org/sc/technology-assisted-abuse>

¹⁰¹ <https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot-resource-list.pdf>

¹⁰² <http://www.endthefear.co.uk/same-sex-domestic-abuse/>