AUSTRALIAN JOURNAL OF FORENSIC SCIENCES
https://doi.org/10.1080/00450618.2023.2252472

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Reviewing the devices of those subject to Sexual Harm Prevention Orders (SHPOs): iOS opportunities, limitations and strategies

Graeme Horsman

Cranfield Forensic Institute, Cranfield University, Bedford, UK

ABSTRACT

In England and Wales, Management of Sexual or Violent Offenders (MOSOVO) teams are often tasked with managing offenders that are subject to Sexual Harm Prevention Orders SHPOs. These orders are put in place to protect the public and contain a series of prohibitions that allow for an offender's conduct to be regulated and reviewed. SHPOs can be used to govern how offenders use their digital devices, particularly with regard to accessing the internet and the sending of electronic communications. To ensure SHPO compliance, officers frequently conduct reviews of any offender's devices, sometimes manually by traversing a device's menus and screens. These device manual reviews are not easy to conduct, often done under time pressures and in the knowledge that any missed evidence of misconduct may facilitate an offender to continue any wrongdoing and potentially increase the risk of harm to members of the public. Further, it is not always technical specialists undertaking this role. This work outlines a manual review strategy for devices running the operating system iOS (Apple products) to support officers in this role. Guided by commonly included SHPO prohibitions, relevant digital traces for evaluating SHPO compliance are highlighted, and limitations surrounding determining user behaviour are also discussed.

ARTICLE HISTORY
Received 21 July 2023
Accepted 20 August 2023

KEYWORDS
Digital forensics; investigation; device examination; sexual harm prevention order; digital evidence

1. Introduction

According to the Office of National Statistics[1] it is estimated that for the year ending March 2022, over 1 million adults were victims of sexual assault (including attempts). For this same period, police recorded almost 200,000 offences[1]. It is suggested that in most cases where a defendant is sentenced for a sexual offence, a Sexual Harm Prevention Order (SHPO) will be applied for by the prosecution[2] and for the period 2020–21, over 4300 SHPOs were imposed[3]. These orders are put in place to protect the public and contain a series of prohibitions that allow for an offender's conduct to be managed and reviewed[4]. In some cases, SHPOs are set up to control how offenders use their digital devices and often particularly in relation to their conduct online, both web browsing and

CONTACT Graeme Horsman graeme.horsman@cranfield.ac.uk

The author is responsible for all work in this article.

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

the sending of electronic communications. In England and Wales, offenders of this type often fall under the control of Management of Sexual or Violent Offenders (MOSOVO) teams who are responsible for 'managing offenders according to the level of risk of harm they pose to the public'[5]. Where a SHPO is in operation that regulates digital device usage, this may involve[6] 'carrying out unannounced visits at an offender's home, accessing their electronic devices and speaking to them about their daily activity'[7]. This is done in an attempt to establish previous and continued compliance to the conditions of their order.

Whilst the installation of monitoring software upon the devices of those subject to a SHPO in order to log behaviour is an option[8], it may not always be technically possible (for example, device incompatibility). Some at-home device reviews may be conducted via the use of triage tools (should they be available and any officer be appropriately trained in their use), however some need to be conducted manually by an officer by traversing a device's menus followed by a review of any content that is displayed on-screen[9]). Manual device reviews are the focus of this work, where the effectiveness of them is dependent on the knowledge and skills of the officer administering the review, who must have both knowledge of the device to be able to effectively navigate it, and an understanding of the types of information that could be available that may show order-breaching behaviour, or conversely compliance. Device manual reviews are not easy to conduct, often done under time pressures and in the knowledge that any missed evidence of misconduct may facilitate an offender to continue any wrongdoing and potentially increase the risk of harm to members of the public. Further, it is not always technical specialists undertaking this role. These difficulties are also compounded by the volume of offenders requiring management, where some MOSOVO teams are reported to handle over 1000 offenders[8].

Creedon[10], notes those organizations tasked with offender monitoring must make changes to ensure their practices are effective when facing the changing nature and complexities in this area of offending. Given the importance of at-home device reviews, it is necessary for those conducting these to have an appropriate strategy in place to ensure a comprehensive and appropriate inspection is administered. This includes understanding what and where any relevant digital traces exist on a device that describe an offender's behaviour, as well as understanding the limitations for carrying out this task. Whilst overarching guidance for conducting manual reviews is offered by[11], this work outlines review strategy for devices running the operating system iOS (Apple products) to support officers in this role. Guided by commonly included SHPO prohibitions, relevant digital traces for evaluating SHPO compliance are highlighted, and limitations surrounding determining user behaviour are also discussed.

2. SHPOs

Crown Prosecution Service[4] guidance notes that from '8 March 2015, Sexual Offences Prevention Orders (SOPOs) were replaced by SHPOs. Section 103 of the Sexual Offences Act (SOA) 2003 deals with SHPOs'. Under Section 103A SOA, a court can make a SHPO where it is satisfied that it is necessary for '(i) protecting the public or any particular members of the public from sexual harm from the defendant, or (ii) protecting children or vulnerable adults generally, or any particular children or vulnerable adults, from sexual harm from the defendant outside the United

Kingdom'. When making a SHPO, ensuring that it is both proportionate, and capable of being policed effectively is important[12], with the latter issue a particular focus of this work. Where a SHPO is in place to manage an offenders conduct in regards to their digital devices, it is typical for the following prohibitions to be in place (a comprehensive discussion of suggested terms is provided by the Crown Prosecution Service (2021)):

- Any devices used for Internet access must be discussed with and approved by a monitoring team, capable of storing and retaining records of internet history, and these devices must be made available for review on request.
- Internet history must not be deleted or 'private browsing' functions used.
- The use of Cloud storage must be declared and approved.
- Encryption or deletion software must not be used, or anything that interferes with relevant data being stored/accessible[13].
- Communication with others, particular via social media, may be prohibited or monitored in regards to specific subsets of society (i.e. under 18s).
- The use of aliases when accessing web services is prohibited unless declared and approved.

Those in receipt of a SHPO that contain some or all of the prohibitions noted above are often subject to regular review, where 'officers will often make unannounced visits to offenders where they are subject to an intrusive investigative interview process. This helps to understand their routines, interests and behaviours'[14], and to 'check compliance with legislation and court orders'[15]. How often an offender is visited can depend on the assumed risk they pose, case circumstances and the types of prohibitions set out in their SHPO[15]. Those conducting a visit and review should adopt an investigative mindset and be wary of manipulation[15]. Whilst monitoring software can be installed on these devices, if this is not possible, it does not preclude the device from being used by the defendant providing that its use has been approved in writing by any monitoring team (noted in R. v Davidoff [2022] EWCA Crim 1253).

As noted, SHPOs are a frequently used offender management tool and breaches of them are not uncommon. SHPO breaches for the use of undeclared aliases[16,17], using undeclared digital devices for accessing the Internet, deleting communication records[7] and deleting history records[14,18] have been reported.

3. A device manual review strategy – iOS

Where monitoring or tool-based reviews are not possible, any officer is limited to manually reviewing any offender devices for signs of compliance to an order, or breaching behaviours. This can be challenging due to the complexity that many devices offer and their ability to be configured in an almost infinite number of ways. It is argued that officers tasked with examining digital devices under these circumstances must have a range of technical skills, knowledge and competencies, and initial and continuing training should be provided[10]. It is necessary to state that continuous upskilling for this task is required due to changes in device functionality, meaning that techniques and knowledge applicable today may no longer be applicable in a year's time. Stagnation of knowledge in this

working role can arguably lead to missed information and a failure to detect breaching conduct. Officers need to know where to look on a device, what digital traces to look for and the meaning of them.

This work provides a strategic review of iOS in order to support those conducting manual device reviews of this type to identify digital traces relevant to assessing an offender's compliance with a SHPO. To supplement this work, all findings and tests were conducted on an iPhone 12 running iOS 16.5, the latest version of iOS at the time of writing. Consideration of the techniques and traces applicable to a device review are structured around core SHPO prohibitions, starting with that of Internet history access.

3.1. Internet history

The Internet has now provided individuals with more opportunities and greater access to child sexual abuse material, creating a regulatory challenge[10]. One of the core aspects of a SHPO involves the use of the internet and retention of records showing this usage – '*Internet History*' where a SHPO can prohibit, limit or manage any specific actions of an offender whilst online[4]. A SHPO cannot typically prohibit a defendant's use in its totality, as the Court of Appeal in R v Parsons; Morgan [2017] EWCA Crim 2163 struck down the use of such clauses that would amount to this in favour of restrictions more appropriate for offender management[19,20]. Therefore in drafted SHPOs, Internet usage is typically confined to devices that any monitoring team is aware of, and the device itself can retain records of Internet use which the defendant must not delete[4]. An example of such clauses can be seen in the case of R. v Davidoff [2022] EWCA Crim 1253 where in regards to a any devices a defendant wishes to use for accessing the Internet, it must have 'the capacity to retain and display the history of internet use and he does not delete such history or conceal the history (not to use such things (as) incognito browsing, in private, private browsing, virtual computer or VPN)'.

Reviewing historical Internet behaviours can be a challenge for any device examiner as there are techniques that an offender can deploy that would remove or obfuscate their behaviour. For example, historic usage of private browsing has been shown to be difficult to detect in some cases[11]. For this reason, monitoring and forensic approaches may be more beneficial given they are likely able to detect in real time actions and log this history.

3.1.1. Safari – the default browser

The Safari Internet browser is proprietary to iOS and cannot be deleted, therefore whilst there is an option to download and instal 3rd party browsers, it is not necessary for users of Apple devices to access the Internet. In regards to Internet history records (IHRs), there are three important points regarding Safari.

IHRs are maintained by Safari for up to one month on some iPhone, iPad and iPod touch models[21]. A review of our test device confirmed this was the case. IHRs display both the full URL and are categorized into blocks by date. Therefore device reviews that take place less frequently than month are unlikely to see some historical browsing records due to the natural function of Safari.

Individual IHRs can be selected and deleted through the browser's user interface, meaning that offenders can selectively remove content they may wish to conceal. In

addition, Safari allows a user to 'clear' all of their IHRs, to clear 'todays and yesterdays', 'todays' or 'the last hour'. Safari cannot be configured to not store IHRs at all.

There are three tab modes that a device examiner should be aware of (shown in Figure 1); normal tabs, user-created tabs and private tabs. Web addresses visited using private tabs are not stored as IHRs and accessible via the Safari interface. Device examiners should be aware that at any one time, all three or any one of the tab group types may be in operation with open websites. To determine what tab groups are in operation and tabs are open a user must select the 'tab selector' icon, then toggle between 'tab groups'. Each available tab group can be reviewed (see Figure 1).

When a user presses the 'tab selector' icon, thumbnail images of the website are shown (See Figure 1, middle screen capture). This screen capture shows the website content as it was when it was last visited by the user, giving an insight into what was present on screen when the site was viewed. By default, testing showed tabs to be kept open for 1 month by Safari, but this time frame can be reduced to 1 week or 1 day by changing the settings located at 'Settings -> Safari -> Close Tabs'.

A device examiner should also determine the presence of extensions ('a small piece of software you can install to customise your browser's appearance or function'[22]) that can be added to Safari, which may include services such as ad-

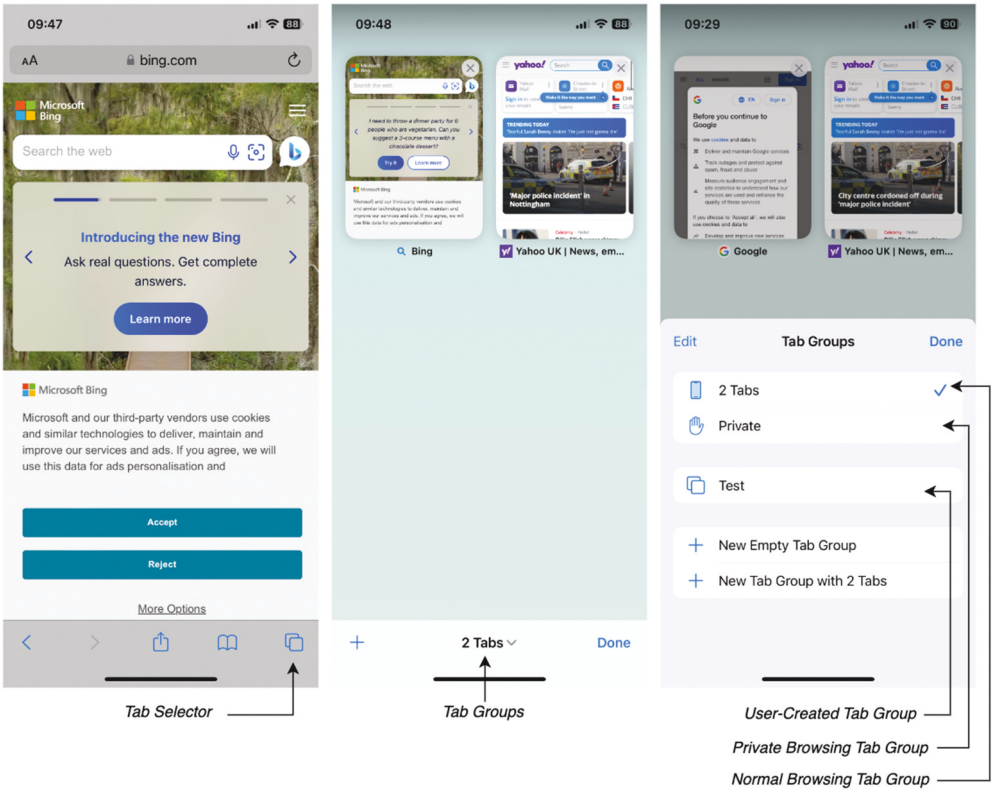


Figure 1. Safari's three tab modes.

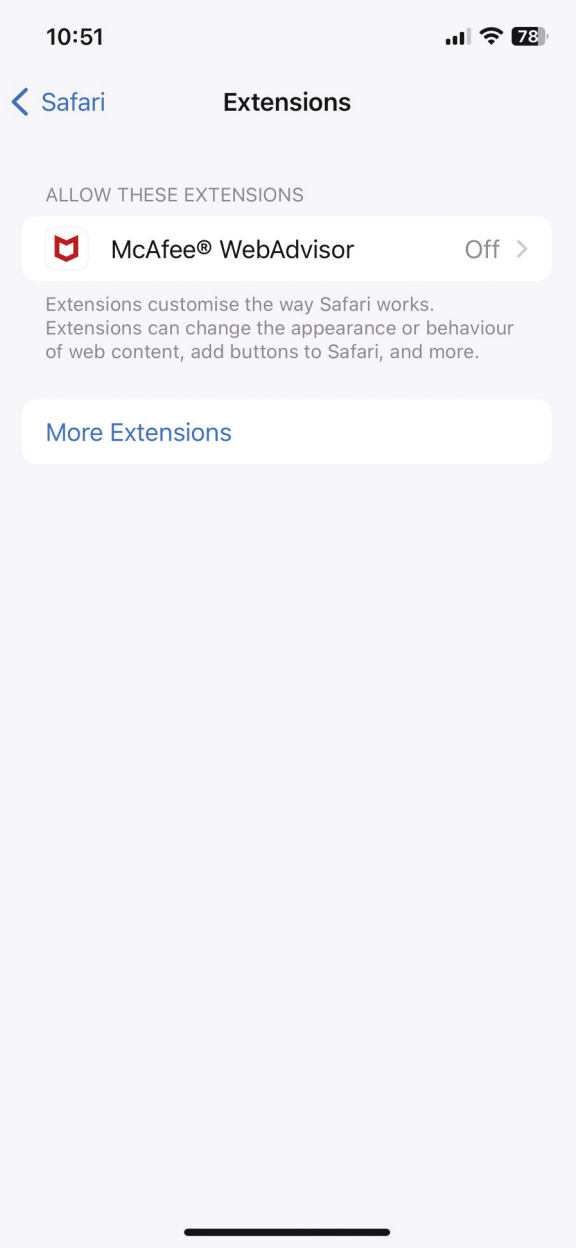


Figure 2. Safari extensions.

blockers, or VPNs depending on what is available from the AppStore. To check for any extensions, a device examiner should navigate to 'Settings -> Safari -> Extensions' (see Figure 2).

Finally, at 'Settings -> Safari -> Downloads', a device examiner should check the location that Safari is configured to store downloaded files. Files can be stored locally on a device or in cloud services such as iCloud.

3.1.2. Chrome (v.114.0.5735.124) – a 3rd party browser

To provide contrast to Safari, Chrome is a 3rd party web browsing application available for download from the AppStore and the most utilized browser worldwide[23], meaning officers are likely to encounter it on suspect devices. Chrome retains IHRs for 90 days[24] where a review of our test device confirmed this was the case. As with Safari, IHRs are organized into date blocks. Testing suggests that like Safari, Chrome cannot be configured so that it does not store IHRs.

A user can delete Chrome's IHRs either individually, or en masse where the 'Clear Browsing Data' option offers time ranges of 'Last hour', 'Last 24 hours', 'Last 7 days', 'Last 14 days' and 'All time' (See Figure 3). Unlike Safari, a user has the ability to clear additional browsing data beyond IHRs, for example cached data.

Chrome offers an 'incognito' browser function where IHRs generated in this mode are not stored by the application and accessible via its interface.

Whilst some of Chrome's settings can be accessed through the main iOS General Settings icon (Settings -> Chrome), these are limited. Instead, Chrome's settings should be accessed from within the application itself (see Figure 4). These settings include the 'History' tile showing up to 90 days of IHRs, 'Downloads' showing the location of and files downloaded, and general application settings including password and payment methods.

Device examiners should also consider whether a Google Account is signed in with Chrome (an initial indicator is shown with the circle icon with an initial inside of it in the top right corner of the screen – see the 'G' account in Figure 4) where the email address associated with it is shown in the main 'settings' window (see Figure 5). Where an account has been signed in, it is possible to view the 'Manage your Google Account' setting and determine which other devices may be used by an offender. This is pertinent for IHR interrogation as within the Chrome application settings – 'Settings -> Privacy and security -> Handoff', where handoff is on, visited websites can be passed to another device to be accessed and potentially, the history of this visit be removed from the iOS device subject to interrogation.

Similar to Safari, open tabs show a thumbnail of the website's contents when it was last viewed, but opening these pages may cause the page contents to reload and change, meaning if these thumbnails are relevant, a record of them should be captured before they are opened. Testing suggests that extensions cannot be added to the Chrome application.

3.1.3. Reviewing IHRs in line with SHPO prohibitions – comments

Both Safari and Chrome store IHRs locally on an iOS device and where IHRs are not present, this can be due to three main reasons, either 1) the user has not browser the Internet with these applications within the period of time subject to a review, 2) the user has browsed the Internet using their private browsing functions, or 3) the user has deleted their IHRs. Individual IHR deletion and private browsing sessions pose a risk to the manual device review process as it is difficult to detect when they have occurred, where it is foreseeable that an offender may plead that they have simply not accessed the Internet. In such scenarios, iOS's ScreenTime facility may help.

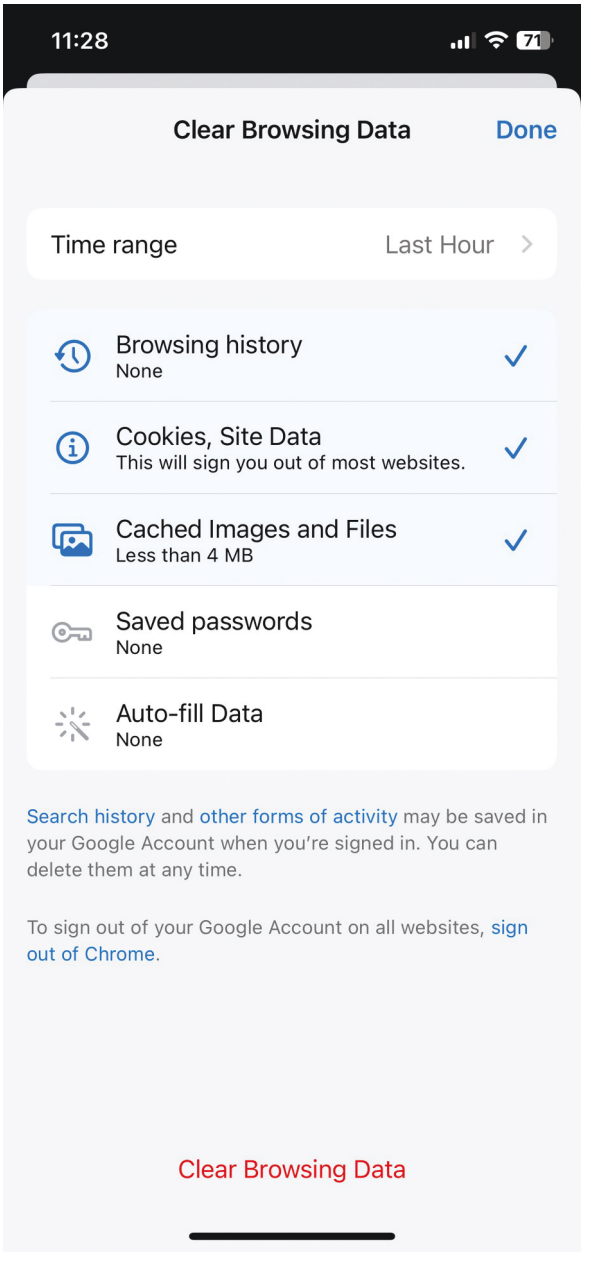


Figure 3. Chrome's IHR deletion options.

3.1.4. How ScreenTime can help

Screen Time on iOS is located in Settings > Screen Time. The 'See All Activity' area of Screen Time provides four weeks of historical user activity if Screen Time has remained active over this period. If at any point Screen Time is turned off, historical records are lost. Screen activity is displayed to users in either 'week' or 'day' view.

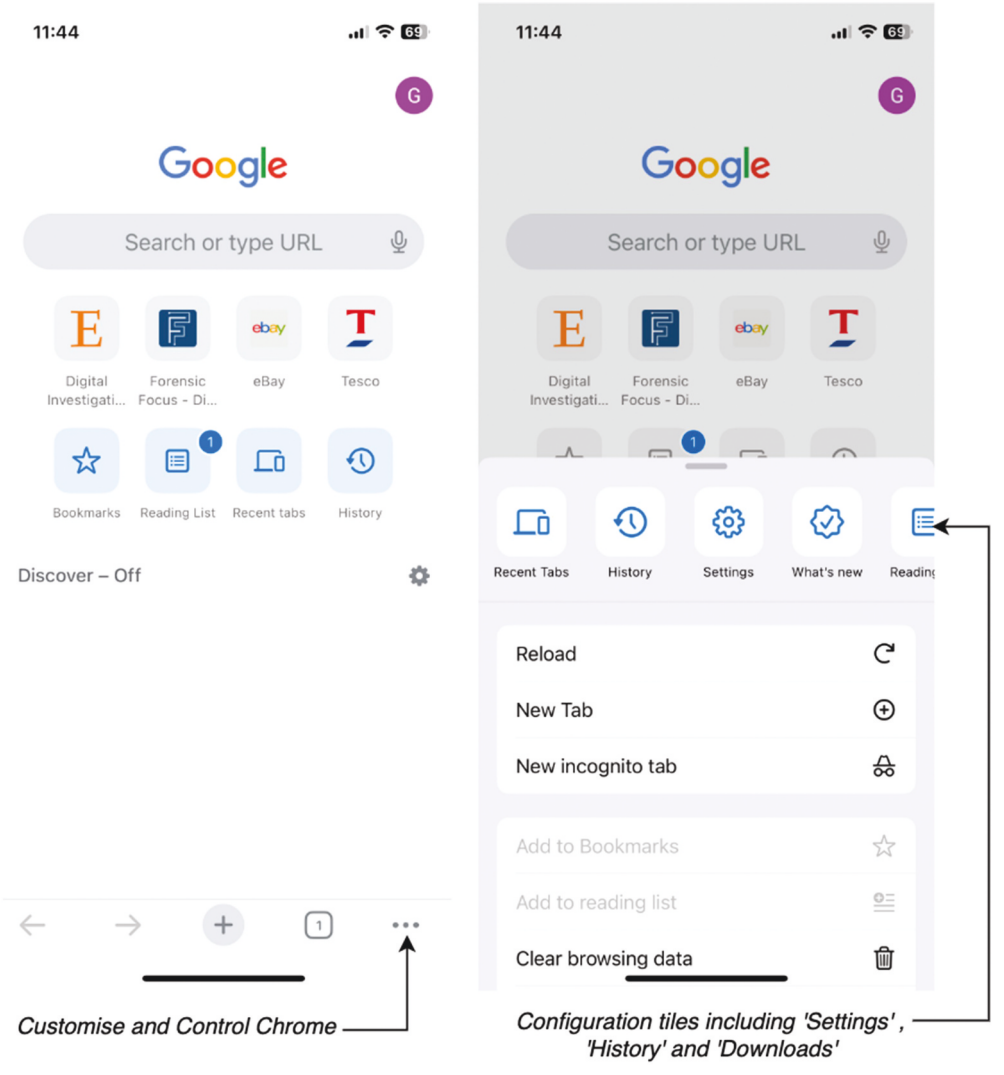


Figure 4. Chrome's internal settings.

3.1.4.1. Interpreting usage information. Each application's usage history is displayed at a week-level, day level and focused-level (see Figure 6). The total time used at both a week and day-level is shown in grey next to each application name (for example, in Figure 6, WhatsApp is shown to have been used for 1 hour 26 minutes across a week period, of which 1 hour 9 minutes was on May 10th). Testing suggests this time is an accumulation of when an application is 'in-focus' on the device's screen. When an application is closed or running in the background, the usage time does not increase.

All applications utilized across each day are recorded and maintain their own usage history. For a given day in the history maintained by ScreenTime, an application's usage across a day can be viewed in detail (see the far-right screen capture in Figure 6 – 'focused-level' mode). This will display how many minutes at each hour an application was used during the 24 hour period.

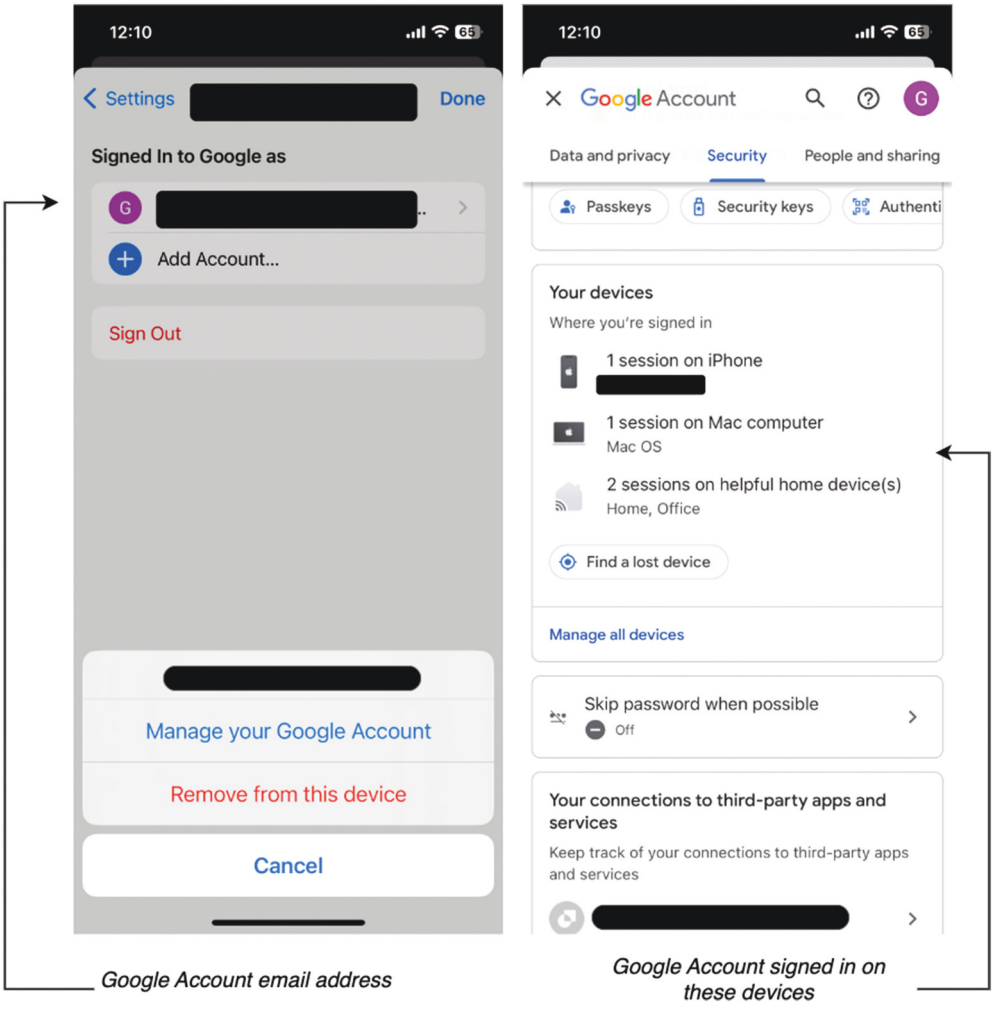


Figure 5. Google account settings and devices.

3.1.4.2. Comparing behaviour. ScreenTime concerns itself with recording when an application is in-focus on a screen and therefore considers this 'usage'. In reality, this description should be treated with caution as the term usage infers that the user is doing something with the application and this may not technically be the case as it is possible for applications to be open but sit idle on a device (i.e. no user interaction). With this in mind, where ScreenTime records usage, we may not be able to say that it is definitive records of an application being used in the sense that most would consider the term usage to mean, but we may treat this information as intelligence that may denote potential periods of application usage by a user. For completeness, an application left in-focus on a device, followed by the device being locked (technically leaving the application in focus on the device) is not recorded by ScreenTime as being used.

The importance of ScreenTime's recording of application usage lies with the fact that it provides a passive and application-independent record of application activity on a device.

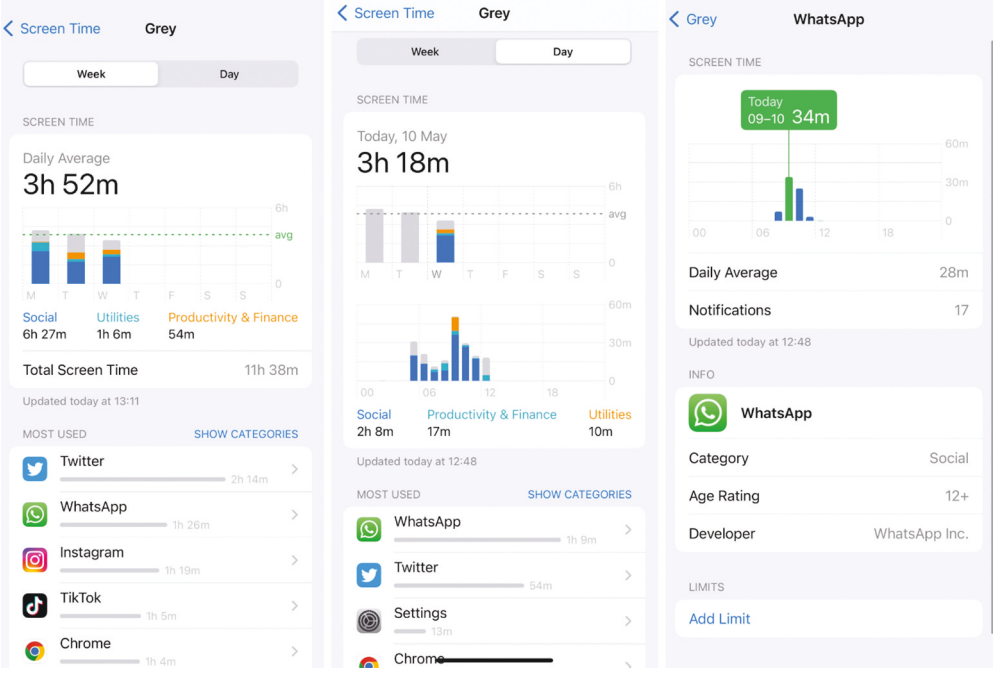


Figure 6. Application usage views – 'week-level', 'day-level' and 'focused-level'.

3.1.4.3. Application records vs. ScreenTime. If we consider those issues regarding IHRs noted in Section 3.1.3, a comparison between ScreenTime and the actual browser's history logs may indicate inconsistencies that could raise concerns. Testing shows one of the benefits of ScreenTimes activity recording is that it doesn't distinguish between Safari or Chrome's normal and private modes when they are active. Figure 7 shows ScreenTime's recording of usage activity on the application Chrome across a day. Highlighted in red is a period of private browsing that occurs just after 18:00 hours. ScreenTime records the user activity on the Chrome application during this period, but a review of Chrome's history does not. There may be two explanations for this, the first, that the application was opened and left idle, or second, that logs of any activity conducted have been removed.

This discrepancy in expected logged activity may raise suspicions that any monitoring order has been breached, either by an offender deleting individual or sections of history, or by using private functions. However, it must be stressed that this cannot be interpreted as an absolute record of private browsing behaviour and should be caveated with the aforementioned information.

4. Determining what applications are on the device

A SHPO may contain prohibitions from using certain applications which could include encryption or wiping software and the use of certain social media applications under certain conditions Scholey and Zadeh[13]. Central to determining whether breaching-

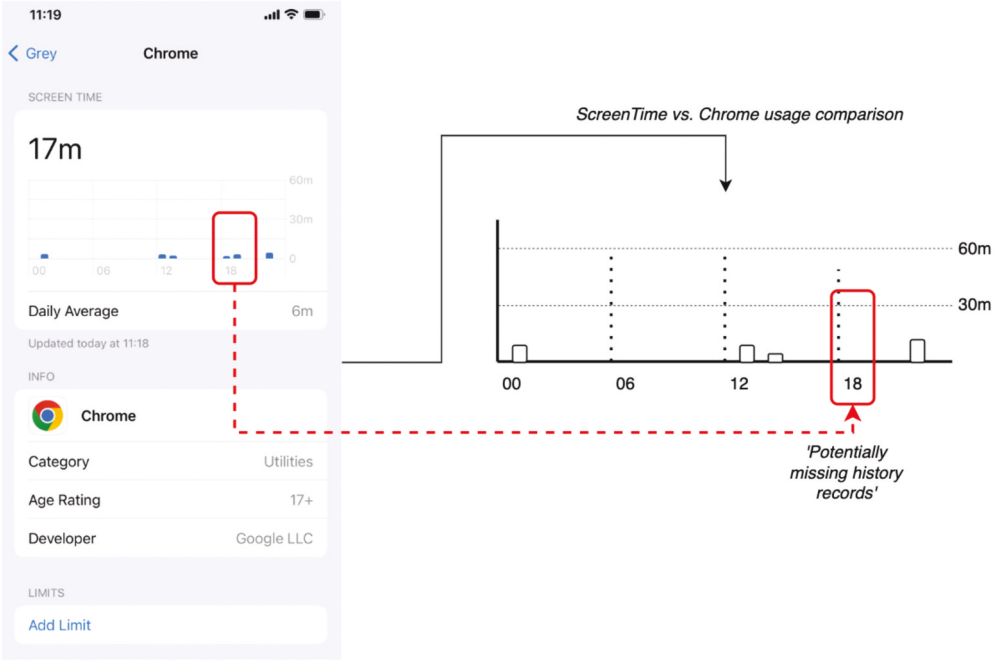


Figure 7. A comparison between activity logged on ScreenTime for Chrome vs. Chrome's internet history records showing private browsing behaviour.

behaviours are present sit with determining what applications are or have been present on the device.

As a start point, device examiners can scrutinize an iOS's home screen, taking into account that multiple screens may exist and are accessible by swiping right and left. However, this should not be considered an exhaustive search of applications on the device. First, application tiles may be present but the application may have been off-loaded by the device as it has remained unused for a period of length (Apple appears to remain silent on how long this is) (see Figure 8 where apps with a 'cloud' icon have been offloaded). Whilst application user data is still present on the device, the application needs to be re-downloaded to access it. The last used date for these applications can be found in 'Settings -> General -> iPhone Storage', meaning that whilst an application may look like it is present and be relevant, the use of it may have been in the past and this date can be determined.

Further, application tiles may not be present on the home screen as when users seek to remove an application from their device, they have the option to delete it, or just to remove it from the home screen (see Figure 10). In addition, it is possible to hide home screens by pressing and holding a home screen followed by selecting the three dots icon, meaning that applications can be hidden from view (see Figure 9).

If an application is removed from the home screen, its tile is removed, but the application is still present on the device. A complete list of all applications on a device (even offloaded applications) can be found in the 'App Library' which is accessible by swiping left as far as possible from an iOS device's home screen (see Figure 10, second

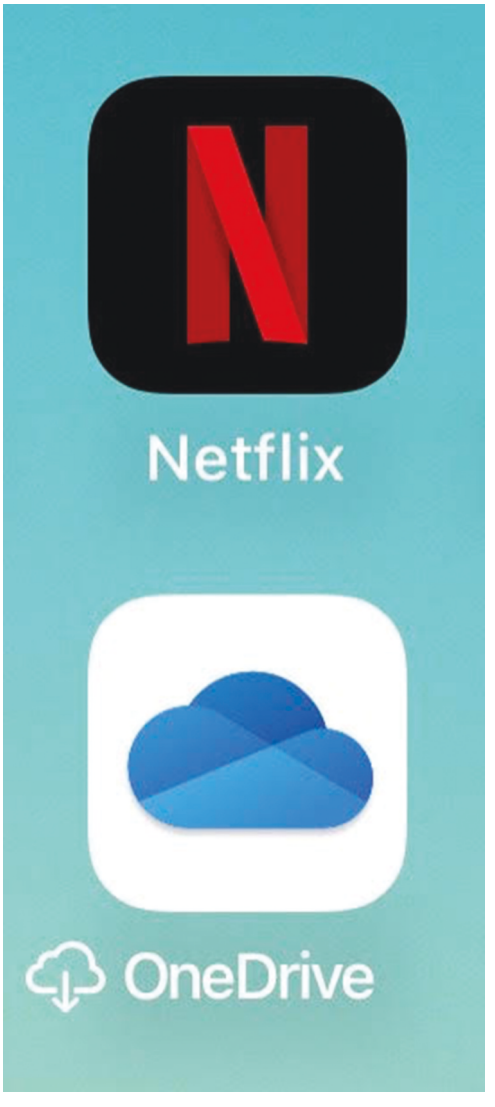


Figure 8. Offloaded applications.

from right screen capture). The App Library also by default organizes applications into categories, for example 'Social' and 'Utilities'. Apple appears silent on the criteria that this categorization is based on, however, there is some correlation between the 'category type' that an application is listed against on the AppStore. The benefits of iOS's application categorization is that it gives a device examiner an indication of what an application is, even if they have never heard of it, based upon the category that it is grouped in.

4.1. Determining something may have been deleted

Using the iOS interface testing suggests it is not possible to determine when applications were deleted from a device. However, it is possible to determine when they were first

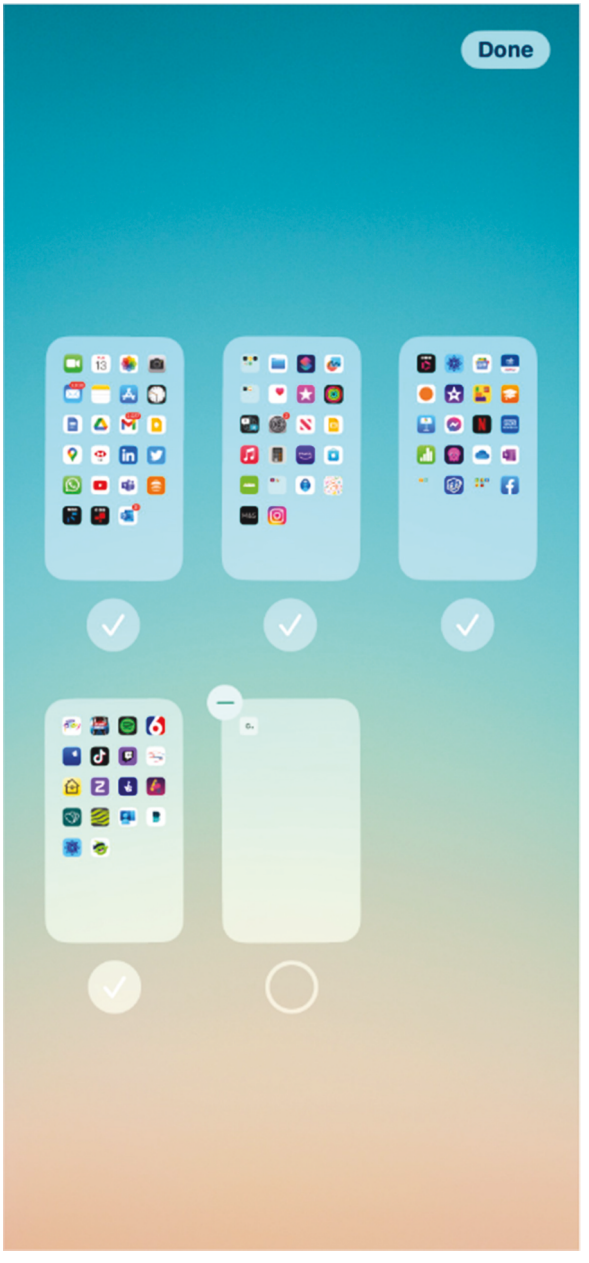


Figure 9. App Library categorization and hiding home screen pages.

installed (Apple phrases this as 'purchased', which includes free applications). Navigating to 'Settings -> Apple ID ->Media & Purchases -> View Account -> Purchase History' a list of all of the applications downloaded (and their download date) by the associated Apple ID is provided. Records appear to be retained for the entire existence of the Apple ID[25] where each application's entry corresponds to the date of first download. Duplicate entries are not created for applications that are deleted and subsequently reinstalled. Cross checking



Figure 10. Application deletion vs. Remove from Home Screen & App Library.

existing applications on a device against those in the 'Purchase History' list can allow an officer to determine the period of time when they were deleted.

*To note: Consideration was given that ScreenTime may record and store activity relating to subsequently deleted apps, however testing showed that when an application is deleted from a device, ScreenTime records immediately update and remove any historic activity relating to the application from their logs.

4.2. Application usage

Determining an offender's patterns of behaviour on their device is often useful when assessing compliance to an order[14]. In Sections 3.1.4.1–3.1.4.3 the value of ScreenTime for showing historic application activity has been noted, but it requires ScreenTime to be turned on and active. There are however two other possible solutions. Under 'Settings -> Mobile Data' a list of all applications currently available on the device is shown and the amount of network data (not wi-fi data) each has been used for a defined period. This period can be 'reset' (See Figure 11, far left screen capture) and from that point data usage is recorded. During each recording period, applications are ranked in order of the most data used, however in addition, if applications are uninstalled, their data is shown under category 'Uninstalled Apps' (see Figure 11, far right screen capture). Officers may see value in resetting data statistics on each visit as on return, not only will they be provided with an indication of applications that are popular on a device, but also that there have been applications on the device that have been uninstalled during the period since the last visit.

In addition, battery statistics located in 'Settings -> Mobile Data' show application activity across 10 previous days giving an indication of those applications that are regularly used (see Figure 12).

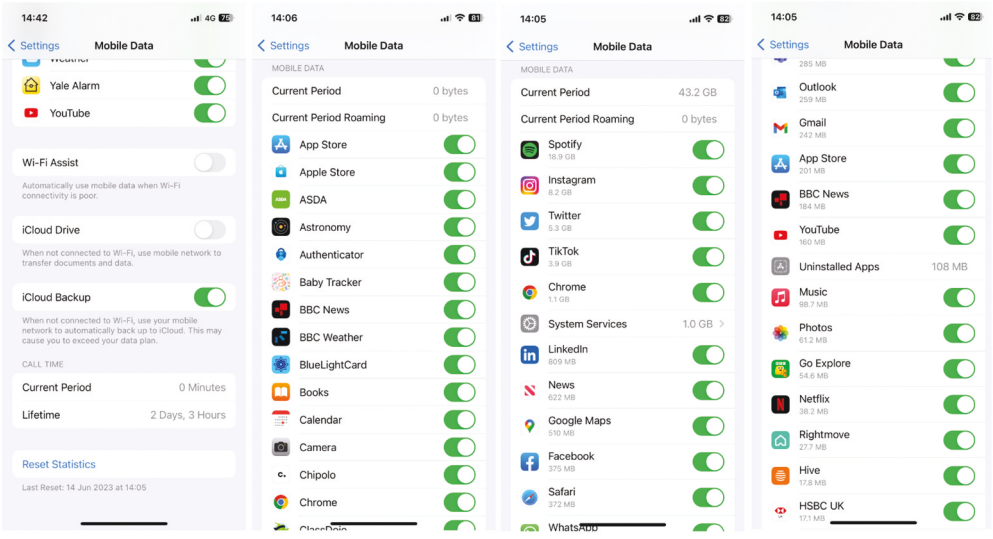


Figure 11. Mobile data statistics.

5. Sending electronic communications

SHPOs may prohibit communication from taking place under certain conditions on social media platforms, and specifically the use of undeclared aliases. Whilst determining which applications are on a device has been discussed in Section 4, this work provides a review of five of the most popular social media platforms to highlight where records of username and account information, direct messaging and account activity can be found within each application. Whilst these applications are not specific to iOS, they have been included given the likelihood of their presence on a device, and that prohibited or limited communication on them is a likely part of any SHPO in place. The aim is to support officers when trying to navigate social media applications to ensure that no relevant information is missed.

(1) Twitter (v9.62):-
   (a) Located at 'Profile tile -> Settings and privacy -> Your account -> Account information', a signed in account's username, phone number and email address can be found. Twitter does not appear to restrict the amount of times that a user can change their username. Nor does the application appear to log a history of username or account information changes. This information may be available via requests to access any accounts archived data ('Profile tile -> Settings and privacy -> Your account -> Download an archive of your data').
   (b) Located at 'Profile tile -> Profile -> Tweets' are tweets made by the account. 'Replies', 'Media' and 'Likes' also show corresponding account activities.
   (c) Located at 'Messages' (the envelope icon), direct message threads can be accessed. Messages sent by the account holder are displayed in blue and received in grey. Details of the message recipient profile can be gained by clicking upon the profile tile at the top of the conversation.

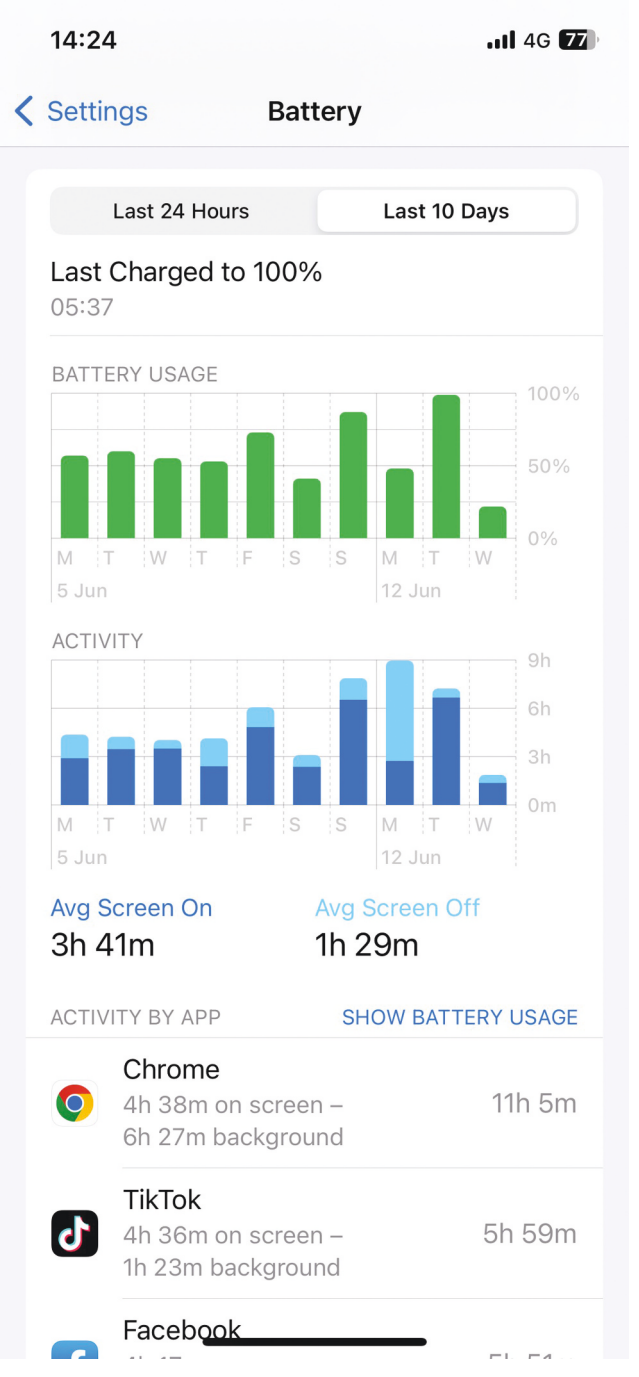


Figure 12. Battery use statistics.

(2) Instagram (v.287.0):-
   (a) Located at 'Profile tile -> Settings and privacy -> Account Centre -> Profiles -> <Profile Name> – > Username', the account username is stored. This can be changed multiple times, however an account 'name' can only be changed twice in 14 days. The account name is visible on the profile's main page. Located at 'Profile tile -> Your activity -> Account History', past account Username and name changes are stored.
   (b) Located at 'Messages' (the paper plane icon at the top right corner of the main screen), direct message threads can be accessed. Messages sent by the account holder are displayed in grey and received in white. Details of the message recipient profile can be gained by clicking upon the profile tile at the top of the conversation.
   (c) Located at 'Profile tile', the main profile page lists 'posts', 'followers' and 'followed accounts'.
   (d) Located at 'Profile tile -> Your activity', records of past account behaviours such as liked content, comments and tags are stored. In addition, search history is stored under 'Recent Searches'.

(3) Facebook (v.419.0):-
   (a) Located at 'Menu -> Settings & privacy -> Account Centre -> Profiles -> <Profile Name> -> Name' the name of the account is stored. Facebook states that this can only be changed every 60 days.
   (b) All accounts associated with the Facebook application can be seen at 'Menu -> Settings & privacy -> Account Centre -> Accounts'.
   (c) Direct message threads are accessible via the 'home wall' by clicking the messages icon (the icon looks like a speech bubble with a lightning bolt in it, located top right of the main screen). This typically loads the separate 'Messenger' application where conversations are stored. In each thread, messages sent by the account holder are displayed in blue and received in grey. Details of the message recipient profile can be gained by clicking upon the profile tile at the top of the conversation.
   (d) Located at 'Menu -> Settings & privacy -> Activity log' behaviours conducted by the profile are stored including interactions, posts and profile information.

(4) WhatsApp (v2.23.9.77):-
   (a) Located at 'Settings -> Profile Tile' the name of the account and the associated phone number is shown.
   (b) Located at 'Chats', all chat threads with contacts are shown. In each thread, the contact's details can be seen by clicking on their profile tile.
      i. Located at 'Settings -> Storage and Data -> Manage Storage' each chat thread is shown. By clicking on each chat thread, the media shared in these threads is shown. This offers a quick way to review media shared between parties.
   (c) Located at 'Calls', WhatsApp call logs are stored.

(5) TikTok (v29.9.0):-
   (a) Located at 'Profile -> Edit profile', the details of the profile signed into TikTok are shown. A profile 'nickname' can only be changed every 7 days. A profile username can be changed every 30 days.

(b) Located at 'Profile', account behaviours including follower accounts, followed accounts and likes can be seen.
(c) Located at 'Settings & privacy -> Content & Display' -> Comment and watch history', comments made by the profile are stored.
(d) Located at 'Inbox', direct message threads are available. In each thread, messages sent by the account holder are displayed in blue and received in grey. Details of the message recipient profile can be gained by clicking upon the profile tile at the top of the conversation.
(e) Located at 'Settings & privacy -> Switch account', all accounts attributed to the application can be seen.

6. Cloud

By default, iOS with an Apple ID offers users access to iCloud and provides 5 GB of free storage (this can be upgraded for subscription costs). Details of iCloud can be found in 'Settings -> Apple ID -> iCloud'. Selecting 'Manage Account Storage' will show an officer the capacity of any iCloud and how much data is stored in there from each of the various applications on the offender's device. Selecting the 'Photos' link, the number of images and videos stored in the iCloud are displayed. iCloud contents can be accessed by visiting www.icloud.com and logging in using the Apple ID credentials.

7. Images

Particularly in relation to cases where an offender has committed offences involving indecent images of children, it is likely that prohibitions in a SHPO include making any device capable of taking or storing images available for review[4]. iOS devices are capable of both, where stored images are accessible via the 'Photos' application. The total number of photos and videos on a device is shown in 'Settings -> General -> About'. In the Photos application itself, to view all images and videos, the 'All Photos' icon should be selected. Metadata regarding each photo (time and date acquired on the device, and where it has come from – for example whether it has been taken by the camera, or saved from Whatsapp) can be seen when the photo is selected and the image is dragged up (press and hold) from the bottom of it.

More details about the type of media in the Photos application can be seen in the 'Albums' tab, where an officer can see what albums a device user has created and any media stored in them. In addition, some applications automatically generate albums to store media that derives from the use of it (see for example WhatsApp where copies of media transfer via conversations are configured to be stored by default). When viewing media in album view an officer must remember that what they are seeing may only be a subset of the overall total amount of media on the device.

7.1. Hidden and deleted images

Images stored in the Photos application can be hidden, preventing them from being accessed by a user without first providing FaceID (but this can be turned off). The 'Hidden' option in Photos is available in the 'Albums' tab, but it will not be visible

unless the 'Settings -> Photos -> Show Hidden Albums' setting has been turned on. There is no way to tell what is inside of the hidden album until access is granted. In addition, when an image or video is deleted, it is moved to the 'Recently Deleted' storage area. This area can only be accessed via FaceID. Each delete image or video shows a '*days until deletion*' value where testing suggests files can exist for up to 30 days, however the app states that it can be up to 40 days before deletion. Users can access these files and permanently delete them before this time period. Like the 'Hidden' album, there is no way to determine what is in the 'Recently Deleted' storage area until access is obtained.

8. Concluding thoughts and discussions

This work provides an examination of iOS in order to help those conducting manual device reviews identify relevant information that could determine that a breach of a SHPO has taken place. Creedon's[10] independent review into the police-led management of registered sex offenders in the community highlights the need for staff in MOSOVO roles to be trained, and have access to continuing training regarding digital devices and their examination. There is an expectation that MOSOVO teams will continue to be relied on heavily to support offender management with no indication that workloads will decrease[10]. SHPOs are in place for the purpose of protecting the public, but they only offer such protection if they can be effectively and appropriately enforced, requiring those in monitoring roles to be able to conduct these duties properly. Worryingly, there are limited existing resources in this area to support officers in these roles where it is suggested that the development of information that highlights those digital opportunities and traces for supporting SHPO device reviews is crucial if it is to remain an effective policing service. This would allow examination strategies to be developed and facilitate more thorough and consistent reviews taking place. This is the motivation behind the production of this work. It is important that in order to fulfil the knowledge and training needs for digital device interrogation under SHPO monitoring conditions, that relevant organizations are tasked with contributing to this area of work. Creedon[10] makes a number of suggestions including a push for the College of Policing to develop appropriate training packages for MOSOVO officers. It is suggested here that this could go further, where collaborative device interrogation guidance could be formalized following contributions from all police force MOSOVO teams in order to establish a comprehensive and agreed upon best practice approach. However, it should be noted that in reality, the logistics of achieving this may be complex. Going further, academic institutes and training providers who conduct current and on-going research into this area should consider whether they can disseminate their findings in appropriate and timely ways. The technology landscape is vast, and therefore it is perhaps unreasonable to expect any single organization to define and maintain best practice training for this task. Nevertheless, attempts at providing such support should be made in some form.

Future research in this area should focus on continuously monitoring and documenting the changes in digital devices and technologies that may impact SHPO device reviews and be seen by officers conducting this work. This involves staying up-to-date with advancements in operating systems, applications, and communication protocols that offenders might use to circumvent SHPO restrictions.

By actively observing these developments, law enforcement officers can better understand the evolving landscape and challenges surrounding their monitoring duties.

Additionally, it is essential to conduct platform-specific reviews for major operating systems such as iOS, Android, Windows, and MacOS. Each platform has unique complexities and security features that require dedicated examination. This focused approach ensures that the findings remain accurate and tailored to the particular platform, preventing any potential cross-contamination of information between different reviews. Furthermore, future studies should explore advanced digital forensic tools and techniques to enhance the efficiency and effectiveness of SHPO device reviews, moving beyond manual reviews to more technological and tool-based approaches. Investigating methods like memory analysis, timeline reconstruction, and data carving can lead to the discovery of more valuable evidence on the offenders' digital activities.

Collaboration and knowledge-sharing among law enforcement agencies, digital forensics experts, and technology companies is also crucial in staying ahead of evolving tactics employed by offenders. Regular workshops, conferences, and training sessions should be organized to ensure that MOSOVO personnel are well-equipped to handle the ever-changing digital landscape effectively. Finally, it is recommended to analyse the impact of emerging technologies such as 5G, Internet of Things (IoT), and artificial intelligence on SHPO device reviews. Understanding how these technologies may influence offender behaviour and communication patterns can help develop proactive strategies for ensuring public safety.

By following these comprehensive recommendations, law enforcement agencies can strengthen their ability to enforce SHPOs effectively, protect the public, and stay ahead of technological challenges posed by offenders.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Graeme Horsman http://orcid.org/0000-0002-0685-0650

References

1. Office of National Statistics. Sexual offences in England and Wales overview: year ending March 2022; 2023 [cited 2023 Jun 13]. Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/sexualoffencesinenglandandwalesoverview/march2022
2. Stone King. Sexual harm prevention orders - a convenient necessity? 2021 [cited 2023 Jun 12]. Available from: https://www.stoneking.co.uk/literature/e-bulletins/sexual-harm-prevention-orders-convenient-necessity
3. Ministry of Justice. Multi-Agency Public Protection Arrangements (MAPPA) annual report 2020/21; 2021 [cited 2023 Aug 3]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1029349/MAPPA_Annual_Report_2020-21.pdf

4. Crown Prosecution Service. Rape and sexual offences - Chapter 15: Sexual Harm Prevention Orders (SHPOs); 2021 [cited 2023 Jun 12]. Available from: https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-15-sexual-harm-prevention-orders-shpos
5. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. Management of sexual offenders and violent offenders (MOSOVO); 2023 [cited 2023 Jun 13]. Available from: https://www.justiceinspectorates.gov.uk/hmicfrs/glossary/management-of-sexual-offenders-and-violent-offenders/
6. Essex Police. MOSOVO DC; n.d. [cited 2023 Jun 13]. Available from: https://www.essex.police.uk/police-forces/essex-police/areas/essex-police/ca/job-descriptions/job-descriptions/mosovo-dc/
7. Hepburn L. Registered sex offender sentenced after deleting intimate messages from phone; 2020 [cited 2023 Jun 12]. Available from: https://www.wisbechstandard.co.uk/news/22651380.registered-sex-offender-sentenced-deleting-intimate-messages-phone/
8. Jacques P. Force using new software app to monitor sex offenders' online behaviour; 2021 [cited 2023 Jun 12]. Available from: https://www.policeprofessional.com/news/force-using-new-software-app-to-monitor-sex-offenders-online-behaviour/
9. Horsman G. Conducting a 'manual examination' of a device as part of a digital investigation. Forensic Sci. Int 40;2022:301331.
10. Creedon M. Independent review into the police-led management of registered sex offenders in the community; 2022 [cited 2023 Jun 16]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145904/Final_Creedon_report_compared.pdf
11. Horsman G. The challenge of identifying historic 'private browsing' sessions on suspect devices. Forensic Sci Int. 2020;34:300980.
12. Sentencing Council. 22. Sexual harm prevention orders; 2023 [cited 2023 Jun 12]. Available from: https://www.sentencingcouncil.org.uk/explanatory-material/magistrates-court/item/ancillary-orders/22-sexual-harm-prevention-orders/
13. Scholey A, Zadeh PB. A digital forensics live suspicious activity toolkit to assist investigators with sexual harm prevention order monitoring. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC), Edinburgh, Scotland; 2022 Jun; IEEE. p. 1–6.
14. Hampshire & Isle of Wight Constabulary. Isle of wight man jailed for sexual harm prevention order breaches; 2021a [cited 2023 Jun 12]. Available from: https://www.hampshire.police.uk/news/hampshire/news/news/2021/october/isle-of-wight-man-jailed-for-sexual-harm-prevention-order-breaches/
15. College of Policing. Home visits; 2020 [cited 2023 Jun 12]. Available from: https://www.college.police.uk/app/major-investigation-and-public-protection/managing-sexual-offenders-and-violent-offenders/home-visits
16. Evans A. Wrexham man who breached sexual harm prevention order avoids jail; 2023 [cited 2023 Jun 12]. Available from: https://www.leaderlive.co.uk/news/23342381.wrexham-man-breached-sexual-harm-prevention-order-avoids-jail/
17. Kennedy P. Recluse breached sex offender order after police visit uncovered online gaming emails; 2023 [cited 2023 Jun 12]. Available from: https://www.gazettelive.co.uk/news/teesside-news/recluse-breached-sex-offender-order-26627955
18. Hampshire & Isle of Wight Constabulary. Sex offender jailed for 30 months for sexual harm prevention order breach; 2021b [cited 2023 Jun 12]. Available from: https://www.hampshire.police.uk/news/hampshire/news/news/2021/november/sex-offender-jailed-for-30-months-for-sexual-harm-prevention-order-breach/
19. Jackson A. Court of appeal: sexual harm prevention orders: appropriate restrictions on Internet access and the use of digital devices R v Parsons; Morgan [2017] EWCA Crim 2163. J Criminal Law. 2018;82(1):11–13. doi:10.1177/0022018318762892.
20. Kelly R, Picton MHHJ. Sexual harm prevention orders and necessity. Criminal Law Rev 2020;2020(5):411–428.

21. Apple. Search your web browsing history in Safari on Mac; 2023 [cited 2023 Jun 13]. Available from: https://support.apple.com/en-gb/guide/safari/ibrw1114/mac#:~:text=On%20your%20iPhone%2C%20iPad%20or,browsing%20history%20for%20a%20month
22. Brave. What are browser extensions, and are they safe? 2023 [cited 2023 Jun 13]. Available from: https://brave.com/learn/what-are-web-browser-extensions/
23. Statista. Global market share held by leading internet browsers from January 2012 to May 2023; 2023 [cited 2023 Jun 13]. Available from: https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/
24. Google. View and delete your Chrome browsing history; 2023 [cited 2023 Jun 13]. Available from: https://support.google.com/chrome/answer/95589?hl=en-GB&co=GENIE.Platform%3DiOS#:~:text=Your%20history%20shows%20the%20pages,deleted%20from%20your%20browsing%20history
25. Horsman G. Can signs of digital coercive control be evidenced in mobile operating system settings?-A guide for first responders. Forensic Sci Int. 2023;44:301483.



https://dspace.org/

Reviewing the devices of those subject to Sexual Harm Prevention Orders (SHPOs): iOS opportunities, limitations and strategies

Horsman, Graeme

2025-01
Taylor & Francis
https://doi.org/10.1080/00450618.2023.2252472
Horsman G. (2025) Reviewing the devices of those subject to Sexual Harm Prevention Orders (SHPOs): iOS opportunities, limitations and strategies, Australian Journal of Forensic Sciences, Volume 57, Issue 1, January 2025, pp. 16-38

Downloaded from a DSpace repository. https://dspace.org/