



Can signs of digital coercive control be evidenced in mobile operating system settings? – A guide for first responders

Graeme Horsman

Cranfield University, College Rd, Cranfield, Wharley End, Bedford, MK43 0AL, UK

ARTICLE INFO

Article history:

Received 30 August 2022

Accepted 20 November 2022

Available online xxx

Keywords:

Coercive control

Domestic abuse

Digital evidence

Mobile phone

Digital investigation

iOS

Android

ABSTRACT

Perpetrators of domestic abuse are now frequently utilising technology to survey and regulate the conduct of their victims. Of all digital devices, mobile phones are considered one of the most common to be misused by perpetrators, with reports of their use to track victims via spyware or a device's location services, and to send abusive communications often seen. As a result, any support services and first responders involved in such investigations must ensure they are in a position to identify and understand any signs of technology-facilitated abuse on a mobile device if an investigative opportunity presents itself. In regards to a victim's phone, attention is often placed upon identifying the presence of unwanted applications or being in receipt of communications showing abuse. However, evidence of abuse can be more subtle, where this work seeks to identify and describe a series of proprietary settings that exist on the mobile operating systems iOS and Android that can be used to exert control, provide oversight of, or, manipulate the way in which a device itself is operated by its user. The intention here is to offer support to those involved in responding to or investigating incidents of abuse to identify and understand the impact of these potentially relevant digital traces.

© 2022 Published by Elsevier Ltd.

1. Introduction

When acts of domestic abuse (DA) take place in environments where only the perpetrator and/or victim are able (but possibly unwilling) to testify in regards to any relevant actions being carried out, conducting an effective investigation maintains its challenges (Rights of Women, 2015; Ramirez and Lane, 2019). In such scenarios, both support services and law enforcement from the outset of an inquiry must be aware of, and seek to note any apparent signs of relevant behaviours that may be evidence of or, be indicative of an abusive course of conduct taking place, to allow them to respond accordingly (College of Policing, 2022a). Those involved in an investigation are encouraged to adopt a proactive approach to gathering evidence of abuse in order to safeguard victims and prevent any conduct from escalating by taking appropriate measures (College of Policing, 2022a).

Perhaps historically, when investigating cases of DA focus has been centred upon determining whether physical acts of abuse have taken place, yet now it is widely acknowledged that non-physical conduct can also fall within this offence type (Williams

et al., 2021). Acts such as 'coercive control and 'gaslighting' are described by Women's Aid (2022) as 'designed to make a person dependent by isolating them from support, exploiting them, depriving them of independence and regulating their everyday behaviour' (Womens Aid, 2022). Further, economic abuse, online abuse, threats and intimidation, and emotional abuse' can also constitute DA (Home Office, 2018), where such conduct may take place through the utilisation of digital platforms (Todd et al., 2021).

Christie and Wright (2019 p.1) state that the 'domestic abuse charity Refuge reported that in 2019, 72% of women accessing its services said that they had been subjected to technology-facilitated abuse'. Refuge (2022a) itself reports that 'as of January 2019, more than 2500 of our clients reported experiences of technology-facilitated abuse'. For the year ending March 2020, the Office for National Statistics (2020) reported that '5.5% of adults aged 16–74 years (2.3 million) experienced domestic abuse in England and Wales in the previous year'. As part of establishing whether non-physical acts of abuse have taken place, there is a need to understand how technology can be used in a way that enables a perpetrator (British Computer Society, 2020). Through the manipulation and control of a victim's digital devices and services, technology can increase both the control that a perpetrator has over their victim, and be a facilitator for abuse (Woodlock, 2017;

E-mail address: graeme.horsman@cranfield.ac.uk.

SafeLives, 2022), where we are arguably now reaching a point where there is an expectation that technology will have been involved in any reported acts of DA (Sugiura and Nurse, 2022).

Harris and Woodlock (2019) use the term 'digital coercive control' (DCC) to describe those who conduct domestic violence facilitated by technology platforms and this article will proceed to utilise this terminology throughout when referring to such acts. Technology is now prevalent in the lives of many, particularly in terms of providing a mechanism to communicate with individuals and services, and to access important information. As a result, it is unfortunate that it should be of no surprise that perpetrators have been shown to manipulate access to and technology as a means to carry out their abuse (Cuomo and Dolci, 2021). The threat posed by acts of DCC requires those who form part of any investigatory team or support services in this area to be given the requisite knowledge and training to allow them to recognise when this has occurred and to respond accordingly (Freed et al., 2019). This is acknowledged by Woodlock (2020) who note that further evaluation of DCC is required in order to ensure any investigative response is appropriate and effective, and that those undertaking this work are fully prepared to do so.

Whilst not always the case, it is likely in some instances the technology found to be involved in DCC incidents was not produced with the intentions for use in this way. Instead, it is the role that it often plays in our lives that gives rise to opportunities for DCC when it can be misused or when a user's access to it is regulated or prevented without permission. Consider the example provided by Lopez-Neira et al. (2019) who indicate that the use of a smart home heating and lighting facilities could be used to restrict a victim's access to heat and light. Facilitators of abuse have been known to deploy 'digital tools and apps, including GPS location tracking (Linham, 2018; Nikupeteri et al., 2021; Yardley, 2021), spyware, mobile phones (Havard and Lefevre, 2020), IoT and smart devices (Silva and Franco, 2020), and social media platforms when conducting abuse (Afrouz, 2021).

Given their prevalence in society (with a reported ownership of over 91% of the world population (Bankmycell, 2022)), mobile phones have been found to be a prominent technology-type for conducting DCC (Woodlock, 2017; Havard, 2019; Havard and Lefevre, 2020). In relation to mobile phones and DCC, research focus has often been placed upon identifying and understanding the use of 3rd party applications to carry out this offence (Chatterjee et al., 2018; PenzeyMoog and Slakoff, 2021), yet in some cases such instances an abusive course of conduct may be more 'technologically subtle'. As proprietary operating systems increase in complexity and functionality, they offer their users greater configurative-control over their devices. In some cases, the control and manipulation of a device for the purposes of conducting DCC may be achievable on a mobile phone straight out of the box. As a result, a failure to understand and scrutinise any victim's device settings may result in missed investigative opportunities for identifying and evidencing when a perpetrator may be exerting control over their device. Identifying this information may be important to an investigation as Ramirez and Lane (2019) note that victims are increasingly seeking to rely on digital traces to evidence the abuse they are subject to.

This work seeks to identify and describe a series of proprietary settings that exist on the mobile operating systems iOS and Android that can be used to exert control, provide oversight of, or manipulate the way in which the device itself is operated by its user. The intention is to offer support to those involved in responding to, or investigating incidents of DCC to identify and understand potential investigative opportunities in relation to incidents of DCC.

2. The role of the first responder and supporting services

Support services and law enforcement may engage with those subject to DCC both in terms of attending a reported initial event of abuse and throughout the management of a relationship, which may extend across a period of months or years. Their involvement may not always be welcome and in some cases be deployed in a way that protects any alleged victim by preventing other parties from having knowledge of their presence. Any first responder attending an incident or support service interacting with potential victims as part of any initial or ongoing inquiry is faced with the complex task of managing their investigative scenario effectively whilst acknowledging the risks posed to any alleged victim (College of Policing, 2022a). When a mobile device is offered or brought to their attention as being of potential value to any alleged DCC, a decision must be made as to how to handle it, its investigative worth, how to ascertain this, and, the risk of harm that any process used to examine the phone may cause to any alleged victim. A seizure or voluntary submission and formal examination in a laboratory environment may not always be an appropriate workflow for the purposes of safeguarding a victim. Such a process may relieve a potential victim of their means of communication for a prolonged period of time, and/or alert an alleged perpetrator to their calls for help which may cause any abuse to escalate. Further, if tracking applications have been placed upon the device, any officer/first responder handling and submitting the device for forensic examination could reveal location information that alerts a perpetrator to this conduct (Louie, 2021). With this in mind, in some instances, a support service/first responder may be required to inspect a device immediately and manually (without forensic tools) given time implications and any risk of harm posed to the potential victim by the presence of an official at a given scene or dwelling (Horsman, 2022).

If an officer/first responder is placed in a position or deems it necessary to interrogate an alleged victim's device manually, their task of ascertaining the presence of any digital traces that may support this type of allegation is not straightforward. This is particularly the case if those conducting the inquiry do not have the in-depth technical knowledge required to conduct an effective interrogation of a device in these circumstances, or the requisite training. If we consider that such inquiries take place in a high pressure environment, prior to any device being submitted to a digital forensic unit (that is if it is even submitted at all), this task may need the support of the wider investigative team in order to ensure it is done appropriately and effectively (for example, in England and Wales, those in a Digital Media Examiner (DMI) may assist procedurally) (College of Policing, 2022b).

When conducting an inspection of the device, arguably an initial course of action is to identify the presence of applications ('Apps') on the device that may indicate DCC or content suggesting any abuse taking place (communication data) (Leitão, 2021). Yet, in some cases, evidence of the device being controlled or manipulated may take a more subtle form, where a device's configuration settings may indicate that restrictions are in place governing how and when the user can operate their device. Establishing this requires some investigative focus being placed on device settings as well as its general digital content.

2.1. A focus on settings

In some instances, perpetrators of DCC are known to restrict access to, and monitor the use of mobile phone content and Apps (PenzeyMoog and Slakoff, 2021). Whilst this can be done physically

(taking a phone and looking at it), the deployment of third party applications on their victim's phones to survey and control the use of it is a technique that is known to support services and law enforcement dealing with instances of DCC. In addition, it is necessary to note that it may also be possible to achieve such control of a device by configuring its proprietary settings, an act that may appear less obvious to an investigator scrutinising a device. Downes et al. (2019) note that victims are often either forced or feel obliged to provide access to their mobile phones so that perpetrators can review any information contained. Such actions provide perpetrators with the ability (providing that they have the knowledge) to configure a device in a manner that allows them to govern a victim's use of their device. Equally, support services and first responders must be in a position that allows them to establish whether this has taken place so that they can better understand any device's potential role in DCC, a task requiring knowledge of a device's setting and their impact.

This work examines the use of proprietary settings on both iOS and Android in relation to DCC. Focus is maintained on devices running the operating systems (OSs) iOS (Apple products) and Android (available across a number of device manufacturers), that together are reported to have over 95% of the mobile operating system market in 2022 (Statcounter, 2022a). As the complexity and functionality of these OSs has increased, those who own devices running these OSs now have an unprecedented amount of control over how the device performs. The result of which arguably increases the chance of support services and first responders encountering these devices as part of DCC inquiries. Settings in relation to iOS are considered first.

3. iOS

In the United Kingdom, iOS is reported to have approximately 50% of the mobile phone OS market in 2022 (Statcounter, 2022b). In regards to configuring these devices, general configuration settings on iOS are located within the 'Settings' tile, and it is these settings that will remain the focus of this work. These settings often impact the accessibility and functionality of the device as a whole as well as providing some basic App-specific configurability, and are present on every iOS device. It should be noted that most Apps maintain their own individual, often more detailed set of internally accessible configuration options which are not considered here as their presence depends upon whether a device user has downloaded the App or not. In contrast, settings within the 'Settings' tile are present on all iOS devices.

Refuge offers an overview of iOS for victims to protect themselves from abuse (Refuge, 2022c). Building upon this work, following an examination of an Apple iPhone 12 operating iOS 15.5, the settings shown in Tables 1–3 are noted as being of potential relevance to support services and first responder's when traversing an alleged victim's comparable device in cases of suspected DCC. Tables 1–3 contain the path to each setting on the device, the name of the setting and key information about the impact that the setting may have on the device, its data and functionality. Each setting has been assigned an ID value where those considered to require additional explanation beyond that provided in Tables 1–3 are discussed below and referenced using this value.

*Note: In relation to the specific discussion of the setting of both iOS and Android (Section 4), it is not the intention of the author to sensationalise or speculate on how services may or may not be used as part of DCC. However, where relevant, the potential use of a setting or functionality is highlighted in order to stress possible intervention or investigative opportunities that could otherwise have been missed or remained unknown.

In relation to details of the Apple ID (ID 1 & 2) assigned to the

device, it should be noted that those details may relate to an account on the device that the victim may not have control over. Therefore whilst they might be the primary user of the device, the device itself may be attributed to a perpetrator's account. ID 1 denotes the name given to the device (and also associated with the Apple ID signed in), however given that this is editable, attention should be given to the details of any email address listed in ID 2. For example, the device may be named after the victim (in field ID 1) but the listed email address may be that (in field ID 2) of a perpetrator. This may suggest that to some degree overarching surveillance and/or control of the handset is taking place, where various actions on the device will trigger email alerts to the account (noted where appropriate in the later discussions of each relevant setting). This is also particularly important as Apple accounts that have child status are subject to 'Family Sharing' - discussed in Section 3.2.

ID 3 indicates whether two factor authentication is operational on the device where any listed trusted numbers (ID 4) are used to provide a verification code. This number does not need to be the number used by any SIM card in the device and can be linked to a separate perpetrator's mobile number. The result being that if a user tries to log into their account on a separate device, a verification code will be sent to the trusted number, which if it is that of a perpetrator, may alert them to this behaviour.

ID 7 lists the redacted details of cards associated with the device as payment methods are listed. Bank names are viewable as well as the last 4 digits of the card. Billing address information may also be provided for those cards listed as 'payment cards'. This information may indicate who is providing financial support and governance for paid App purchases and subscriptions - if there are any.

In regards to the device's iCloud, consideration of the types of data entering the iCloud should be given (ID 8). By default, testing showed data types such as pictures were configured to sync to the iCloud by default, whereas SMS and Safari data were not. The amount of data in the iCloud for each App is viewable via the 'manage storage' (ID 9) option. If Apps are configured to sync to the iCloud but are not present in this list, there is no data of that type in the iCloud for the account. Given that syncing is often autonomous, if an App is configured to sync its data to the iCloud and there is space to do so, this may indicate that its data has been deleted from it. Alternatively the App may just not have been used, or possibly that the sync setting has only just been activated.

ID 10 provides a list of all of the Apps 'purchased' (includes free and paid) by the Apple account, including the date of their download. Testing suggests this is for the entirety of the Apple account (including other devices) as records of downloads dating back over 10 years could be found. Testing suggests that these records cannot be deleted via the phone's interface, and therefore provide a record of Apps that may have historically been on the phone, where for example, records of tracking Apps previously installed could be revealed to an investigator. To access this information, the Apple ID password must be provided.

Tracking is acknowledged as an abused phone function for perpetrators of DCC (Harris and Dragiewicz, 2019; Louie, 2021) and IDs 11 & 12 concern the 'Find My' function which enables location settings to provide 'findability' services for the device. ID 11 indicates whether the 'Find My iPhone' function is operational on the device and allows the user of the Apple account to locate, lock or erase their device. In reference to ID 1 & 2, if the account associated with the device is a perpetrator account, there is oversight of the device and the potential to lock/erase it exists. ID 12 concerns location sharing, where an option to share your location with listed 'Family' members, is offered. These family members can see the location of this handset on their device's 'Find My' App. Family members are added via the 'Family Sharing' functionality discussed in Table 3 (IDs 41–45) as additional contextualised discussions are required.

Table 1
General settings.

ID	Path	Setting Name	Key Information
1	Settings > Apple ID > Name, Phone Numbers, Email	Name	The name associated with the Apple ID that is signed into the phone. Changing this value triggers an alert email to be sent to the email address assigned to the ID.
2	Settings > Apple ID > Name, Phone Numbers, Email	Contactable at	The email address that is associated with the Apple ID is listed. The phone number that is associated with the mobile service provider contract is listed.
3	Settings > Apple ID > Password & Security	Two-Factor Authentication	On or off value. Trusted numbers are used to verify the device user's identity.
4	Settings > Apple ID > Password & Security	Trusted Phone Numbers	These are phone numbers that are associated with the Apple account that can be used to verify the account's ID. Multiple can be added.
5	Settings > Apple ID > Password & Security	Account Recovery	This is contact information for trusted contacts for the purposes of account recovery. Trusted contacts are listed and their contact number. Their 'access key' status is also recorded showing whether they have saved the access key for your account.
6	Settings > Apple ID > Password & Security	Legacy Contact	Permitted contact details of trusted contacts who can download account data after death. Legacy contacts are listed and their contact number. Their 'access key' status is also recorded showing whether they have saved the access key for your account.
7	Settings > Apple ID > Payment & Shipping	Payment Methods	Redacted details of cards associated with the device as payment methods are listed.
8	Settings > Apple ID > iCloud	Storage	iCloud settings including the data-types that are and are not synced to the iCloud.
9	Settings > Apple ID > iCloud	Manage Storage	A list of Apps with data in the iCloud.
10	Media & Purchases	Purchase History	A list of all of the Apps 'purchased' (includes free and paid) by the Apple account is provided, including the date of download. Testing suggests this is for the entirety of the Apple account as records of downloads dating back over 10 years could be found.
11	Settings > Apple ID > Find My	Find My iPhone	On or off value controlling the 'Find My iPhone' function.
12	Settings > Apple ID > Find My	Share My Location	On or off value. The device location can be shared with permitted contacts.
13	Settings > Apple ID	–	Devices that are associated with the Apple ID are listed at the bottom of this menu. Device metadata is also provided including device type and device name.
14	Settings > Bluetooth	My Devices	A record of paired bluetooth connections is maintained.
15	Settings > Mobile Data	–	On or off value for the whole handset.
16	Settings > Mobile Data	Mobile Data	Each App is listed and its use of mobile data can be turned on or off using the switch. By default, most individual Apps are configured to use mobile data and need to be turned off by the user if they do not want this to happen. These settings cannot be password protected.
17	Settings > Notifications	Show Previews	By default, previews of notifications (i.e. SMS content etc.) are not shown when the device is locked. This can be changed to 'Always' where anyone can see notification content on the device screen.
18	Settings > Notifications	Notification Style	Individual App notifications can be controlled to display or not display through a locked screen. Specific notifications can also be assigned specific alert sounds.
19	Settings > Focus	–	The device can operate four modes by default - 'Do Not Disturb', 'Personal', 'Sleep' and 'Work' that can be configured to regulate notifications from specific Apps or contacts. Each mode can be controlled via a defined schedule. For example, the device when in 'Do Not Disturb' Focus mode can be configured to only show notifications from Contact 'A' between 08:00–21:00. Additional modes can be added and configured.
20	Settings > General > About	Name	Name of the device and its associated metadata is listed.
21	Settings > Display & Brightness	Auto-Lock	By default, an iPhone locks after 2 min, but this can be changed to 'never'.
22	Settings > Accessibility > Guided Access	–	On or off value. Guided Access allows a user to fix the device to one App screen and prevent the user from accessing menus. This can be password protected or via Face ID indefinitely or for a specific time period.
23	Settings > Face ID & Passcode	Use Face ID For	iPhone Unlock - On or off value. This value controls whether Face ID can be used to unlock the phone. If Face ID is turned off, only the numeric password is active.
24	Settings > Face ID & Passcode	Turn Passcode Off	On or off value. The iPhone can be left in a state where no authentication is required to access it.
25	Settings > Wallet & Apple Pay	Payment Cards	Payment cards and their metadata associated with Apple Pay are listed. The 'Wallet' App stores data relating to registered non-payment cards.
26	Settings > Passwords	–	Passwords saved on the device for accessing various accounts are available in plain text providing the device password/Face ID can be provided. However, if both the password and Face ID have been disabled, password information is available in plain text.
27	Settings > Phone	Blocked Contacts	Records of contacts blocked on the device. These are also recorded in the Messages, Facetime and Mail App settings.
28	Settings > Messages	Message History	The device can be set to store messages forever, 1 year or 30 days.
29	Settings > FaceTime	Blocked Contacts	Records of contacts blocked on the device. These are also recorded in the Messages, Facetime and Mail App settings.

ID 13 lists all of the devices that are associated with the Apple ID signed in on the current device and in conjunction with IDs 1 & 2, may reveal if the Apple ID is that of the victim or potentially associated with devices that they do not own (i.e. those of the perpetrator).

ID 14 denotes the settings determining whether bluetooth is on or off, the name of the device (what it is 'discoverable as') and a list of previously connected devices and their metadata. Whilst bluetooth may enhance the discoverability of a victim's phone (Queensland Government, 2019), information here may offer an insight into previous connection records which may help to determine whether the device is or has previously been subject to surveillance or access by others.

IDs 15 & 16 control the use of mobile data on the handset. At ID 16, each App is listed and its use of mobile data can be turned on or off using the switch. By default, most individual Apps are configured to use mobile data and need to be turned off by the user if they do not want this to happen. Doing so would in many cases prevent use of the Apps until the phone is able to access an Internet connection with credentials known to the user/device - possibly one that the perpetrator is in control of. In line with this point, it should be noted that the iOS interface does not show records of connections to past Wi-Fi networks. Whilst these settings cannot be password protected, the phone does record the amount of data used in a 'current period' of usage which could record whether the user has turned mobile data back on and used it. The 'current

Table 2
Screen time settings.

ID Path	Setting Name	Info
30 Settings > Screen Time > See All Activity	Most Used & Pick Ups	Usage statistics for the device are provided for up to 3 weeks prior. Apps used on the handset are listed, where each one when clicked, has the option to set a usage limit. Where a limit is set in terms of amount of time per day, this will be listed within the particular App's settings here. These limits cannot be enforced with passwords and can be overridden by the device user.
31 Settings > Screen Time > Downtime	—	The device can be configured to schedule 'downtime' making designated Apps unavailable to the user. The chosen downtime schedule is recorded here.
32 Settings > Screen Time > App Limits	—	Here, individuals can set usage limits for individual Apps. Limited Apps are listed. Note - App limits are not password locked and can be overridden by the user.
33 Settings > Screen Time > Communication Limits	—	The user can limit the contacts that can interact with the handset during downtime and Screen Time.
34 Settings > Screen Time > Always Allowed	Allowed Contacts	Here, a list of contacts allowed to communicate with the handset during downtime is provided.
35 Settings > Screen Time > Always Allowed	Allowed Apps	Here, a list of Apps allowed for use on the handset during downtime is provided.
36 Settings > Screen Time > Use Screen Time Passcode	—	A password can be set to prevent access to Screen Time settings. When this label shows 'Change Screen Time Passcode' a passcode is set and in operation.
37 Settings > Screen Time > Content & Privacy Restrictions	iTunes & App Store Purchases	The device can be prevented from installing and deleting Apps on the devices. In-App purchases can be prevented.
38 Settings > Screen Time > Content & Privacy Restrictions	Allowed Apps	A list of applications that can be 'removed' from the device - i.e. they are inaccessible when disabled. Their App tile is removed and even searching for them on the device will not return the App.
39 Settings > Screen Time > Content & Privacy Restrictions > Content Restrictions	Web Content	Access to websites can be restricted to specifically listed sites.
40 Settings > Screen Time > Content & Privacy Restrictions	Allow Changes	Password and account changes can be prohibited along with other usage settings.

Table 3
Screen time settings.

ID Path	Setting Name	Info
41 Settings > Apple ID > Family Sharing	—	Members of the device's 'Family' are listed here including contact detail metadata. Locations Sharing and Screen Time settings are governed here for family devices.
42 Settings > Apple ID > Family Sharing	Screen Time	A list of family members who can be controlled via Screen Time.
43 Settings > Apple ID > Family Sharing	Include Website Data	Internet history is recorded as part of Screen Time.
44 Settings > Apple ID > Family Sharing	Location Sharing	A list of 'family' members and their Apple IDs is provided showing who the device's location is shared with.
45 Settings > Apple ID > Family Sharing	Ask to Buy	A child account can be prevented from downloading Apps from the App Store without permission from a controlling account.

period' of usage can be reset and there is no information presented to the user as to when this reset has occurred.

IDs 17 & 18 control the notification settings for the device. By default, previews of notifications (i.e. SMS content etc.) are not shown when the device is locked. This can be changed to 'Always' where anyone can see notification content on the device's locked screen (i.e. previews of message content). A perpetrator may seek to enforce such a setting to increase their surveillance of the device without having to unlock it. In addition, notifications for each application can be configured individually, including setting a distinct alert sound for each notification type. This may again alert a perpetrator to specific actions on a victims handset without physically seeing content. [Refuge \(2022b\)](#) note SMS monitoring is commonly experienced by victims of abuse.

ID 19 relates to 'Focus' on the handset, a functionality which when engaged allows the user to control which notifications and alerts are shown on the device. The device can operate four modes by default - 'Do Not Disturb', 'Personal', 'Sleep' and 'Work' that can be configured to regulate notifications from specific Apps or contacts. Each mode can be controlled via a defined schedule. For example, the device when in 'Do Not Disturb' Focus mode can be configured to only show notifications from Contact 'A' between 08:00–21:00. Additional modes can be added and configured.

ID 21 concerns the time before the device locks. By default, an iPhone is set to lock after 2 min of inactivity, but this can be changed to 'never', meaning that an unlocked, inactive device remains accessible indefinitely until it is locked.

ID 22 relates to the 'Guided Access' function and whether it is turned on - it is off by default. Guided Access allows a user to fix the device to one App screen and prevent the user from accessing menus. For example, Guided Access could be used when viewing Youtube, which when active, prevents the user from interacting with the screen or changing Apps until it is turned off. Guided Access can be configured so that it can only be turned off when the correct password is entered or via Face ID. Alternatively, the length that Guided Access is in operation for can be either indefinite or for a specifically defined time period. If a time limit is set and the passcode is not known to terminate it, then the device is unusable until the correct code is entered. Guided Access can also be used to make parts of an App inactive (displayed in dark grey), for example, [Fig. 1](#) shows Guided Access used to lock the device to the iOS phone App where the user can only press the dial 'home' button - all other options are unavailable ('greyed out').

Whilst ensuring a device is locked is recommended protection mechanism (Hampshire [Constabulary, 2019](#)) perpetrators may seek to deploy regular checks on a victim's device where the way that a device can be unlocked is changeable ([Havard and Lefevre, 2020](#)). Testing showed that by turning Face ID (ID 23) off and turning off the passcode (ID 24), the device could be left in an open state where anyone could access it without requiring credentials. Linked to the method of device access is that of the iOS 'Passwords' function (ID 26) where the device lists accounts and credentials held by the device. By default, Face ID is required to gain access to this area, however if this is turned off (ID 23) as well as the device's passcode

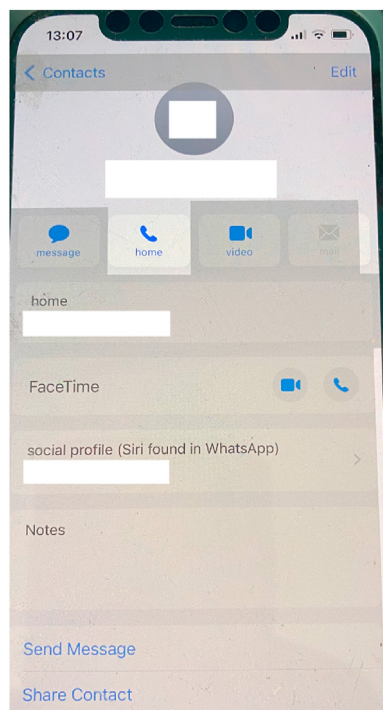


Fig. 1. Guided Access used to restrict a user to only being able to phone home.

(ID 24), then all of the user's accounts and credentials are available in plaintext.

ID 25 contains details of the payment cards and their metadata associated with Apple Pay are listed. The 'Wallet' App stores data relating to registered non-payment cards. This information may be pertinent if there is a concern that the device owner is subject to financial control.

Following [Havard and Lefevre's \(2020 p.7\)](#) study, it was found that 'general monitoring and control of the women's access to and use of mobile phones, whom they could speak to, when, and for how long was most common'. IDs 27 & 29 concern contacts that are blocked on the device from calling or facetime where a list of blocked contacts is provided. In addition, ID 28 governs the retention period for SMS on the handset. By default, messages are kept 'forever', however the device can be configured to keep messages for 1 year or 30 days. [Havard and Lefevre \(2020\)](#) note that one of the most common forms of abuse is the sending of threatening communications via mobile phone, where phones configured to purge SMS are preventing this type of evidence collection.

3.1. Screen time

Screen Time is an iOS functionality that allows an owner of a device to manage the use of their phone and its applications, and to provide usage statistics ([Apple, 2021](#)). This functionality can be used to control the user's device, and in conjunction with iOS's 'Family Sharing' function, it is possible to control and monitor the devices of others (this particular functionality is discussed further in Section 3.2). A decision has been made to separate the settings and capability of Screen Time from those more general settings located in [Table 1](#) due to the fact that this function specifically relates to device management and control.

Screen Time can be accessed through the general *Settings* tile on iOS, where the following specific functions are listed in [Table 2](#) and described below.

Screen Time settings can be protected through the use of a

Screen Time Passcode (ID 36), however this is optional. When this setting has a visible label showing the string 'Use Screen Time Passcode', no passcode is in operation. When this setting has a visible label showing the string 'Change Screen Time Passcode' a 4 digit numeric passcode is set and in operation.

ID 30 provides information showing the overall usage of the device, where each App's usage is described across the course of each day and for up to 3 weeks of historical usage data. These statistics may offer an investigator an insight into a device's pattern of usage and help to identify periods of anomalous behaviours, corroborate times of abuse or indicate when periods of inactivity (possibly forced or due to supervision) have taken place. In addition, devices 'pickups' are recorded for the same duration periods as device usage noted above, showing which App is first used when the device is unlocked ([Apple, 2022](#)). Both these features offer a profile of a user's behaviour across a three week period.

ID 31 concerns the 'Downtime' function, where the device can be scheduled to make designated Apps unavailable to the user. If a Screen Time passcode is set, then Downtime schedules cannot be seen. Downtime schedules are listed and available for review. When an App is in Downtime, its usage is not password locked and this feature can be overridden by the user unless the 'Block at Downtime' option is selected. If this option is selected, when in Downtime, the device user can either ask for 'One More Minute' of access to the App (which provides 1 min of usage before locking the App), or provide the Screen Time Passcode set at ID 36. If the user does not know the passcode, these Apps cannot be used until Downtime is deactivated. IDs 34 & 35 concern a list of contacts and Apps that are allowed during any Downtime period.

In addition to Downtime, ID 32 allows the user to limit how long individual Apps can be used on a device where a specific daily schedule can be set and is available for review. Similar to Downtime (ID 31), the option 'Block at End of Limit' prevents an App from being used once the limited period of usage is up.

ID 33 allows the user to define specific contacts that the device can communicate with during Downtime. During Downtime, communications from all other contacts are blocked and message content is not visible.

ID 37 governs a user's ability to install and delete Apps, and to make in-App purchases. By default, these settings allow a user to do all of the aforementioned, but these can be prevented. [Havard and Lefevre \(2020 p.7\)](#) note that perpetrators have been shown to place limits on what Apps a victim can download and use. ID 38 gives the user the option to prevent all Apps from being available on the device, which when operational prevents all Apps on the device from being visible to the user except for those that come default with the device. ID 39 gives the user the chance to define a list of specific websites that can only be accessed using the device.

ID 40 provides a number of settings which can be used to prevent changes occurring on the device. Here a user can be prohibited from to following:

- Changing their device's Face ID and passcode (this option is removed from view).
- Changing account information (settings in Settings > Apple ID)
- Changing mobile data settings. Note that configuration changes to mobile data settings could not be prevented at IDs 15 & 16, however these can be prevented using this function.

3.2. Family Sharing

Family Sharing is a function of iOS that allows the user to link their device and account with other members of their 'family' and to utilise features such as Location Sharing and Screen Time across

different devices. Key settings are described in [Table 3](#).

At ID 41, members of the device's 'family' are listed along with metadata about each individual. Both the Apple ID of any family member device is listed and their 'role'. An individual can be an 'organiser' (someone who has initiated the family group), an 'adult', a 'Parent/Guardian' or a child (where age is listed). These roles govern the amount of control that can be exerted over another device.

Organiser and Parent/Guardians can utilise Screen Time (ID 42) to control the devices of child accounts that have been set up. Those accounts subject to Screen Time are listed where those settings noted in [Table 2](#) are available to control the child account's device. In addition, the device's Internet history can also be maintained (ID 43) and reviewed as part of Screen Time's 'See All Activity' settings.

ID 44 provides a list of all the Apple IDs in the 'family' that the device is sharing its location with. ID 45 prevents a child account from downloading Apps from the App Store without permission from a controlling account.

4. Android

To review proprietary settings on Android, a 'Huawei P Smart' test device running EMUI 9.2.0.293 (Huawei's deployment of an Android OS) was utilised. Similar to iOS, proprietary settings can be found in the 'Settings' tile. [Tables 4 and 5](#) contain the path to each setting on the device, the name of the setting and key information about the impact that the setting may have on the device, its data and functionality. As with those settings noted with iOS above, here each setting has been assigned an ID value where those considered to require additional explanation beyond that provided in [Tables 4 and 5](#) are discussed below and referenced using this value. Where settings have a comparable function to those noted with iOS, links will be drawn in order to avoid repetition in the narrative below.

In an effort to avoid repetition, where settings are considered analogous to those already described in section 3 regarding iOS, a link to the appropriate ID has been made within [Table 4](#). Settings that are believed to require additional discussion are highlighted below.

ID 54 provides a list of 'running' and 'stopped' applications on the device. This may be of value to a first responder who is trying to determine the presence of any Apps of potential relevance to their inquiry.

ID 55 allows a schedule to be set for when the device is powered off and on with details of any schedule set displayed. Whilst these cannot be enforced, for example, a device can be powered back on straight away following a scheduled power off, device activity can be correlated against information stored by the device's 'Digital Balance' feature. A perpetrator may correlate such activity to determine adherence to a scheduled period of device inactive defined by them.

IDs 56–60 concern the back up settings and Google account associated with the backup process on the device. As with IDs 1 and 2 on iOS, first responders should be alert to the actual controller of these accounts as backups can include a range of device metadata that a perpetrator may seek as part of their abusive conduct and device surveillance.

IDs 62–64 govern the three lock mechanisms for the handset – the lock screen password, fingerprint or face. First, it is possible to leave the device unprotected and accessible by anyone. Whilst in such cases, access the an open device will be obvious to a first responder if they have tried to access it, by checking the configuration of all three lock types, it is possible to establish that they have

not been activated. If a device lock screen password is not set then the user is presented with the option 'Set lock screen password' (ID 62). If face recognition information is not active on the device, a user is prompted to 'enrol' their face on the device (ID 64). Finally, details of any stored fingerprints are listed in ID 63. Determining the use of fingerprint or face unlocking information requires the user to first input the lock screen password. If no lock screen password is set, then the user must set one before using these functions. If the user removes the lock screen password, this automatically removes any stored fingerprint and face information. Whilst with the test device used in this work, only one face could be stored for the purposes of unlocking the device, several fingerprints could be stored and these can be given a bespoke naming label by the user. If the first responder has the lock screen password (for example, it has been provided by the user), then they can check how many prints are in use on the device and correlate these against any testimony from an alleged victim. Further, the device offers an inbuilt 'print test' function where fingers can be placed on the device and the device highlights whether it matches an existing stored print.

ID 65 relates to App Lock which allows the user to pin lock specific Apps on the device. If this is disabled, when selected the user is prompted to enable it. If App Lock is enabled, the pin code set by the user is required in order to see which Apps have been locked. Locked Apps cannot be accessed without the pin. If a first responder does not have the pin lock to access the App Lock list of locked Apps, they may opt to try to access specific Apps on the device and see whether they are met with a prompt to input a pin.

4.1. Digital balance

Similar to iOS's Screen Time, the test Android device maintained a 'Digital Balance' feature maintaining some of the functionality previously seen in [Table 2](#). Digital Balance settings are noted in [Table 5](#) and described below.

ID 66 is an on or off switch denoting whether a 6 digit screen time management pin has been set in order to access and change Digital Balance settings. When activated, settings cannot be accessed without inputting the pin. Similar protection is also present with Screen Time, where the pin is required in order to access and review the settings operating within Digital Balance.

ID 68 provides details of any set screen time schedule (access requires the screen time management pin). Once active, Apps can only be accessed using the screen time management pin. Core services such as the calls, messaging and 'always allowed' Apps are still available.

ID 69 provides a list of Apps installed upon the device and when selected, a daily use limit can be set (for example, App 'A' can be limited to 1 h per day). If no screen time management pin is set, this can be overridden by the user. If a screen time management pin is set, once the usage limit has been reached, the pin is required in order to use the App.

ID 70 concerns 'Bedtime' which can be configured to schedule a time where access to Apps can be restricted unless the screen time management pin is entered. Phone and messaging remain accessible, as do any Apps that are set to always be allowed.

5. Discussion and concluding thoughts

As mobile operating systems continue to offer users increasing configurability over their devices, in cases of suspected DCC, it is important that those involved in responding to an incident or inquiry understand that such settings may also provide an opportunity for perpetrators to control the device of their victim. The settings discussed within this work are proprietary to devices

Table 4
General settings.

ID Path	Setting Name	Info
46 Settings > Wireless & networks > Wi-Fi > Wi-Fi settings	Saved networks	A list of saved networks is provided.
47 Settings > Device connectivity > Bluetooth	Paired devices	A list of the names of paired bluetooth devices is provided. This setting is considered analogous to ID 14.
48 Settings > Notifications	Lock screen notifications	This setting is considered analogous to ID 17. Notifications content can be 'shown' when the device is locked or protected.
49 Settings > Notifications	Notifications	Each App's notification settings can be configured individually as to what is presented on screen. This setting is considered analogous to ID 18.
50 Settings > Apps > Apps	—	Apps on the device are listed and each App when selected provides its 'App info'. Here, some Apps can be disabled, however testing suggested that core services like messages could not be disabled. Each Apps ability to use mobile data can also be turned off, and notification settings can be configured. These settings cannot be protected via a password or pin. This setting is considered analogous to ID 16.
51 Settings > Display	Sleep	This setting is considered analogous to ID 21. Here, by default the locks after 30 s of inactivity, but can be configured to never lock due to inactivity.
51 Settings > Sounds > Do not disturb	Do no disturb	This setting is considered analogous to ID 19. When active, do not disturb mode silences calls and messages and prevents banner notifications from being shown. This mode can be turned off at any time.
52 Settings > Sounds > Do not disturb	Scheduled	If a schedule for the 'do not disturb' mode is set, details of it are shown here.
53 Settings > Sounds > Do not disturb	Allow Interruptions	Specific contacts can be permitted to call and message a handset during 'do not disturb' mode. Alternatively, all contacts can be blocked.
54 Settings > Battery	Battery usage	A list of 'running' and 'stopped' applications on the device are shown.
55 Settings > Smart assistance	Scheduled power on/off	A schedule can be set for when the device is powered off and on. Details of any schedule set are displayed.
56 Settings > System > Backup & restore	Back up to Google	If 'Back up to Google' is enabled, device and App data is backed up to a designated Google account.
57 Settings > System > Backup & restore	Backup account	The email address of the account used to backup device and app content.
58 Settings > System > Backup & restore	Google Account	Details of the backup processes and data can be accessed.
59 Settings > System > Google	—	Details of the Google account(s) associated with the device can be found here including links to backup information (ID 58). The 'Find My Device' function can also be turned on/off here, allowing the device to be located and if required, erased. This setting is considered analogous to ID 11
60 Settings > Accounts	—	Details of accounts linked with the device are listed here. The sync status for device metadata is also provided (for example, when Gmail was last synced).
61 Settings > Security & privacy	Find My Device	On or off switch. This is also located at ID 59.
62 Settings > Security & privacy >	Lock screen password	If a device lock screen password is not set then the user is presented with the option 'Set lock screen password'. If a password is set then the option 'Change lock screen password' is present.
63 Settings > Security & privacy > Fingerprint ID	Fingerprint Management	Details of which fingerprints are stored on the device that can be used to unlock it are proved where multiple prints can be listed. Each print can also be named by the user. The usage of the prints is also defined, including whether it is used to unlock the device, access Safe or access App Lock. The lock screen password is required to access this information.
64 Settings > Security & privacy	Face recognition	If face recognition information is stored on the device, its usage settings are described. If it is not, the user is prompted to 'enrol' their face on the device. The lock screen password is required to access this information.
65 Settings > Security & privacy	App Lock	App Lock allows the user to pin lock specific Apps on the device. If this is disabled, when selected the user is prompted to enable it. If App Lock is enabled, the pin code set by the user is required in order to see which Apps have been locked. Locked Apps cannot be accessed without the pin.

Table 5
Digital balance.

ID Path	Setting Name	Info
66 Settings > Digital balance	Screen time management pin	This is an on or off switch denoting whether a 6 digit pin has been set in order to access and change 'digital balance' settings. When activated, settings cannot be accessed without inputting the pin. This setting is considered analogous to ID 36.
67 Settings > Digital balance	SCREEN TIME	Up to 7 days of device usage can be viewed. This setting is considered analogous to ID 30.
68 Settings > Digital balance	Screen time	A screen time limit schedule can be defined where once active, Apps can only be accessed using the screen time management pin.
69 Settings > Digital balance	App limits	Apps installed upon the device are listed which when selected, a daily use limit can be set. If no screen time management pin is set, this can be overridden by the user. If a screen time management pin is set, once the usage limit has been reached, the pin is required in order to use the App.
70 Settings > Digital balance	Bedtime	This setting is considered analogous to ID 31. Bedtime can be configured to schedule a time where access to Apps can be restricted unless the screen time management pin is entered. Phone and messaging remain accessible, as do any Apps that are set to always be allowed (ID 69).

running these operating systems, and therefore unlike third party Apps which require a user/perpetrator to install them, they will be present in all cases where these operating systems are. It is understandable that attention often gravitates towards malicious Apps in relation to mobile devices and DCC, however it must now be recognised that in regards to the control and surveillance of a

device, proprietary services and their settings on mobile operating systems are now offering such abilities. Device settings may offer a more subtle form of intelligence describing DCC, and in turn a form of intelligence that a perpetrator may not realise exists. It is important that in any inquiry involving a mobile device, a first responder considers the way in which a device is configured and

that these settings could offer a source of evidence which may reveal all or part of an abusive course of conduct. Of Course, the settings described have legitimate uses and therefore first responders must be cautious when interpreting how they are deployed on a device, taking into account surrounding case circumstances and testimonies from any parties involved. Some settings like limits placed upon App usage may genuinely be deployed for purposes of productivity/prevention of procrastination and therefore it is important not to immediately judge the deployment of these settings as malicious without further scrutiny.

Proprietary settings can be difficult to understand, particularly in regards to their cause and effect on the device, and the impact that this may have in relation to a suspect offence and the surrounding scenario. Time must be spent not just horizon scanning with regards to emerging malicious Apps and technology, but also to assess and evaluate the impact of proprietary capability that is shipped with technology straight 'out of the box'. Settings must also be critically evaluated in terms of their impact, and as noted above, a first responder should determine what the impact of any setting is on a device, and how this could facilitate abuse in certain circumstances. It is also important to note that some settings provide capability but do not evidence how it is subsequently deployed. An example of this is iOS's 'Guided Access' function. Whilst this is off by default, the fact that it has been turned on is not an indicator of DCC alone, and how Guided Access has been used is not described in the system. However, if it is active, it does provide an indicator that such features have been considered or acknowledged at some point by a device user, where further testimony by an alleged victim may provide some context.

As DCC continues to offer challenges to law enforcement, future work includes not just recognising changes to mobile phone operating systems, but also to recognise proprietary settings and capability shipped with a range of technologies.

Declaration of competing interest

No conflicts of interest to declare.

References

- Afrouz, R., 2021. The nature, patterns and consequences of technology-facilitated domestic abuse: a scoping review. *Trauma Violence Abuse*, 15248380211046752.
- Aid, Women's, 2022. What is coercive control? Available at: <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/>. (Accessed 20 June 2022). Accessed:
- Apple, 2021. Use Screen Time on Your iPhone, iPad or iPod Touch. Available at: <https://support.apple.com/en-gb/HT208982>. (Accessed 11 July 2022).
- Apple, 2022. View Pickups in Screen Time Preferences on Mac. Available at: <https://support.apple.com/en-gb/guide/mac-help/mchl9724f790/mac>. (Accessed 11 July 2022).
- Bankmycell, 2022. How many people have mobile phones in the world? Available at: <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world>. (Accessed 5 July 2022).
- British Computer Society, 2020. 'Coercive control resistant design' Available at: <https://www.bcs.org/articles-opinion-and-research/coercive-control-resistant-design/>. (Accessed 4 July 2022).
- Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., Ristenpart, T., 2018. The spyware used in intimate partner violence, 2018, May. In: *IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 441–458.
- Christie, L., Wright, S., 2019. 'Technology and domestic abuse' Available at: <https://post.parliament.uk/technology-and-domestic-abuse/>. (Accessed 4 July 2022).
- College of Policing, 2022a. 'Investigative development' Available at: <https://www.college.police.uk/app/major-investigation-and-public-protection/domestic-abuse/investigative-development>. (Accessed 5 July 2022).
- College of Policing, 2022b. 'Digital Media Investigator' Available at: <https://profdev.college.police.uk/professional-profile/digital-media-investigator/>. (Accessed 7 July 2022).
- Constabulary, Hampshire, 2019. 'Digital domestic abuse' Available at: <https://www.hampshire.police.uk/advice/advice-and-information/daa-domestic-abuse/digital-domestic-abuse/>. (Accessed 7 July 2022). Accessed:
- Cuomo, D., Dolci, N., 2021. New tools, old abuse: technology-enabled coercive control (TECC). *Geoforum* 126, 224–232.
- Downes, J., Kelly, L., Westmarland, N., 2019. 'It's a work in progress': men's accounts of gender and change in their use of coercive control. *J. Gend.-Based Violence* 3 (3), 267–282.
- Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., Dell, N., 2019. "is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. *CSCW Proc. ACM Hum.-Comput. Interact.* 3, 1–24.
- Harris, B., Dragiewicz, M., 2019. Migrant women are particularly vulnerable to technology-facilitated domestic abuse. *Conversation* 1–4.
- Harris, B.A., Woodlock, D., 2019. Digital coercive control: insights from two landmark domestic violence studies. *Br. J. Criminol.* 59 (3), 530–550.
- Havard, T.E., 2019. *Beyond Proximity: the Covert Role of Mobile Phones in Maintaining Power and Coercive Control in the Domestic Abuse of Women*. Doctoral dissertation, University of Sussex.
- Havard, T.E., Lefevre, M., 2020. Beyond the power and control wheel: how abusive men manipulate mobile phone technologies to facilitate coercive control. *J. Gend.-based Violence* 4 (2), 223–239.
- Home Office, 2018. Domestic Abuse: How to Get Help. Available at: <https://www.gov.uk/guidance/domestic-abuse-how-to-get-help>. (Accessed 4 July 2022). Accessed:
- Horsman, G., 2022. Conducting a 'manual examination' of a device as part of a digital investigation. *Forensic Sci. Int.: Digit. Invest.* 40, 301331.
- Leitão, R., 2021. Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Hum. Comput. Interact.* 36 (3), 203–242.
- Linhm, L., 2018. Hundreds of Mobile Phone Apps Can Allow Stalkers and Abusers to Track Their Victims - This Is what You Need to Know. Available at: <https://www.somersetlive.co.uk/news/somerset-news/hundreds-mobile-phone-apps-can-1637429>. (Accessed 4 July 2022). Accessed:
- Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., Tanczer, L., 2019. 'Internet of Things': how abuse is getting smarter. *Safe – Domest. Abuse Quart.* (63), 22–26.
- Louie, Y.M., 2021. Technology-facilitated domestic abuse and culturally and linguistically diverse women in Victoria, Australia. In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, pp. 447–467.
- Nikupeteri, A., Katz, E., Laitinen, M., 2021. Coercive control and technology-facilitated parental stalking in children's and young people's lives. *J. Gend.-Based Violence* 5 (3), 395–412.
- Office for National Statistics, 2020. Domestic Abuse Prevalence and Trends, England and Wales year ending March 2020' Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseprevalenceandtrendsenglandandwales/yearendingmarch2020>. (Accessed 5 July 2022). :
- PenzeyMoog, E., Slakoff, D.C., 2021. As technology evolves, so does domestic violence: modern-Day tech abuse and possible solutions. In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, pp. 643–662.
- Queensland Government, 2019. 'Technology safety planning' Available at: <https://www.qld.gov.au/community/getting-support-health-social-issue/support-victims-abuse/domestic-family-violence/how-can-i-stay-safe/how-can-i-safely-use-technology/technology-safety-planning#mobile-devices>. (Accessed 5 July 2022). :
- Ramirez, F.A., Lane, J., 2019. Communication privacy management and digital evidence in an intimate partner violence case. *Int. J. Commun.* 13, 18.
- Refuge, 2022a. 'Tech abuse and empowerment service'. Available at: <https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/>. (Accessed 20 June 2022). :
- Refuge, 2022b. What is abuse? Available at: <https://www.nationaldahelpine.org.uk/en/What-is-abuse>. (Accessed 12 July 2022). Accessed:
- Refuge, 2022c. 'Guide to securing your iPhone' Available at: <https://refugetechsaftey.org/iphone-guide/>. (Accessed 12 July 2022). Accessed:
- Rights of Women, 2015. 'Evidencing domestic violence: nearly 3 years on' Available at: <https://rightsofwomen.org.uk/wp-content/uploads/2014/09/Evidencing-domestic-violence-V.pdf>. (Accessed 4 July 2022). Accessed:
- SafeLives, 2022. 'Digital and online safety' Available at: <https://safelives.org.uk/tech-vs-abuse>. (Accessed 4 July 2022). Accessed:
- Silva, S., Franco, T., 2020. How Smart Devices Are Exploited for Domestic Abuse. Available at: <https://www.bbc.co.uk/news/technology-54554408>. (Accessed 4 July 2022). Accessed:
- Statcounter, 2022a. 'Mobile Operating System Market Share Worldwide' Available at: <https://gs.statcounter.com/os-market-share/mobile/worldwide>. (Accessed 5 July 2022). Accessed:
- Statcounter, 2022b. 'Mobile Operating System Market Share United Kingdom' Available at: <https://gs.statcounter.com/os-market-share/mobile/united-kingdom>. (Accessed 5 July 2022). Accessed:
- Sugiura, L., Nurse, J.R.C., 2022. How Tech Is Driving New Forms of Domestic Abuse. Available at: <https://theconversation.com/how-tech-is-driving-new-forms-of-domestic-abuse-176187>. (Accessed 4 July 2022). Accessed:
- Todd, C., Bryce, J., Franqueira, V.N., 2021. Technology, cyberstalking and domestic homicide: informing prevention and response strategies. *Polic. Soc.* 31 (1), 82–99.
- Williams, S.R., Afrouz, R., Vassos, S., 2021. Exploring Rural and Regional Social Workers' Perceptions and Practices of Technology-Facilitated Domestic Abuse. *Australian Social Work*, pp. 1–14.

Woodlock, D., 2017. The abuse of technology in domestic violence and stalking. *Violence Against Women* 23 (5), 584–602.

Woodlock, D., Mandy McKenzie, Deborah Western & Bridget Harris, 2020. Technology as a weapon in domestic violence: responding to digital coercive

control. *Aust. Soc. Work* 73 (3), 368–380. <https://doi.org/10.1080/0312407X.2019.1607510>.

Yardley, E., 2021. Technology-facilitated domestic abuse in political economy: a new theoretical framework. *Violence Against Women* 27 (10), 1479–1498.



DSPACE

<https://dspace.org/>

Can signs of digital coercive control be evidenced in mobile operating system settings? - A guide for first responders

Horsman, Graeme

2023-03

Elsevier

<https://doi.org/10.1016/j.fsidi.2022.301483>

Horsman G. (2023) Can signs of digital coercive control be evidenced in mobile operating system settings? - A guide for first responders. Forensic Science International: Digital Investigation, Volume 44, March 2023, Article number 301483