

OLD LAW, NEW TECH AND CONTINUED OPACITY: POLICE SCOTLAND'S USE OF MOBILE PHONE EXTRACTION

PRIVACY INTERNATIONAL WRITTEN SUBMISSION TO THE SCOTTISH PARLIAMENT JUSTICE SUB-COMMITTEE ON POLICING AND EXTERNAL REFERENCE GROUP ON CYBER KIOSKS

*"SUBJECTING SURVEILLANCE AND PRIVACY HUNGRY TECHNOLOGIES TO
CRITICAL ANALYSIS ... HARDLY GUARANTEES A JUST AND ACCOUNTABLE
SOCIETY, BUT IT IS SURELY A NECESSARY CONDITION FOR ONE."*



Privacy International was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, focuses on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

11 September 2019

Table of Contents

Summary	4 -
1. Review of Police Scotland Inquiry	6 -
2. How should our devices be treated?	10 -
What is mobile phone extraction?	12 -
Types of data extracted	17 -
Cloud Analytics	25 -
Machine learning / AI	35 -
3. How the Cyber Kiosks work	37 -
4. Hubs : The wider picture	43 -
5. Security and digital forensics	45 -
Security and data breaches	45 -
Training and digital forensics	46 -
Audit	49 -
Device security	51 -
6. Legality	52 -
Police Scotland’s position on lawfulness	56 -
Reliance on JL & EI v HMA and HMA v Rollo.....	57 -
Legal Opinion obtained by Police Scotland	58 -
Police Scotland’s Human Rights Impact Assessment.....	59 -
<i>Police Scotland’s Data Protection Impact Assessment</i>	60 -
Scottish Government Position	62 -
International judicial decisions	63 -
Communications data	65 -
Data Protection	66 -
Victims and Witnesses.....	69 -
Article 8	73 -
7. Recommendations	80 -
Conclusion	82 -

SUMMARY

“...A MOBILE DEVICE IS NOW A HUGE REPOSITORY OF SENSITIVE DATA, WHICH COULD PROVIDE A WEALTH OF INFORMATION ABOUT ITS OWNER. THIS HAS IN TURN LED TO THE EVOLUTION OF MOBILE DEVICE FORENSICS, A BRANCH OF DIGITAL FORENSICS, WHICH DEALS WITH RETRIEVING DATA FROM A MOBILE DEVICE.”ⁱⁱ

Mobile phone extraction technologies present great risks to privacy, inappropriate use will be in breach of data protection and human rights safeguards and insufficient consideration has been given to the implications, from the point of view of forensic science, of police officers using new technologies to carry out digital forensics. There are risks relating to quality and reliability of evidence, as highlighted by the House of Lords Science and Tech Committee report into forensicsⁱⁱⁱ, published May 2019.

To ensure that use of these technologies does not result in harm, law enforcement and government must undertake impact assessments in advance of trial, testing and deployment of new technologies. They must develop and implement appropriate legal safeguards, including robust security and risk assessments. Transparency, accountability and consultation is key. As has been seen in recent attempts to force rape survivors to hand over their phones^{iv}, ill-thought through deployment of new technologies can have a chilling effect, in this case stopping the reporting of serious crimes.

It has been said repeatedly by Police Scotland during engagement with the Justice Sub-Committee on Policing and the External Reference Group that investigations increasingly have a digital element. In the document titled Digital Triage Devices, dated 8 May 2019, presented by Scottish Police Authority to the Justice Sub-Committee^v it states:

“Within the UK alone there are over 51 million Smartphone users, which number is growing every year. In 2017, Police Scotland reported that over 40,000 mobile devices were seized. 90% of those submitted for examination were Smartphones....”

These figures are only going to rise. This fact alone is a stark reminder that the law must be sufficient to deal with new realities. Regrettably at present it does not. Police Scotland are relying on a patchwork of statutory provisions and common law powers, none of which are fit for purpose. Despite submission after submission from stakeholders that the legal basis is inadequate, despite the Justice Sub-Committee on policing, who have conducted a detailed inquiry, stating that clarity if needed on the legal framework, and Police Scotland’s own legal advice highlighting the desirability of a “proper legislative framework fit for a digital age” and the merit of a Code of Practice, we are concerned that Police Scotland are determined to deploy cyber kiosks relying on out-dated laws and gloss over concerns and recommendations raised in the Legal Opinion they commissioned. We dispute that the Legal Opinion is

unambiguous, as Police Scotland claim in their letter dated 2 September 2019, in which they confirm operational roll-out as soon as possible:

“As reported to the Scottish Police Authority on 22 May 2019, now that we have unambiguous clarity from both the Crown Office and Procurator Fiscal Service and independent Senior Counsel on the legal basis for their use, and subject to ongoing discussions with the SPA, our intention is to start operational roll-out of cyber kiosks as soon as is practically possible.”^{vi}

As we set out below, extracting and/or examining data from a mobile phone device, either by cyber kiosks or via the cybercrime hub, is self-evidently different from the seizure and examination of physical tangible property, despite claims by Police Scotland that mobile phone extraction is nothing new, and comparable to traditional searches.

It is imperative that a sufficiently up to date legislative framework is applied, that search warrants are required to search electronic devices, which contain specificity with respect to the use of extraction tools. Concerns raised by Privacy International in correspondence with the Investigatory Powers Commissioner’s Office that extraction could constitute interception or Equipment Interference must be borne in mind when considering the appropriate legislative framework and criteria.^{vii}

Despite the tireless efforts of the Justice Sub-Committee to inquire into the previously secret roll out of cyber kiosks, it is a concern that the use of powerful extraction technologies at cybercrime hubs remains relatively unexamined. We highlight below by way of example the deeply concerning developments in cloud analytics and use of artificial intelligence which may likely being used at cybercrime hubs.

There are other unanswered questions, such as the proposal to extend use of cyber kiosks to export and store data, as highlighted by the Sub-Committee. There are also areas that have not received any or any sufficient attention such as the concerns raised by the House of Lords Science and Technology Committee (which whilst focussed on England and Wales merit consideration in Scotland) in relation to digital evidence.

In this document we look at the background to the inquiry including the failure of Police Scotland to originally carry out impact assessments; review our understanding of the functioning of mobile phone extraction technologies and the cyber kiosks and cyber crime hubs in Scotland; highlight issues relating to security and digital forensics; and examine the problems with the existing legal framework.

We are grateful to the Justice Sub-Committee on Policing for pursuing their inquiry and encourage ongoing critical examination of the use of new technologies by the police. We note that Police Scotland have now committed to a Post Implementation Review of Digital Triage Devices approximately six months following roll out^{viii}.

We acknowledge the engagement by Police Scotland in the process and believe that police forces in the rest of the UK would do well to note the value of this experience, even if we have reached a conclusion to the process which we deem unsatisfactory, given the points regarding lawfulness.

1. REVIEW OF POLICE SCOTLAND INQUIRY

- 1.1 In March 2018 Privacy International produced its report 'Digital Stop and Search: How the UK police can secretly download everything from your mobile phone'.^{ix}
- 1.2 As detailed in our report, in response to our Freedom of Information Act request, Police Scotland stated that they do not carry out mobile phone data extraction in low level crime cases using self-service / downloading kiosks. They stated they had previously trialled the use of kiosks in East of Scotland for low-level crime, defined as that which appears from the outset to be a case likely to be prosecuted at 'summary' level.
- 1.3 Privacy International wrote to Michael Matheson, then Cabinet Secretary for Justice, on 4 May 2018, citing concerns that:
 - There is no clear legislation, policy framework, regulation or independent oversight in place for the police's use of this technology, and to protect the public from abuse of this technology.
 - The police are taking data from people's phones without obtaining a warrant.
 - This is often taking place secretly, without individuals – whether they are suspects, witnesses or even victims of crime – being informed that content and data from their phone is being downloaded and stored indefinitely by the police.
 - There is an absence of record keeping or national statistics which leaves this technology open to abuse and unfair targeting of minority groups.
- 1.4 The Herald Scotland reported on 1 April 2018 that the trials, which took place in Edinburgh and Stirling saw 375 phones and 262 sim cards accessed during investigations. Kiosks trials took place at Edinburgh's Gayfield Square Police Station between 10 May and 2 September 2016 and at Stirling Police Station between 19 June 2017 and January 5, 2018. At Gayfield police accessed 195 mobile phones and 262 sim cards. At Stirling 180 phones were accessed^x. No records of the success-rate or legal bases used for the seizure of these devices were retained. Neither were any warrants issued for testing or screening these phones.^{xi}
- 1.5 Police Scotland intend to roll out cyber kiosks to selected police stations across Scotland. There will be 41 kiosks.^{xii} As noted in the Justice Sub-Committee report, Police Scotland purchased these kiosks in April 2018 with the intention to deploy their use throughout Scotland in autumn 2018.
- 1.6 The Justice Sub-Committee on Policing undertook an inquiry into Police Scotland's intention to introduce the use of digital device triage systems (cyber kiosks). The Sub-Committee began its inquiry on 10 May 2018.
- 1.7 During the Sub-Committee inquiry concerns raised, including regarding the legal basis for their use and whether human rights and data protection assessments were in place, meant that Police Scotland postponed the deployment of cyber kiosks.

1.8 At the Sub-Committee meeting of 10 May 2018 Police Scotland confirmed that they had carried out an evaluation of the Edinburgh and Stirling trials, and that a “couple of brief reports were completed at the end of the trials, and prior to moving to the procurement of the kiosks.”^{xiii} The Sub-Committee inquiry resulted in an admission that in fact no report was done for Stirling^{xiv} and Detective Chief Superintendent McLean told the Sub-Committee that for both trials “there could probably have been better record keeping” and that “...if we were to run the trials again I would ensure that there was better governance with regard to the provision of detail.”^{xv}

1.9 In April 2018 Police Scotland provided written submissions to the Justice Sub-Committee on Policing regarding Police Scotland’s digital data and ICT strategy. In this they referred to ‘Digital device triage system – cyber kiosks’. In this they stated that^{xvi}:

Police Scotland Specialist Crime Division Cybercrime Unit anticipate deploying later this year, a system of triage which allows officers to make a very early assessment of which mobile devices require to be examined more fully. The extraction of information locally provides a quick time assessment as to whether or not a device is evidentially meaningful before sending to Cybercrime for examination.

Key information will enable accurate records to be maintained of who has examined what, when and why. Only user logs will be retained on the actual systems for audit purposes.

1.10 At the 13 September 2018 Sub-Committee hearing Police Scotland stated^{xvii} they were working on three documents: a public information leaflet; principles-of-use document that articulates the mechanisms by which data will be managed and the cyber kiosks will be used; and one is an internal document for the users – a toolkit. We understand these remain outstanding as of August 2019.

- A Cyber Kiosk Toolkit: this is a document to provide step by step guidance on the process and use of kiosk;
- A Principles of Use Document – this document seeks to provide an articulation from Police Scotland as to our commitment in how we will use kiosks in compliance with our Code of Ethics and all lawful considerations;
- A Public Information Leaflet – to provide information on what the public need to know should their device be subject to a digital forensic examination

1.11 Police Scotland have also produced in draft the following impact assessments:

- Data Protection Impact Assessment
- Equality and Human Rights Impact Assessment

1.12 On 8 April 2019 the Justice Sub-Committee on Policing published their Report^{xviii} on Police Scotland’s proposal to introduce the use of digital device triage systems (cyber kiosks).

1.13 As acknowledged by Police Scotland, the inquiry of the Sub-Committee has highlighted the importance of this type of engagement. The members of the Sub-Committee have stated on a number of occasions that the process of Police Scotland was back to front, with significant public expenditure purchasing equipment prior to carrying out relevant assessments.

1.14 The report of the Justice Sub-Committee noted that:

“Police Scotland confirmed to the Sub-Committee that no assessments were carried out prior to the trials, saying that: “No assessments i.e. human rights, equalities, community impact assessments and data protection and security assessments were completed prior to trial commencement.” Police Scotland added that it accepted that the introduction of the cyber kiosks had wider implications for data privacy and security and would require its current protocols to be reviewed and that there would need to be wider engagement to inform the required impact assessments.”

1.15 The Sub-Committee report highlighted the comments of Diego Quiroz of the Scottish Human Rights Commission (‘SHRC’) that human rights and equality impact assessments are essential prerequisites, as they ensure that police policy, programmes and projects are compliant with human rights. In relation to the trials, Mr Quiroz said that the assessments should have been undertaken in advance, adding that the Commission questioned the legality of the trials, saying that:

“The Commission has significant concerns about the trial of 600 phones and the legality of how the process has been run so far. We must acknowledge that we do not have the full information about the trial.”

1.16 The Sub-Committee’s report is critical of Police Scotland undertaking trials without undertaking the required governance, scrutiny and impact assessments. **We encourage police forces throughout the UK to take note of this report and inquiry conducted by the Justice Sub-Committee.**

“This lack of effective scrutiny puts the reputation of the police service, and the rights of the public, at risk. It has also led to the investment of over half a million pounds in technology that, at present, Police Scotland is unable to use.”

“The Sub-Committee recommends that the Scottish Government assess the scrutiny and approval process undertaken by Police Scotland and the Scottish Police Authority prior to the trials being approved and report its findings to the Sub-Committee. This should include lessons to be learned to avoid any proposed future technology being trialled by frontline officers, without the necessary safeguards being put in place, and the vital human rights and data protection impact assessments being carried out before any such technology is deployed.”

1.17 Deputy Chief Constable Kerr, in evidence to the Sub-Committee on 9 May 2019^{xix} stated:

“I think that, internally, we fixated too quickly on the technology that was involved and simply did not spend enough time considering how the use of that technology would be perceived by the very citizens we were looking to protect. The significant learning point for us was not just to take a technical approach to the use of a new tool and a new power but to consider how we use it how we explain it and how we engage with community and reference groups. That was a key bit of learning for us that we will take forward.”

- 1.18 Open Rights Group have noted^{xx} the openness and engagement in the consultation process that Police Scotland have undertaken.

“Their willingness to take criticism and advice to improve their current practices is a refreshing one and something police forces across the United Kingdom would do well to take on.”

- 1.19 Privacy International believes it is vital that as police purchase, trial and deploy new forms of surveillance technology, including cyber-kiosks and hubs, there must be transparency and accountability. **Regrettably, the testing, trialling and deployment of new forms of highly intrusive technologies used by the police throughout the UK are by in large not accompanied by impact assessments, adequate safeguards and engagement with the public and civil society.**

2. HOW SHOULD OUR DEVICES BE TREATED?

- 2.1 In their submissions^{xxi}, Open Rights Group asked a key question, how should our devices be treated in criminal investigations:

“Are they to be looked at as a very extensive diary? Is that sufficient to reflect the sophistication of this technology?”

- 2.2 In our submission, the statements by Police Scotland that they are doing nothing new fails to appreciate the wealth of information stored on smart phones. Whilst it has been explored by the Sub-Committee and in written submissions, we set out below a short explanation of mobile phone extraction and the types of data that can be extracted.
- 2.3 We do this not only to underline that what is happening now is new. We seek to emphasise that extracting and/or examining information from a mobile phone device, either by cyber kiosks or via the cybercrime hub, is self-evidently different from the seizure and examination of physical tangible property. We note below that Police Scotland seek to compare mobile phone extraction to examining a briefcase or filing cabinet. It appears this is done in order to justify reliance on existing legal basis. In contrast, Diego Quiroz from the Scottish Human Rights Commission highlighted in evidence to the Committee that “it is possible to find more private information in a mobile phone than in a bedroom or a house.”^{xxii}
- 2.4 We use the term extraction in relation to both the cyber kiosks and the cybercrime hubs. Whilst their operation and use may be different, it is Privacy International’s contention that taking data from mobile phones and viewing this data using Cellebrite tools (or other similar technology), even if it does not constitute a complete physical or logical extraction of mobile phone data, or storage of extracted data, still involves extraction. We briefly explain physical and logical extraction below. We also note that the types of data extracted using cyber kiosks indicates that physical extraction may in fact be used. This is important as physical extraction involves the use of exploits and we note again our submissions to the Investigatory Powers Commissioner’s Office that extraction could constitute interception or Equipment Interference.
- 2.5 In the Data Protection Impact Assessment [“DPIA”] version 0.12, Police Scotland refer to ‘accessing’ data. However, later in the DPIA version 0.12 at Q.37 Police Scotland use the term ‘extraction’ and that there is a need to wipe the kiosk device, indicating that extraction takes place:

“Will the data be encrypted? Any data extracted for display on the kiosk will not be encrypted. Will the data be pseudonymised? If so how? Any data extracted for display on the kiosk will not be pseudonymised.

How will the data be protected against risk of loss, confidentiality, availability and integrity? Any data extracted for display on the kiosk will be securely wiped from the kiosk when the examination is complete.

Will back-ups be taken? If so, when/how often? As data extracted for display on the kiosk is securely wiped after examination, and as no data egress is possible from the kiosk it follows that no backup from the device is possible.”

2.6 We also believe that cyber kiosks are and should be seen as different to what could be termed mobile phone browsing, whereby an officer might look directly at the phone itself by hand, without the use of Cellebrite technology.

2.7 Returning to the issue about whether what is happening is something new, in the first Sub-Committee hearing on cyber kiosks on 10 May 2018^{xxiii}, Kenneth Hogg, Scottish Police Authority stated:

“The authority has asked Police Scotland about implications for data handling that are associated with cyber kiosks. A key assurance that Police Scotland has provided is that the new technology does not extend the powers that the police already have in relation to accessing information on mobile phones. Instead, it lets officers do what they already do more quickly and more locally.”

2.8 On 10 May 2018^{xxiv} Sub-Committee hearing DS Burnett stated that:

“...because the technology is not new – it has been available to United Kingdom law enforcement since the 1990s, and it has been made available to and used by Police Scotland since the force started. The difference is that, due to advances in the technology by 2016, we were able to provide the facility at the front end.”

2.9 As rightly noted by Daniel Johnson MSP^{xxv} in the same hearing:

“You are saying that the kiosks do not provide genuinely new powers and that you have had the technology, in one form or another, since the 1990s. However, the amount of information that is contained on devices has exploded exponentially. Some information is of a sensitive and personal nature, and the information that is available now is not comparable to the data that was captured on SIM cards in the 1990s, which has been referred to. An officer having a look at what home numbers somebody has on their SIM card is one thing, but giving officers the ability to look routinely at all the data that is now available requires additional sensitivity, because we are talking about a different category of information and level of intrusion. Do you acknowledge the difference?”

WHAT IS MOBILE PHONE EXTRACTION?

- 2.10 Mobile phone extraction, also known (rightly or wrongly) as mobile forensics, is growing. Extraction devices are constantly updating due to the rapid changes in technology and the fast-paced evolution of mobile software.

“MOBILE DEVICE FORENSICS IS LIKELY THE MOST RAPIDLY ADVANCING DISCIPLINE THAT DIGITAL FORENSICS HAS EVER SEEN OR EVER WILL SEE, PRIMARILY BECAUSE OF THE RAPIDLY CHANGING ENVIRONMENT OF THE ACTUAL DEVICES. DEVICE OPERATING SYSTEMS HAVE BECOME MORE ADVANCED, AND THE STORAGE CAPACITY ON THE CURRENT DEVICES IS ASTRONOMICAL. TODAY’S DEVICES ARE MOBILE COMPUTING PLATFORMS, BUT ACCESSING THE DATA CONTAINED ON THESE DEVICES IS MUCH MORE DIFFICULT THAN ACCESSING DATA FROM ANY OTHER DIGITAL DEVICE.”xxvi

- 2.11 Mobile phone extraction entails the physical connection of the mobile device that is to be analysed and a device that extracts, analyses and presents the data contained on the phone. Whilst the cyber kiosks are said to be limited in what they obtain, the hubs do not appear to be restricted and the following information is therefore provided on physical, logical and file system extraction on the basis that it may offer insights into the types of extraction that could be carried out in the cybercrime hubs. **We are of the opinion, as are a number of other stakeholders, including Open Rights Group and the Scottish Human Rights Commission, that consideration of the legality of the use of cyber kiosks cannot be divorced from cybercrime hubs.**
- 2.12 There are three generic types of extraction: logical, file system and physical, which can provide a framework to consider extraction technologies. Factors such as the status of the mobile device will determine what type of extraction is possible.

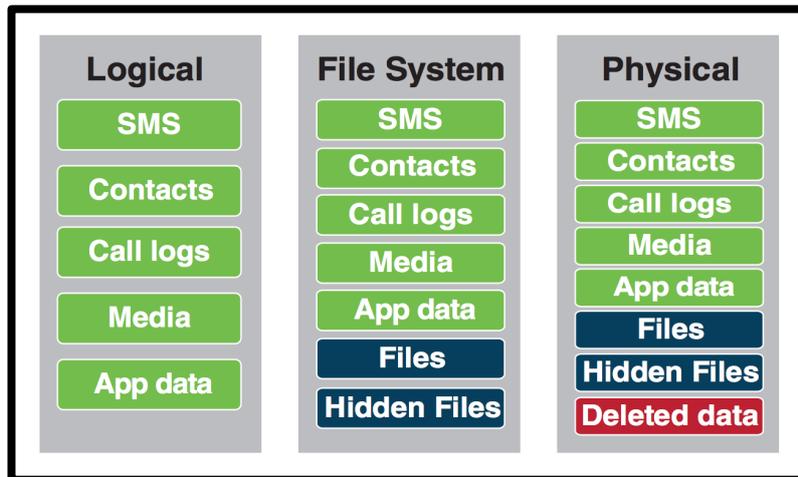


FIGURE 1: SUMMARY OF TYPES OF DATA THAT CAN BE EXTRACTED USING LOGICAL, FILE SYSTEM AND PHYSICAL EXTRACTION^{xxvii}

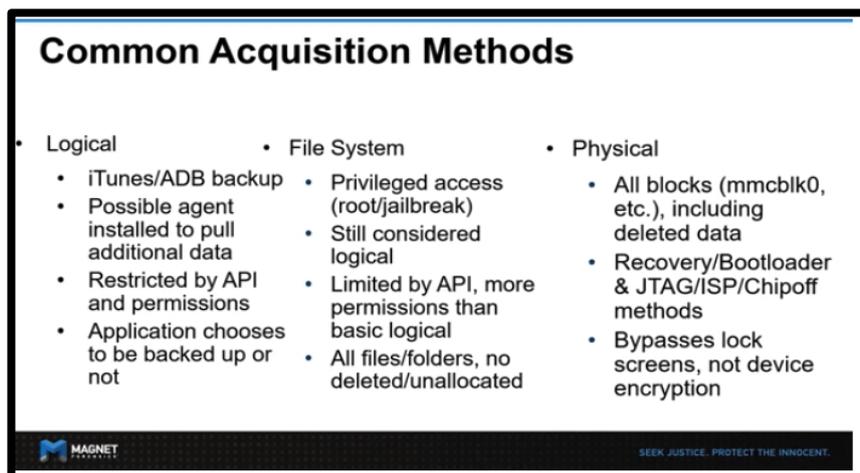


FIGURE 2: COMMON ACQUISITION METHODS^{xxviii}

2.13 Logical extraction is seen as the quickest but most limited. It creates a copy of user accessible files such as phonebook, calls, messages, some app data and other data you might expect from an iTunes or Android backup. Physical extraction is generally the preferred method of the forensics expert. It extracts the raw memory data. Cellebrite refers to file system extractions, although not all providers of extraction technology identify this as a separate type of extraction. This type of extraction can generally obtain more data than a logical but less than a physical extraction.

2.14 There is a valid argument to make that looking at mobile phone extraction through the lens of the common acquisition methods is of limited assistance as different companies interpret them differently. However, it is useful to understand that there are different levels of

extraction and each of these, depending on the phone and operating system, use different techniques and exploits to extract personal data from mobile phones.

2.15 Given that logical extraction is compared to iTunes / ADB backup, we note the following:

iCloud backups include nearly all data and settings stored on your device.

- App data
- [Apple Watch backups](#)
- Device settings
- HomeKit configuration
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Photos and videos on your iPhone, iPad, and iPod touch
- Purchase history from Apple services, like your music, movies, TV shows, apps, and books
- Ringtones
- Visual Voicemail password (requires the SIM card that was in use during backup)
- App data
- [Apple Watch backups](#)
- Device settings
- HomeKit configuration
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Photos and videos on your iPhone, iPad, and iPod touch
- Purchase history from Apple services, like your music, movies, TV shows, apps, and books
- Ringtones
- Visual Voicemail password (requires the SIM card that was in use during backup)

Your iPhone, iPad, and iPod touch backup only include information and settings stored on your device. It doesn't include information already stored in iCloud, like Contacts, Calendars, Bookmarks, Mail, Notes, Voice Memos: [shared photos](#), [iCloud Photos](#), Health data, call history, and files you store in [iCloud Drive](#).

1. When you use [Messages in iCloud](#) or turn on [iCloud Photos](#), your content is automatically stored in iCloud. That means they're not included in your iCloud Backup.
2. Your iCloud Backup includes information about the content you buy, but not the content itself. When you restore from an iCloud backup, your purchased content is automatically redownloaded from the iTunes Store, App Store, or Books Store. Some types of content aren't downloaded automatically in all countries or regions. Previous purchases might be unavailable if they've been refunded or aren't available in the store. Find out [what you can redownload from iTunes in your country or region](#) and [what you can buy from the iTunes Store in your country or region](#).

3. If you use iOS 11 or earlier, Voice Memos are included in iCloud Backup.
4. If you use iOS 10 or earlier, call history is included in iCloud Backup.

iCloud backups don't include:

- Data that's already stored in iCloud, like Contacts, Calendars, Notes, iCloud Photos, iMessages, Voice Memos, text (SMS) and multimedia (MMS) messages, and Health data*
- Data stored in other cloud services, like Gmail and Exchange mail
- Apple Mail data
- Apple Pay information and settings
- Face ID or Touch ID settings

iCloud Music Library and App Store content (If it's still available in the iTunes, App, or Apple Books store, you can [tap to re-download](#) your already purchased content.)

*When you use [Messages in iCloud](#), Health data on iOS 12 or later, or [Voice Memos](#), your content is automatically stored in iCloud. If you turn on [iCloud Photos](#), your content is also automatically stored in iCloud.

iTunes backups

From your Mac or PC, you can [make a backup of your device in iTunes](#). Syncing your device with your computer isn't the same as making a backup. An iTunes backup includes nearly all of your device's data and settings. An iTunes backup doesn't include:

- Content from the iTunes and App Stores, or PDFs downloaded directly to Apple Books
- Content synced from iTunes, like imported MP3s or CDs, videos, books, and photos
- Data already stored in iCloud, like iCloud Photos, iMessages, and text (SMS) and multimedia (MMS) messages
- Face ID or Touch ID settings
- Apple Pay information and settings
- Apple Mail data
- Activity, Health, and Keychain data (To back up this content, you'll need to use [Encrypted Backup](#) in iTunes.)

TYPES OF DATA EXTRACTED

“THINK ABOUT HOW PERSONAL A SMARTPHONE IS TO A USER; NOTHING ELSE DIGITAL COMES CLOSE. WE RARELY LEAVE OUR HOMES OR EVEN WALK AROUND OUTSIDE WITHOUT OUR SMARTPHONES WITHIN ARM’S REACH. IT IS LITERALLY A GLIMPSE OF THE MOST PERSONAL ASPECTS OF A HUMAN, ALMOST LIKE A DIARY OF OUR EVERYDAY ACTIVITY.”^{xxxix}

- 2.16 Mobile phones have come a long way since their inception. In a short space of time, devices whose data would disappear when shut down have exploded into powerful computers with enormous storage capacity and processing power. Always within arm’s reach they constantly generate data, from motion and body sensors to applications that record where you are all the time. They hold extra-ordinarily intimate data about our lives and enable minute by minute if not second by second reconstruction of someone’s activities. Mobile phone extraction technology allows an almost unimaginable degree of intrusion into a person’s private life from accessing, extracting and analysing the data. Browsing history alone is like being inside an individual’s mind. The intimacy is phenomenal.

“THERE IS ALMOST NOTHING THAT A PERSON CANNOT DO WITH THESE SMART DEVICES - INCLUDING ACTIVITIES THAT ONLY TEN YEARS AGO REQUIRED DEVICES THOUSANDS OF TIMES THEIR SIZE.”^{xxx}

“... THE INFORMATION CONTAINED ON A MOBILE DEVICE DETAILS, DOCUMENTS, AND EXPOSES THE THOUGHTS, ACTIONS, AND DEEDS OF A USER SUBSTANTIALLY MORE THAN ANY DATA STORED ON A PERSONAL COMPUTER.”^{xxxix}

- 2.17 Mobile phones, and therefore mobile phone extraction technologies, provide the ability not only to relive a phone user’s every step, thought or action, but to do this with a level of recall and analysis that is impossible for the human brain. We cannot remember every place we went yesterday, what we browsed, emailed, messaged, photographed or did on social media. Let alone what we did ten years ago. But these devices can.
- 2.18 As noted by Lee Reiber, author of Mobile Forensic Investigations^{xxxii}, if a picture of an individual were painted with the personal data recovered from a PC, the picture would be a blurry representation with no clear edges. If, however, the data recovered from a mobile device were examined, it would most likely paint a very personal and potentially embarrassing, picture of the individual.

2.19 Police Scotland's DPIA version 0.14 states that personal data and sensitive data will be processed:

"Personal Data including name, identification numbers, location data, online identifiers and factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the individual."

"The data may include anything which can be held on the device and may include, or from which the following may be inferred;

Racial or ethnic origin, political opinions, religious or philosophical beliefs or TU membership; genetic data or of biometric data, for the purpose of uniquely identifying an individual; data concerning health; data concerning an individual's sex life or sexual orientation.

2.20 Data held on mobile phones relates to a large number of individuals who are not the owner/user. As Police Scotland note in DPIA version 0.14:

"...the potential for a large number of individuals to have their data accessed either directly or indirectly (for example as a consequence of their data being held on the device of another person which is obtained and triaged using a kiosk machine) is significant."

2.21 The DPIA version 0.14 states in relation to what personal data will be processed:

"In general terms any data that is held on a device. Mobile data / internet connection will be disabled via SIM removal at point of seizure and confirmed as disconnected / removed by the operator to ensure only data on the device can be seen. There will be no access to the internet / cloud.

The data may include anything which can be held on the device and may include, or from which the following may be inferred;

Examples of data include but are not limited to

- Device information: Phone number, IMEI, IMSI, MEID, ESN, MAC ID
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and picture messages

- Videos and Pictures (in some cases with GeoTag-location info) and creation
- Date and time
- Audio files
- Emails and Web Browsing Information
- GPS and location information
- Social Networking messages and contacts
- Deleted data – call logs, messages, emails
- PIN lock and pattern lock
- Attached media or memory card data (pictures, files, app data located on media card)
- Wireless networks connected to the device”

2.22 The types of data that can be included when using the cyber kiosks are notable, particularly when it is considered, that on 13 September 2018 in evidence to the Sub-Committee DS Burnett stated that^{xxxiii}:

“On the point that Mr Johnson made, because of the huge amount of data on a phone, the search parameters are there to make sure that, if we are looking for a text within a specific timeframe, we can do so. **Can I guarantee that that will be done on every occasion? No, because the data that would potentially be pertinent to an inquiry depends on what is under investigation.**”
[emphasis added]

2.23 The types of data include ‘deleted data – call logs, messages, emails’; ‘emails and web browsing history’; ‘GPS and location information’; ‘Social Networking messages and contacts’. This is considerably more than the owner of a phone would be able to view themselves. It underlines that referring to what the cyber kiosks are doing as ‘mobile phone browsing’ i.e. similar to looking at a phone as the user, is misleading.

2.24 Individuals think that they own their phones, but there is data on their devices they cannot access, they cannot delete, and they cannot check for accuracy, which is only available to those with sophisticated tools, such as the police.

2.25 To elaborate, data that can be obtained from a successful extraction includes address book (contact names, numbers, email etc.), call history (dialled, received, missed, duration, date/time), SMS/MMS, emails, calendar and call logs could be obtained but the forms of data

extend to documents, web browser history, media (e.g. photos, videos), notes, recordings, Bluetooth connections, cell tower connections, Wi-Fi networks, deleted data, maps, autofill, bookmarks, cache, cookies, keyboard cache^{xxxiv} and application data (e.g. social networking data). Individual apps on our phones communicate with the internet, play music, are used for banking, map a house, determine our internal body vitals and track our friends and families movements.

2.26 As part of our research Privacy International extracted^{xxxv} two android phones and one iPhone using Cellebrite UFED Touch 2. By way of example below is the extracted data from an HTC Desire and iPhone SE, both used for around 12 months.

Device information extracted includes:

Bluetooth MAC address

Android ID

Bluetooth device name

Operating System

Android fingerprint

Detected Phone Model

Detected Phone Vendor

Phone Activation Time

Locale Language

Country name

Time Zone

Mock locations allowed

Auto time zone

Auto time

Location services enabled

IMSI

ICCID

Advertising id

MSISDN

Tethering: hotspot password required; last activation time

Unlock pattern.

Physical extraction:

Autofill

Calendar

Call Log

Cell Towers to which the phone had connected

Chats: Facebook; Signal PM; Twitter; WhatsApp

Contacts

Cookies

Device locations

Device notifications

Device users

Emails

Installed Applications

Instant Messages

MMS Messages

Passwords

Powering events

Searched items

SMS Messages

User Accounts

Web Bookmarks

Web History

Wireless Networks

2.27 In addition, under ‘Data Files’ the Cellebrite UFED extracted: applications; audio (e.g. audio recordings); configurations; databases; documents; images; text; uncategorised.

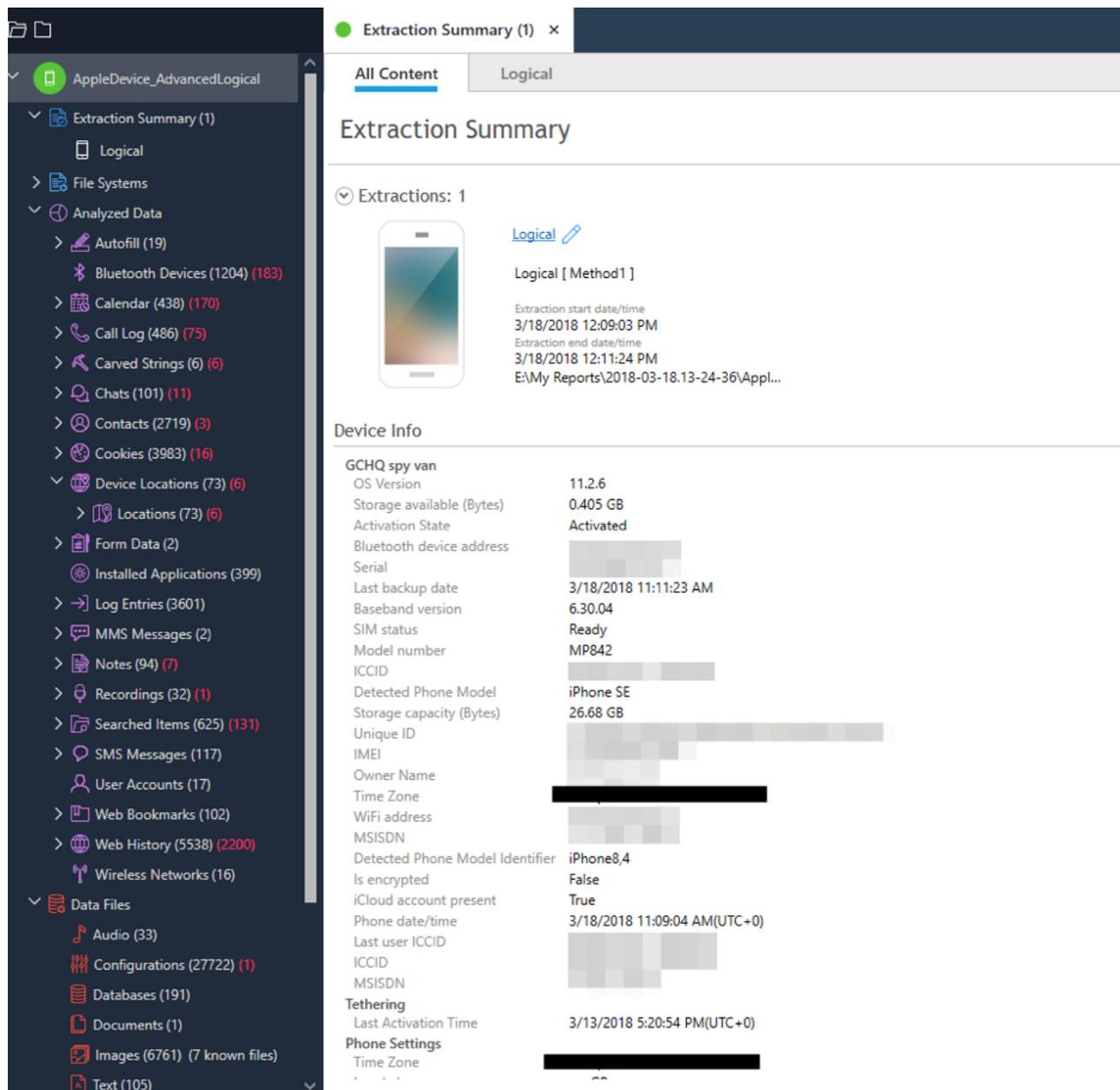


FIGURE 3: LOGICAL EXTRACTION OF AUTHOR'S IPHONE SE USING CELLEBRITE UFED. NUMBERS IN BRACKETS INDICATE DELETED DATA EXTRACTED.

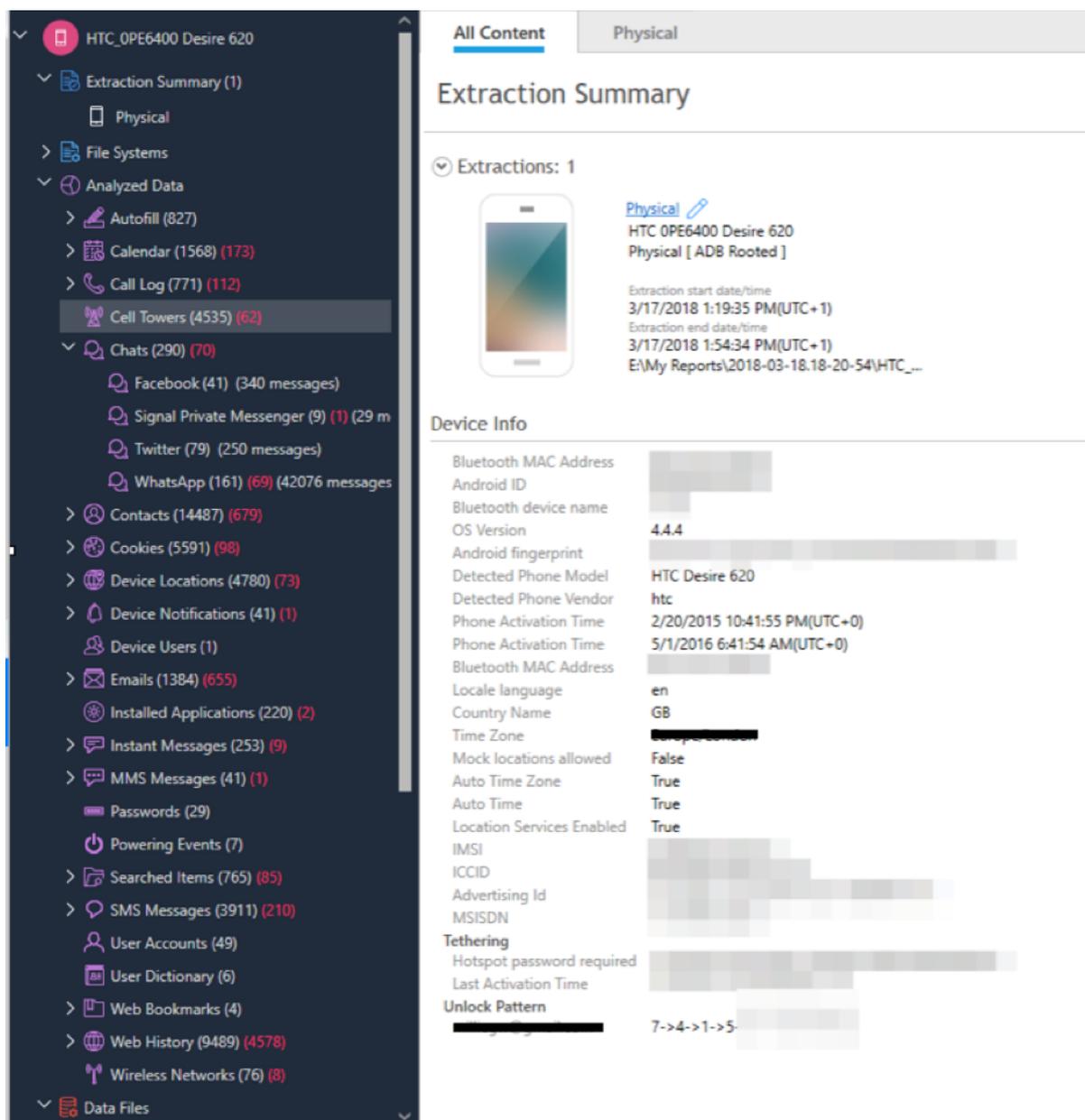


FIGURE 4: PHYSICAL EXTRACTION OF HTC DESIRE USING CELLEBRITE UFED. NUMBERS IN BRACKETS INDICATE DELETED DATA EXTRACTED.

2.28 In the DPIA version 0.14 Police Scotland state that for the cyber kiosks “There will be no access to the internet / cloud.” Police Scotland’s statement needs to be elaborated and interrogated. The question as to whether you can access the Cloud or Cloud stored data is in a sense an arbitrary distinction. Mobile phones store data locally that is hosted in the Cloud. For example, you might store locally (and sync offline) on your phone documents from Google Drive. You have photos on your phone that are synced with a Cloud account. The DPIA 0.14 notes that

cyber kiosks can access, for example: Emails and Web Browsing information; Social Networking messages and contacts.

- 2.29 Admittedly additional data it likely to be accessible if you can then access Cloud based accounts. As explored below this could be a sizeable volume of personal data, which is a further reason why consideration needs to be given to the capabilities of cybercrime hubs and what cloud analytics they are conducting.

CLOUD ANALYTICS

- 2.30 At the Sub-Committee session on 15 November 2018, Clare Connelly (Faculty of Advocates) stated^{xxxvi}:

“In 2013, Mr Justice Cromwell, a Canadian Supreme Court judge, highlighted that the traditional legal framework that would surround search of individuals and their property requires updating in order to protect the unique privacy interests that are at stake in computer searches. The reason for that is that searching a computer- smartphones are computers – is not the same as searching a cupboard or a filing cabinet. A warrant that is granted to allow an office to be searched can set very strict parameters. When you access a person’s mobile phone, you do not access only what is contained in the device in your hand; it is a **gateway to the cloud** and to external sources of information.”

(emphasis added)

- 2.31 At the Committee session on 13 June 2019^{xxxvii} Stewart Stevenson MSP questioned the need for a code for examination of Cloud stored data:

“The cabinet secretary’s comments lead us to the question whether a statutory code of practice is needed ... Does the cabinet secretary think we should have a statutory code of practice not simply for digital device triage systems, but for the seizure and examination of information and communication technology devices more generally? Indeed, to take that little bit further, should we have a code for the examination of data that may be stored beyond a device that someone physically holds in what is now generically called **“the cloud”?**”

(emphasis added)

- 2.32 Cloud analytics or cloud extraction is an area of concern given how much of our data is held on remote servers and accessible with the push of a button using tools such as Cellebrite. Cloud extraction is a leap from what is on the phone to what is accessible from it. It is seen by some as the future of mobile forensics and **its potential use by Police Scotland, whether at cyber kiosks or hubs should be examined**. The risks associated with secrecy surrounding hubs is underlined when one considers use of cloud analytics.

- 2.33 This use of mobile phone extraction tools opens the door to a huge amount of personal information related to social media, internet-connected devices and apps. Cellebrite, with whom the Scottish Police have contracted, claims they can “extract, preserve and analyze public domain and private social media data, instant messaging, file storage, web-pages and other cloud-based content using a forensically sound process”^{xxxviii} The below extracts show a comparison of the amount of data you can extract from a phone compared to the Cloud, showing significantly more in relation to social media, emails, file sharing and location and search history from the latter. Notably “Minute by Minute location information, searches and visited websites” using Google’s time-stamped Location History and Google My Activity data and backups.

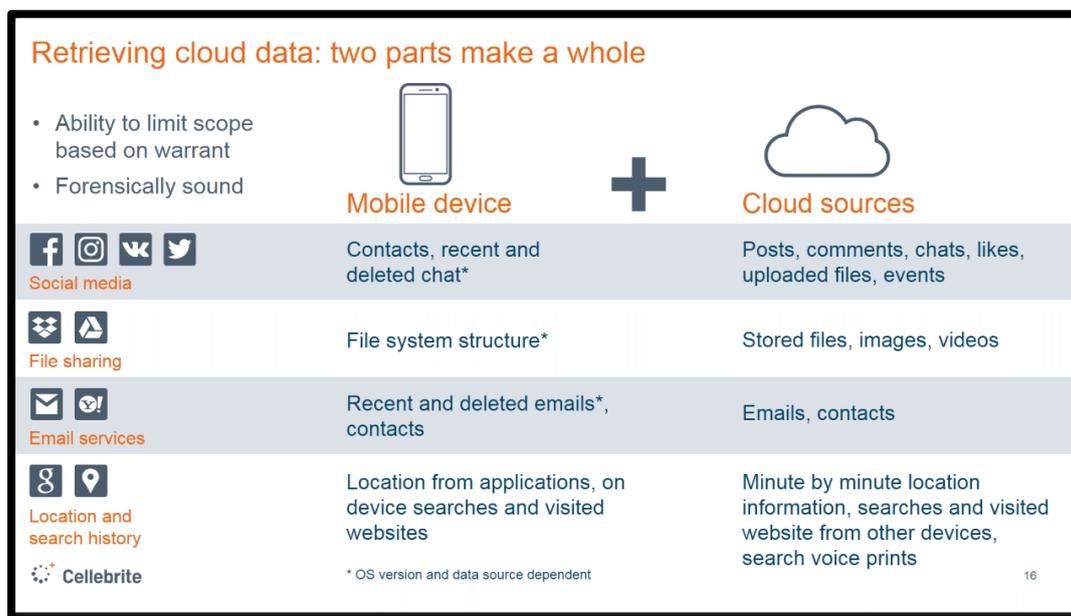


FIGURE 5: COMPARISON BETWEEN MOBILE AND CLOUD DATA^{xxxix}

Source	Type	Mobile Device	UFED Cloud Analyzer
	• Social	• Contacts, recent and deleted chats	• Posts, comments, chats, likes, files, events
	• Storage	• Files stored on the device	• Any uploaded file
	• Email	• Recent and deleted emails, contacts	• Any email on the server
	• Location	• Locations from on device applications	• Minute by minute location with accuracy
	• Browser	• Searches, auto complete, bookmarks and visited pages	• Searches, auto complete, book visited pages and passwords
	• My activity		• Passwords, My activity from an including Google home
	• Backup		• Searches, contacts, call logs, c from locked phone

FIGURE 6: COMPARISON BETWEEN MOBILE AND CLOUD EXTRACTION^{xl}

2.34 The types of data accessible via Cloud Analysis is impressive as it is concerning. Cellebrite’s Cloud Analytics includes a whole suite of Google products, whose ‘History’ function alone enables:

“insights into the subject’s intentions and interests by pulling out the history of text searches, visited pages, voice search recordings and translations from Google web history and viewing text searches conducted with Chrome and Safari on iOS devices backed-up iCloud.”^{xli}

- 2.35 It includes smart devices such as Alexa and Google Home. Cellebrite’s UFED Cloud Analyzer 7.2^{xlii} “provides access to user requests including audio”^{xliii}. As Cellebrite notes,

“The Internet of Things (IoT) has created more ways to use data to make our lives easier, but it has also created more sources of digital intelligence for investigators to access in their criminal investigations.”^{xliv}

- 2.36 Cloud analytics not only reaches into people’s homes but also their bodies with access to data from health wearables.

“Many of today’s users are into health wearables, from the Fitbit to the Apple Watch, which includes information such as heart rate, location, food intake, messaging and other valuable data that is often available only on the cloud service and not on the mobile device.”^{xlv}

- 2.37 Cellebrite can access Fitbit “user profile, logs, activities, goals, friends, heart rate, exercise track (speed, location, time etc.)”

- 2.38 Another area relates to travel and location with UFED Cloud Analyzer 7.3 accessing Google location data and Booking.com “user profile, purchase history, messages and searches” and UFED Cloud Analyzer 7.6 supports extraction from the UBER App and can:

“gain passenger and driver profile data, pick-up and drop-off location logs, and the last 4 digits of a user’s credit card...retrieval of ... credit card details that new users are required to fill in on their first login. As the passenger chooses their pickup location, desire destination, and available driver, each journey is well documented. Recorded routes are aggregated and then categorised by favourite designations. The driver’s information includes the name and photo identification.”^{xlvi}

- 2.39 As of the fourth quarter of 2018, Facebook had 2.32 billion monthly active users.^{xlvii} Amazon had 300 million users in 2017^{xlviii}. Cellebrite’s UFED Cloud Analyzer 7.5^{xlix} Facebook update includes “five brand new capabilities that enable access to activity logs, search histories, pages, user group data and IP address records.” The software can:

“... extract information from the stories and photos a suspect was tagged in to find new leads or new suspects. Additional data points include identification of connections made when liking a page or adding someone as a friend, as well as comments posted, articles read, videos seen, places visited and more.

For user data on groups and pages, UFED Cloud Analyzer 7.5 can also flag if a suspect is a member or administrator of a certain page or group.

This version can also surface the Facebook Log IP address records to allow you to identify a phone or computer's location used to access an account."

- 2.40 UFED Cloud Analyzer 7.5^l "enables access to [Amazon's] the search history, purchase history and delivery addresses that can contribute vital digital evidence to an investigation."

"In this version, you can also view the last 4 digits of a credit card registered on an Amazon account, including the billing and shipping addresses."

"The buyers' search history and wish list over time can indicate suspicious behaviour leading up to a crime."

- 2.41 UFED Cloud Analyzer 7.6^{li} added DJI Drone App and SkyPixel social network which

"Allows examiners to access the app as well as the corresponding users account on the SkyPixel social network. User profile data and stored drone flight log data is retrievable and includes: date, distance, flight time, location, video and imagery. SkyPixel user profile can also assist examiners to verify if any collaboration was performed on specific videos as well as track tags, follows and more."^{lii}

- 2.42 Accessible data relates not just to personal life but includes their work. For example:

"Cellebrite delivers access to shared files and instant messaging data from Slack, the popular communication tool of the business community."^{liii}

- 2.43 UFED Cloud Analyzer 7.9^{liv} includes support for Snapchat and Instagram enhancements:

"Snapchat is a global multimedia messaging app that enables users to share pictures and messages that are only available for a short time before they become inaccessible to their recipients. To date, Snapchat has 190 million daily active users worldwide and more than 400 million Snapchat stores are created per day.

UFED Cloud Analyzer 7.9 introduces first-time support for the Snapchat application, with access using tokens retrieved from any Android device. With this version, you can retrieve backed up files, also known as Memories, and review direct message communications between

contracts. Get access to the contact information of the account and password protected My Eyes Only files.”

“This version of UFED Cloud Analyzer introduces comprehensive support for the Instagram application. On top of already supported data sets in previous versions, you can now view responses to posts which include images and videos. You can also get access to all data associated with chat messages including sharing of post/story, likes, comments within a message.”

Currently supported cloud services^{lv}

	Oxygen Forensics Cloud Extractor	UFED Cloud Analyzer	Magnet Axium
Alexa	YES		
Android Cloud (Google)	YES		
Apple Watch	YES		
Box	YES		YES
DJI Cloud	YES		
Dropbox	YES	YES	YES
Endomondo	YES		
Facebook	YES	YES	YES
Facebook Workplace	YES		
Fitbit	YES		
Google Accounts	-	YES	YES
Google Bookmarks	YES	YES	
Google Calendar	YES	YES	
Google Contacts	YES	YES	YES
Google Chrome	YES		
Google Drive	YES	YES	

Google Events			YES
Google Fit (Google Takeout)		YES	
Google Keep	YES	YES ^{vi}	
Google Location History	YES	YES	
Google Mail	YES		
Gmail		YES	YES
Google My Activity	YES	YES	
Google Photos	YES	YES	YES
Google Password		YES	
Google Profile		YES ^{vii}	
Google Play (Google Takeout)		YES	
Google Tasks	YES	YES	
Google Search History		YES	
Google+ (Google Takeout)		YES	
Keep (Google Takeout)		YES	
Profile (Google Takeout)		YES	
YouTube (Google Takeout)		YES	
Hangouts (Google Takeout)		YES	YES
Chrome – Autofill, Browsing, Bookmarks, Passwords		YES	

Huawei Cloud	YES		
iCloud Applications	YES	YES	
iCloud Backup	YES		YES
iCloud Calendars	YES	YES	
iCloud Call History	YES		
Call Logs (iCloud)		YES	
iCloud Contacts	YES	YES	
iCloud Drive	YES	YES	YES
iCloud iTunes Store	YES		
iCloud Location		YES	
iCloud Mail			YES
iCloud Notes	YES	YES	
iCloud Photo Stream	YES		
iCloud Photos	YES	YES	YES
iCloud Reminder		YES	
iCloud Safari Bookmarks	YES	YES	
iCloud Safari History	YES	YES	
Safari Search (iCloud)		YES ^{viii}	
iTunes purchases		YES	
Instagram	YES	YES	YES
Live Calendars	YES		
Live Contacts	YES		
MAIL (IMAP)	YES		
Mi Cloud	YES		
OneDrive	YES	YES	YES

Outlook Mail IMAP		YES	
QQ Mail	YES		
Samsung Cloud Backup	YES		
Samsung Cloud Data	YES		
Samsung Secure Folder	YES		
Swarm (Foursquare)	YES		
Telegram	YES	YES	
Twitter	YES	YES	YES
Viber (Google Backup)	YES		
Viber (iCloud backup)	YES	YES	
VKontakte	YES	YES	
WhatsApp Cloud	YES		
WhatsApp Google Backup	YES	YES	
WhatsApp iCloud Backup	YES	YES	
WhatsApp (iCloud)		YES	
Yahoo Mail (IMAP)		YES	
Hotmail			YES
IMAP Mail			YES
Live			YES
MSN			YES
Office 365			YES
Outlook		YES ^{lix}	YES

POP mail			YES
SharePoint			YES
Slack App ^{lx}		YES	
Lyft ^{lxi}		YES	
Uber ^{lxii}		YES	
Drone Apps ^{lxiii}		YES	

2.44 Cellebrites Cloud Analyser, using WebCapture, can capture user and device details from routers. This includes WIFI passwords and a list of connected devices.

“Web Capture enables you to:

Automatically collect and hash digital evidence such as media files, recover data and take snapshots of entire web sites.

Focus web searches with customizable capture settings, such as depth level, page downloads and specific URLs.”^{lxiv}

2.45 In addition to the data that can be obtained, once you have an individual’s credentials, you can:

“Track online behaviour

Analyse posts, likes, events and connections to better understand a suspect or victim’s interests, relationships, opinions and daily activities.”^{lxv}

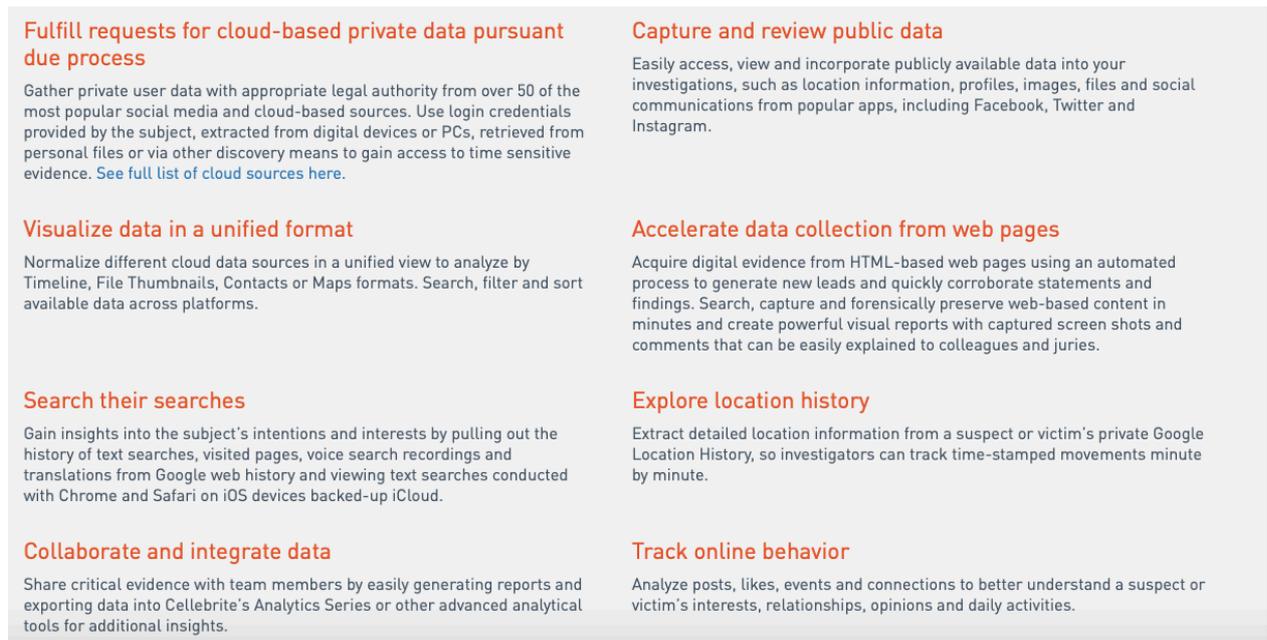


FIGURE 7: CELLEBRITE CLOUD ANALYZER^{lxvi}

2.46 There are a number of ways to access Cloud data. Cellebrite's UFED Cloud Analyzer uses login credentials that can be extracted from the device to pull history of searches, visited pages, voice search recording and translations from Google web history and view text searches conducted with Chrome and Safari on iOS devices backed-up iCloud. Unless login credentials are changed, it allows you to continue to track online behaviour even if you are no longer in possession of the phone.

2.47 It may also be possible to obtain these credentials from a PC. Cellebrite's PC Cloud Collector:

"is an independent tool that creates tokens from a suspect's PC using the cookies in the browsers and the applications that are installed on that PC."^{lxvii}

MACHINE LEARNING / AI

- 2.48 It is worth ending this section with a note on machine learning. Machine learning is promoted by companies including Cellebrite as a way to analyse extracted data. It is not known to what extent this is used by the cyber kiosks for example to identify images or by the cyber-crime hubs on extracted data. Police in the UK are reported to be trialling^{lxviii} Cellebrite's machine learning tools to interpret images, match faces and analyse patterns of communication. Cellebrite states:

"...data can be extracted along with other sources of critical information, such as online activity from email and social media accounts. These sources can then be filtered, compared and analysed using artificial intelligence and machine learning to generate actionable insights, such as locations ... Extracted data can be combined with data from public sources – such as websites or social media accounts – to find crucial information and make comparisons. Investigators can use the combined data to build profiles of attackers, their contacts, and members of terror cells."^{lxix}

- 2.49 Professor Peter Sommer, Professor of Digital Forensics, Birmingham City University, in evidence to the UK Parliament noted:

"Use is also made of data visualisation / link analysis techniques to demonstrate frequencies over time of contacts between phone numbers and between IP addresses, financial transactions and chronologies among others."^{lxx}

"There are, however, weaknesses which should not be underestimated. The first of these is the quality and quantity of the training material offered to the learning program. If the training material is not representative of what you hope to predict results will be poorer. The larger the quantity of material the greater the chance that accurate rules will be derived. Secondly some material is more difficult to parse than others - information conversational language is a classic example. Third, anyone wishing to deploy machine learning has to look at the possibility of bad outcomes - false and negative positives - where a prediction from machine learning gives a misleading results."^{lxxi}

- 2.50 Dr Jan Collie, Managing Director and Senior Forensic Investigator, Discovery Forensics, warned that^{lxxii}:

"... with artificial intelligence, it is very hard to explain what happened and how the machine came up with a particular answer. As a science, it is difficult to put your finger on it and say, "How did the machine come up with an answer?" I did some Ai programming and sometimes you have to say, "I don't know. I put in that and it came out with that."

2.51 Mark Stokes, Head of Digital, Cyber and Communications Forensics Unit, Metropolitan Police in evidence to the UK Parliament^{lxxiii} stated:

“If you imagine a modern mobile phone today, it could have 1 terabyte of data on it, which is 78 million documents or pages of information on one mobile device, and it is becoming impossible for an investigator to review, disclose, analyse, view and read all that information. Therefore, artificial intelligence and machine learning both have a part to play in this, but we have to be very careful in the application of these technologies. We need academia and science to work with us to do the testing and validation. These systems learn—there is a clue in the name—from how they are taught, and if the wrong people teach them they will learn the wrong things, so they could bias themselves in one direction or another. They absolutely have a part to play. Large-scale computing and data storage systems have a part to play. I come back to the fundamental challenge: it requires investment and money because huge amounts of data need processing.”

“It is in its infancy. Some of it is being applied, but we still need to do a lot more work to understand how those systems are working. Are they missing data? Do they produce false negatives? There is a whole lot of science that needs to go behind that. Again, it is a problem within digital forensics and forensic science that we do not have that co-ordinated research and development, so you can have one force applying something and one force saying, “I am not going to do it”, a private company applying something and another one not. It is very disorganised and not done together in terms of that validation and testing and ensuring that that software is giving us the right answer.”^{lxxiv}

2.52 The purpose of this section is to highlight the volume of data that can be obtained using extraction technologies. **We emphasise that this necessitates the need for a new legislative approach and a closer look at cybercrime hubs and the safeguards in place, with a focus on machine learning and cloud analytics.**

3. HOW THE CYBER KIOSKS WORK

- 3.1 We briefly look at how cyber kiosks are to work in Scotland in order to highlight some gaps and concerns.
- 3.2 Mobile phone extraction involves the collection [and in the case of cybercrime hubs the retention] of vast quantities of communications data and content data, including personal and sensitive personal data (special category data) of both the user and many others with whom the user interacts.
- 3.3 In the Justice Sub-Committee report^{lxv} it is stated that cyber kiosks:

“are software systems, which look like small laptops, and are designed to image or extract electronic data held on a variety of digital devices, such as mobile phones, tablet/surface devices etc. This allows that data to be analysed by a third party, such as the police.”

“Digital devices like mobile phones normally have security features, such as passwords and data encryption, to prevent anyone other than the owner of the device from accessing the data stored on it. **Cyber kiosks enable the police service to bypass passwords, overcome locks and encryption security to access the data held on a mobile device.** This data can be wide-ranging, such as biometric data, and data stored externally from the device, such as information held on cloud-based server accounts”

(emphasis added)

- 3.4 The cyber kiosks are all provided by Cellebrite. The Justice Sub-Committee report notes that:

“The Cellebrite cyber kiosk is a desktop personal computer which can take an image of all of the data on a mobile device, and can also extract and store data. It enables search parameters to be inserted to search the data on the device. The cyber kiosks are not able to change or delete any data held on a mobile device.”

- 3.5 In the Data Protection Impact Assessment (version 0.14) Police Scotland state that:

“The project concerns the introduction of 41 Digital Triage Devices (DTD) – ‘Cyber Kiosks’ spread across Police Scotland Estate as part of Police Scotland’s commitment to its Policing 2026: Serving a Changing Scotland programme of work...

A DTD/Cyber Kiosk is a computer terminal that can view data on a device in a targeted and focused way i.e. only looking at what is necessary. The only devices that may be subject of Triage using a kiosk is a mobile phone or tablet. If unsure as to whether a device holds information relevant to an investigation it may undergo a triage process using a Cyber Kiosk. This process is only performed by trained staff, the purpose of which is to identify if the mobile

phone or device contains any evidential data using, where appropriate, selected parameters. Selected parameters refer to the areas of the device within which the kiosk has detected the existence of data available to view and to which filters are applied such as Text Messages, Call Data, Chat (WhatsApp / Snap chat), Multimedia (Audio, Video, Photographs), Internet history, Email, etc – This also includes the ability to limit the search using a date range or keyword search criteria. If no potential evidence is found it will be returned to the owner. The Kiosk only provides a viewing facility. It does not record any data from the mobile phone / device.

Seized / submitted mobile devices will include those of victims, witnesses, suspects or accused persons including those obtained voluntarily, under common law powers, the authority of a judicial warrant or statutory power including search. All such devices are treated as productions by Police Scotland and are handled in accordance with the Productions SOP and subject to associated retention Policies.”

“It will only be used in cases where the evidential relevance of the device is unknown. If it is known that the device contains potential evidence that device will be submitted without triage within existing processes.

No device data is retained by the kiosk machine. **The equipment has the capacity to copy data however this facility is disabled and cannot be enabled by standard operators. It is possible that Police Scotland may review use of the extraction functions in future** however there is no intention to do so at this time. Any change in the functionality of the device to be anything other than ‘view only’ will require a resubmission of new associated DPIA / EqHRIA.”

“Contemporaneous notes may be taken by officers...for use in association with the investigation in question for example if during triage of a suspect's phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview...”

- 3.6 In the Data Protection Impact Assessment provided with supplementary written submissions from Police Scotland on 14 November 2018^{lxxvi} (version 0.12) it was stated that personal data to be processed includes: name, identification numbers, location data, online identifiers and factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- 3.7 Police Scotland have proposed procedures whereby devices seized or provided in relation to certain high priority cases or specialised alleged crimes, such as child abuse, will not involve the cyber kiosks but will go direct to cybercrime hubs for full examination. Otherwise, the officer in charge of the case will be required to prepare a submission form of search criteria specifying what names, numbers, identifiers or other data types are to be searched for by the kiosk.
- 3.8 In the Sub-Committee hearing of 10 May 2018^{lxxvii} Detective Superintendent Burnett stated:

“Perhaps it would help if I explained how we propose in our policy, practice and procedure to use the cyber kiosks...

If a digital device is seized for a lawful policing purpose and we are trying to identify whether there is data on it that could expedite or support the inquiry that is under way, that device will be inserted in the cyberkiosk by one of our specially trained officers. Thereafter, we can put in parameters for our search. For instance, if we were looking specifically for text messages to support a domestic abuse inquiry, we would be able to put in specific search parameters to identify whether the device held such information. If that was the case, we would confirm that the device contained information that would support the inquiry, then send it to one of our Police Scotland cybercrime hubs for full digital forensic analysis.”

[I take it from what you said that data that is extracted from a device that has been seized and analysed on the kiosk, for the purpose of triage, never leaves that kiosk.]

“No – and the data does not remain on the kiosk. When we insert the device, we have a view of any data that is held on the device. We then identify whether the device contains anything that is pertinent to the investigation that is under way, and if it does, the next stage is to submit the device for full digital forensic analysis. If it does not, the device will be returned in due course to its owner. However, at the end of an examination on the cyberkiosk, that examination is closed down. Any data that was viewed through the window of the kiosk will not remain on the kiosk device, but a clear audit trail will remain. There will be a unique reference number, so that we will have a form of audit and governance that understands when activity has taken place, but does not retain data that was viewed on the device.”

- 3.9 According to Open Rights Group, Police Scotland envisage that devices which go to the kiosks will be examined semi-automatically, based on submitted search criteria. It is not required or anticipated that the human operator will examine the device, as opposed to entering the search criteria. If relevant hits are found, the consequences are that a record of the search is prepared, and the device forwarded to a cybercrime hub for further examination. If not, the requesting officer and if need be by COPFS will be notified that no relevant data was found.^{lxxviii}
- 3.10 Assistant Chief Constable Johnson, in evidence to the Sub-Committee on 9 May 2019^{lxxix} stated that when mobile phones are examined at cyber kiosks the SIM card will be removed and the data that is held on the handset is examined. He stated that SIM cards would not be examined as part of the current process.
- 3.11 However, further to email correspondence with Police Scotland, they have clarified that the SIM card will be removed at the point of seizure. Thereafter at the kiosk both the device and SIM card will be examined separately. It is not understood why it was previously said that the SIM card would not be examined and later that it would. Removing the SIM card means that the device is off-line. However, the SIM card is likely to hold some personal data including contacts and SMS.

3.12 Detective Chief Superintendent McLean informed the committee that:

“On my esteemed colleague’s point about a filing cabinet or storage, as a point of accuracy, when a kiosk examines a device, **that device will be switched off**. If it has a **SIM card, it will be removed**. It will only be stored data, which brings it very much in line with the case law that looked at stored data on devices and found that the police acted correctly when using those powers to search devices.”

“What happens is that the mobile device in question – let us call it a phone – is switched off and the SIM card removed, which means that it does not connect to any external source of information through a network, wi-fi or the internet. The cyber kiosk then provides some search parameters that allow us to ask a series of questions about the data that is stored on the device, be it a phone or whatever.”

3.13 Counsel’s opinion obtained by Police Scotland states:

[5] As I understand it, the machines are configured, so that it is only the stored contents that can be examined and, to this end, the examination is conducted “off-line” with the sim-card removed from the device. The examination is, where possible, restricted to certain parameters, such as timescales, or by entering search terms such as the names of individuals or other keywords. This should minimise the scope for “collateral intrusion”. Once viewed the data is not retained or downloaded as “...the kiosk are unable to copy and store device data.” An audit trail is automatically generated showing the details of the examiner and the time of examination.

3.14 It is incorrect as stated by Detective Chief Superintendent McLean that the device will be switched off. It is accurate to state that it will be ‘off-line’ in the sense that the SIM-card will be removed. Police Scotland have since confirmed this.

3.15 Whilst we appreciate that Police Scotland have provided evidence at a number of hearings and in writing on the cyber kiosks, having reviewed the submissions we believe there are **certain aspects relating to the operation of the cyber kiosks which justify clarification**.

3.16 It is noted that whilst Police Scotland have repeatedly stated that any data viewed on the cyber kiosk will be deleted and not retained, DS Burnett stated on 10 May 2018^{lxxx} that:

“...another option is available to trained officers. If, while viewing the data on the kiosk, there is an opportunity to download data that is of consequence on to a disk, they can do so. We are looking at how we will manage that.”

“Although downloading data on to a disk is an option, we are looking at the solutions for how those disks can be encrypted. We have yet to be fully satisfied that that will be a workable option, but it is under consideration.”

3.17 At the Sub-Committee hearing on 13 September 2018^{lxxxix} DCS McLean stated:

“In my view we are less focused on the equipment itself, the substantive point being that the equipment does not extract or store data.”

3.18 Fulton MacGregor MSP questioned Police Scotland regarding the statement that downloading data from devices on to disc might be an option. He asked whether it was still being considered. DCS McLean responded that the technology can export data but they have taken the decision not to export any data on to disc. “The position is that the devices will not extract data, store data or export data on to disc or any other format.” He did not completely discount the possibility, stating^{lxxxix}:

“As soon as we export data, we need to consider a range of audit and compliance issues. As part of the ongoing review, we will see whether there is an evidence base but, in the absence of that, we are not going to put that process in place at this time.”

3.19 It would be important to clarify: **(1) whether the Cellebrite devices to be used in the cyber kiosks have the capability to extract and store data; (2) whether there is any future intention that data can be downloaded at the kiosk as has been indicated, and (3) if this is the case, what procedure the police intend to adopt in relation to impact assessments, public and parliamentary consultation.**

3.20 DS Burnett further stated during the same hearing that:

“On the point that Mr Johnson made, because of the huge amount of data on a phone, the search parameters are there to make sure that, if we are looking for a text within a specific timeframe, we can do so. **Can I guarantee that that will be done on every occasion? No, because the data that would potentially be pertinent to an inquiry depends on what is under investigation.**”

(emphasis added)

3.21 In DPIA version 0.14 it states:

“Whilst an examination will only be undertaken in association with the investigation of an incident/crime/event, for a policing purpose and within existing legal frameworks it is possible that much of the data on a device may not be relevant to the investigation, but **some of this may be assessed during triage** and if irrelevant will be disregarded.

3.22 It is noted that in version 0.12 and 0.14 of the DPIA it states that:

“The data will be accessed but not extracted from the device.
Process types will potentially include –
Retrieving / Consulting

Using – as Evidence or intelligence

Disclosing or otherwise making available – for example by including identified relevant evidential data as evidence thereafter submitted to Crown as part of a case, or using that data during an interview of a suspect.”

- 3.23 It is not clear what it means to use ‘evidence’ or ‘intelligence’. Clarification is sought. Despite emphasis on the use of search parameters, it is clear, as shown by the citations above, that this will not always be the case. In addition, it is admitted that irrelevant data may be assessed at the triage phase. **We believe that it is imperative independent audit exists in order to ensure this technology is not used for fishing expeditions.**
- 3.24 **The use of cyber kiosks for reasons other than prevention, investigation or detection of crime or prosecution of offenders has not been fully explored.** There is a secondary law enforcement purpose as set out in the DPIA version 0.14 at Q27. But this only provides examples rather than an exhaustive list of what non-criminal purposes for which they can be used.

4. HUBS : THE WIDER PICTURE

- 4.1 Police Scotland state (7 September 2018 written submissions^{lxxxiii}) that kiosks are used as a ‘triage’ to identify devices that are of evidential value. If as a consequence of the kiosk triage items of evidential value are identified, then progression would be made for that device to be submitted to one of the Police Scotland Digital Forensic Hubs for detailed examination.
- 4.2 The extraction of data is inextricably linked to the use of the kiosks. Yet all the work done by the Reference Group / Sub-Committee has focused exclusively on the kiosks. This is artificial and means, as has been pointed out by Open Rights Group^{lxxxiv} (November 2018) that work has only scrutinised laws and policies that underpin the kiosks, arguably missing the bigger picture. If there are concerns about the legal basis for the use of cyber kiosks this is even more so for cyber crime hubs.
- 4.3 Open Rights Group, in their report, has argued for a holistic model that encompasses the seizure, examination and extraction of data from a digital device. We agree that without taking a view of the whole system, Police Scotland face continued questions being raised regarding the suitability of their digital forensics regime:

“The kiosks may bring benefits in terms of reducing backlogs, particularly if underpinned by a proper legal framework but if that framework fails to apply to the operation of the Cybercrime Hubs then it would undo all of that worthwhile work.”^{lxxxv}

- 4.4 We support Open Rights Group’s call for a full assessment of Scotland’s digital forensic legal framework and support a holistic approach incorporating all stages of device seizure, examination and extraction of data.^{lxxxvi}
- 4.5 We note that the Sub-Committee has questioned Police Scotland regarding the cyber crime hubs and in their Report asked Police Scotland to provide the following specific information on the cyber hubs^{lxxxvii}:

In response to this request the Sub-Committee asked Police Scotland to provide the following specific information on the cyber hubs:

- Copies of the formal proposal by Police Scotland to create the initial 3 cyber hubs, and then to extend the number to 5, the date/s that these proposals were considered and approved by the Scottish Police Authority Committees / Board.
- The location of the initial 3 hubs, and then the additional 2 cyber hubs.
- Details of the equipment to be included in the hubs, the rationale for their use, and the date/s when these proposals were considered and approved by the Scottish Police Authority Committees / Board. Also, details of any contracts published following these decisions.

- Details of the process and engagement undertaken by Police Scotland to ensure that the hubs were using processes and equipment that were legal and satisfied human rights, privacy, data protection and security requirements, including copies of any equalities impact assessments, and data protection impact assessments made at the time of approval etc.
- Details of any equipment used in the hubs that can capture, access or download data from mobile devices.
- Details of how the processes undertaken in the cyber hubs differs from practice prior to the establishment of Police Scotland to capture, access or download data from mobile devices.
- Details of Police Scotland's consideration of informed consent from those whose phones etc. are to be sent to the hub, in particular, witnesses.

4.4 Regrettably, as the Report^{lxxxviii} states:

In its response, Police Scotland provided some of the background information requested, but was unwilling to provide details of the equipment used in the hubs, citing that providing this information may provide criminals with an unnecessary advantage in evading law enforcement, what they were used for, how the practices differed from the procedures of the legacy forces, or the impact assessments and informed consent considerations.

The Sub-Committee is therefore unable to make any informed assessment of the work carried out in Police Scotland's digital forensic hubs.

Similar legal concerns regarding Police Scotland's digital forensic hubs were raised in evidence. This issue was not part of the remit of the Sub-Committee's inquiry but would merit consideration by the Cabinet Secretary for Justice.

4.5 We note that not only does the failure to examine hubs mean that examination and extraction of data at the hubs is not considered. There also has been no consideration of the use of the analytical software offered by Cellebrite (and other companies with similar products).

4.6 We believe Police Scotland must respond to the questions of the Sub-Committee. We recommend clarification on the use of tools such as cloud analytics and AI/Machine learning.

5. SECURITY AND DIGITAL FORENSICS

- 5.1 An additional area deserving of further analysis relates to security, digital forensics and related to this, the risk of miscarriages of justice from poor quality or inaccurate evidence.

SECURITY AND DATA BREACHES

- 5.2 With threats to information security worsening each year, the problems and risks associated with obtaining vast amounts of highly personal data are complex. This concern is perhaps more pertinent to the 'hubs', which makes it regrettable that this aspect of the debate has not received as much discussion and consideration.
- 5.3 Police in the UK are no strangers to appalling data breaches^{lxxxix} and malware attacks^{xc}. The data extracted by cyber kiosks and retained by Hubs is deeply personal and valuable in the wrong hands. Phones can contain legally privileged information, sensitive commercial information and hold the digital keys we use for banking as well as intimate details about our lives. As stated by the National Cyber Security Centre ("NCSC") "bulk data stores make very tempting targets for attackers of all kinds. So, it is essential to ensure they're adequately protected."^{xcii}
- 5.4 In a previous investigation^{xcii}, the Police and Crime Commissioner for North Yorkshire found that:
- In half of cases sampled there was a failure to receive authorisation for the use of mobile phone extraction tools;
 - Poor training resulted in practices which undermined prosecution of serious crime offences such as murder and sexual offences;
 - There are inadequate data security practices including the failure to encrypt and files which may contain intimate details of people never charged with a crime are lost.

TRAINING AND DIGITAL FORENSICS

- 5.5 Whilst the Sub-Committee has received evidence from Police Scotland regarding training and knowledge, there does not appear to have been much information regarding what that training will constitute, nor consideration of the risks of police officers utilising forensic extraction technologies.

“AN EXAMINER MUST NOT ONLY KNOW HOW TO USE FORENSIC TOOLS, BUT MUST ALSO UNDERSTAND THE METHODS AND ACQUISITION TECHNIQUES DEPLOYED BY THE TOOLS THEY USE IN THEIR INVESTIGATIONS. FORENSIC TOOLS NOT ONLY SAVE TIME, BUT ALSO MAKE THE PROCESS A LOT EASIER. HOWEVER, EACH TOOL HAS ITS FLAWS, AND THE EXAMINER MUST CATCH ANY MISTAKES AND KNOW HOW TO CORRECT THEM BY LEVERAGING ANOTHER TOOL OR TECHNIQUE.”^{xciii}

- 5.6 We would encourage the Sub-Committee and External Reference Group to take note of proceedings and the report from the UK Parliament House of Lord Science and Technology committee investigation into forensic science. Although focussed on England and Wales its findings are also pertinent to Scotland. In evidence to the committee, Dr Jan Collie, Managing Director and Senior Forensics Investigator at Discovery Forensics highlighted the lack of forensic skill by those using MPE technology:

“What I am seeing in the field is that regular police officers are trying to be digital forensic analysts because they are being given these rather whizzy magic tools that do everything, and a regular police officer, as good as he may be, is not a digital forensic analyst. They are pushing some buttons, getting some output and, quite frequently, it is being looked over by the officer in charge of the case, who has no more training in this, and probably less, than him. They will jump to conclusions about what that means because they are being pressured to do so, and they do not have the resources or the training to be able to make the right inferences from those results. That is going smack in front of the court.”^{xciv}

- 5.7 Dr Gillian Tully, UK Forensic Science Regulator commented that:

“There is a lot of digital evidence being analysed by the police at varying levels of quality. I have reports coming in in a fairly ad hoc manner about front-line officers not feeling properly trained or equipped to use the kiosk technology that they are having supplied to them.”

- 5.8 Ignorance of the functioning of these tools is dangerous to the proper functioning of the criminal justice system. The technology is far outpacing safeguards and technical standards. As highlighted in a recent update from Magnet Forensics, updates can permit tools to do far more than is understood and legally permissible:

“When we introduced Magnet.AI, it ran automatically when you opened your case in AXIOM Examine... this could be a problem in some cases: if it revealed evidence that was outside the scope of your warrant ... risk the admissibility of all the evidence on the device.”^{xcv}

- 5.9 Lee Reiber, author of *Mobile Forensic Investigations*, emphasises in his book the need for an innate understanding of the data for successful examination of digital evidence from a mobile device:

.....
“IT IS WIDELY KNOWN THAT TODAY’S DIGITAL FORENSICS EXAMINATIONS HAVE BEEN DUMBED DOWN, WITH A HEAVY RELIANCE PLACED ON USING TOOLS TO EXTRACT AND COLLECT DATA. THESE METHODS HAVE BRED AN INFLUX OF “DATA COLLECTORS” RATHER THAN MOBILE DEVICE FORENSIC EXAMINERS.”^{xcvi}
.....

- 5.10 Evidence to the UK Parliament Science and Technology Committee reveals there is no testing of devices purchased by law enforcement unlike other forensics tools. Dr Gillian Tully, Forensic Science Regulator stated^{xcvii}:

“As yet, those [mobile phone extraction tools] have not all been properly tested...”

Dr Jan Collie, Managing Director and Senior Forensic Investigator, Discovery Forensics, commented that:

“Most of the forensic tools we use are tested to within an inch of their lives by the companies who produce those tools. We are not allowed to reverse engineer them [mobile phone extraction tools] because that would be illegal anyway.”

- 5.11 Academic and forensics practitioner Angus M. Marshall, Director and Principal Scientist, n-gate Ltd, commented that:

“...the commercial tool providers unwillingness to disclose information about their own development and testing methods means that the evidence base for the correctness of many digital methods is extremely weak or non-existent.”^{xcviii}

- 5.12 Angus Marshall and Richard Page state (2018:4)^{xcix}:

“In the world of digital forensics, we tend to rely on third-party tools which we trust have been produced in accordance with good engineering practices. For the most common analytical tools, this is software which we trust has been correctly specified, implemented and tested. However, the responses to our questions about development models suggest that there is some disconnect between the tool producers and the way end-users are expected to provide evidence of fitness for purpose.

...

In the forensic context...examinations start with a source of potential evidence whose contents are unknown. Thus, the inputs to the whole forensic process are unknown. Although the user may have some experience of what abnormal outputs look like, this depends entirely on the tool actually producing abnormal outputs or indications of errors. It is entirely possible for a tool to process inputs incorrectly and produce something which still appears to be consistent with correct operation. In the absence of objective verification evidence, assessment of the correctness, or otherwise, of any results produced by a tool relies solely on the experience of the operator.

...

It should also be borne in mind that updates to hardware and software may have no apparent effect on system behaviour as far as a typical user is concerned, but may dramatically change the way in which internal processing is carried out and data is stored.”

AUDIT

- 5.13 Police Scotland stated in its September 2018 written submissions that the Kiosk retains transaction information which includes details of date, time and log in details^c.
- 5.14 In the Data Protection Impact Assessment version 0.12 it states that "Once the triage is complete only management information such as operator, data, reference number, start time, end time etc is retained can be viewed and will be subject of audit and assurance processes." We query whether this is sufficient information to identify any abuse, misuse or discriminatory application of the cyber kiosk.
- 5.15 We note the comments of David Lammy, MP for Tottenham and author of the 2017 Lammy Review into the treatment of, and outcomes for Black, Asian and Minority Ethnic individuals in the criminal justice system, in response to Privacy International's report on MPE:

.....

"The lack of transparency around new policing tools such as mobile phone extraction is a serious cause for concern. There are no records, no statistics, no safeguards, no oversight and no clear statement of the rights that citizens have if their mobile phone is confiscated and searched by the police.

My Review of our criminal justice system found that individuals from ethnic minority backgrounds still face bias in parts of our justice system, and it is only because we have transparency and data collection for everything from stop and search incidents to crown court sentencing decisions that these disparities are revealed and we are able to hold those in power to account. Without the collection and audit of data about the use of mobile phone extraction powers scrutiny will be impossible.

Given the sensitive nature and wealth of information stored on our mobile phones there is significant risk of abuse and for conscious or unconscious bias to become a factor without independent scrutiny and in the absence of effective legal safeguards.

We entrust so much personal information to our phones that the police having the power to download every message and photo we have sent or received without any rights and protections is another worrying example of regulations not keeping up with advances in technology."

5.16 In written submissions on 7 September 2018^{ci}, Police Scotland stated that they were in liaison with Audit and Assurance to consider publication of relevant information pertaining to kiosk activity on at least an annual basis.

5.17 In their letter dated 2 September 2019^{cii}, Police Scotland stated that the scope of the Post Implementation Review which will take place approximately six months following roll out, will assess:

- Engagement and consultation
- Training
- Implementation process
- Benefits: Benefits Forecast, Benefits Realised, Benefits Yet to be Realised
- Lessons Learned: Determine if there is any lessons that can be learned from the experience of the Force during Digital Triage Device delivery and implementation.

5.18 We do not believe that Police Scotland have provided sufficient detail regarding the Post Implementation Review, we believe that the review should consider a number of our recommendations that apply to Police Scotland and we believe that there is an absence of statistics which would enable effective scrutiny of the use of Digital Triage Devices.

DEVICE SECURITY

5.19 The Police Scotland Data Protection Impact Assessment version 0.12 states “Only the Police Scotland officers viewing the kiosks at the time can view the data. The manufacturer cannot access the kiosk or data.” Police Scotland have also stated that the devices are not yet networked. **Should these devices be networked, security must be a factor to consider.**

5.20 We note that companies can have remote access to the software. This is not only for product updates but analytics:

“When you use our Products such as the UFED Cloud Analyzer, then subject to your separate and explicit consent, we will collect information about how you use the Product under the license Cellebrite gives you, such as the number of extractions you perform with the software, which types of data source you extract, any errors you came across using the Product, the number of events you collect, how often you use the Web Crawler and which views you use ... All of the above data is referred to as Analytical information.” ^{ciii}

5.21 Given the Justice Sub-Committee have not had the opportunity to fully consider these issues, we set out a number of recommendations in relation to security and forensics issues:

1. **Cybersecurity standards should be agreed and circulated, specifying how data must be stored, when it must be deleted, and who can access.**
2. **All authorities who use these powers must purchase relevant tools through procurement channels in the public domain and regularly update a register of what tools they have purchased, including details on what tools they have, the commercial manufacturer, and expenditure amounts.**
3. **Technical standards must be created and followed to ensure there is a particular way of obtaining data that is repeatable and reproducible, to ensure verification and validation. This should be accompanied, for example, by a clearly documented process.**
4. **Technical skill is required as with this unprecedented amount of electronic evidence comes the need for highly skilled mobile forensic investigators (Reiber 2019:2).**

6. LEGALITY

- 6.1 The legal basis for mobile phone extraction and use of cyber kiosks has been examined in detail during the Sub-Committee's inquiry. However, given Police Scotland believe they have lawful basis to use cyber kiosks, we look at legality to highlight concerns.
- 6.2 The use of MPE is highly intrusive of the rights to privacy, home and correspondence and of data protection rights; it is arguably the most intrusive form of technology used by the police. It engages not only the privacy and data protection rights of the user of a phone but also those of many other people who have communicated with the user.
- 6.3 While the character of the information contained on individuals' mobile phones varies greatly, there is little doubt that many if not all mobile phones will include:
- (1) Personal data (of both the owner/user and many others), including special categories data within the meaning of Article 9 of the General Data Protection Regulation (such data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or as to an individual's sex life or sexual orientation) and confidential data or "sensitive" personal data within the meaning of section 35(8) of the Data Protection Act 2018);
 - (2) Private information and correspondence within the meaning of Article 8 of the Convention; and
 - (3) Information in respect of which the user enjoys a reasonable expectation of confidence.
- 6.4 The use of cyber kiosks and hubs engages both data protection and human rights legislation. Data protection and privacy are intrinsically linked, and Data Protection laws are one mechanism to protect privacy rights.
- 6.5 We agree with Open Rights Group that a full and proper legal framework is required for both use of cyber kiosks and the cybercrime hubs.

"The kiosks may bring benefits in terms of reducing backlogs. The means by which devices are sent for kiosk review must be underpinned by a full and proper legal framework, well beyond the present state of the assessments. If the full framework does not also apply to the operation of the cybercrime hubs, then the validity of material applying only to kiosks is undermined."^{civ}

- 6.6 This could go further. The Information Commissioner's Office wrote to John Finnie MSP on 10 June 2019^{civ} that:

"We would welcome a commitment from the Scottish Government to make the necessary arrangements for ensuring that digital forensic investigations are conducted "in accordance with the law", be that through a code as Counsel indicates or other measure. This would ideally be based on clear principles which can keep pace with technological advancements..."

We also believe that the Government should make arrangements for a wider review of the legislative framework for criminal justice in the digital age. This could underpin the use of other digital tools by law enforcement bodies such as automated facial recognition technology, which is also currently subject to a legal challenge.”

- 6.7 **We support this submission and whether for example a legislative framework could be tied to wider concerns around police use of new technology such as facial recognition, IMSI-catchers and social media surveillance.**
- 6.8 We support the views held by authoritative groups including the Scottish Human Rights Commissioner, UK Information Commissioner’s Office and Scottish Criminal Bar Association, who are critical of the current legal basis put forward by Police Scotland. **Until a clear legal basis is provided, and the use of cyber kiosks and cybercrime hub is subject to appropriate safeguards and oversight, the roll out of the programme should not proceed.**
- 6.9 The Justice Sub-Committee stated in their report^{cv} that:

“143. The Sub-Committee is still not reassured that the legal framework being relied upon by Police Scotland for the use of cyber kiosks is suitably robust or provides the necessary safeguards for members of the public. Any process must be mindful to protect the integrity and robustness of the investigation and prosecution service.

144. The Sub-Committee recognises the importance of public confidence in policing and policing by consent. There is, therefore, an urgent need for clarity and public reassurance before this new technology can be introduced.

147. The Sub-Committee asks the Scottish Police Authority to consider introducing a code of conduct for use of the cyber kiosks and recommends that any such code should include a risk assessment of collateral intrusion and details of how to mitigate that risk.

150. The Sub-Committee do not believe that the cyber kiosks should be deployed by Police Scotland until clarity on the legal framework is established.”
(emphasis added)

- 6.10 We note the written submissions of the Scottish Human Rights Commission^{cvi}:

“a. **The Scottish Parliament should consider the enactment of legislation (i.e. a code of conduct for digital forensics).** This would satisfy the Article 8 requirements for all possible cases where Police Scotland will be using this technique. In doing so the Scottish parliament would ensure clarity of the law and the incorporation of adequate and effective guarantees against abuse and arbitrary interference, which are “necessary in a democratic society”. Regulation would also consider the appropriate threshold allowing seizure of the e-device.

b. **There should be a judicial warrant requirement for any search of mobile phone** (and digital media), unless it is explicitly and clearly defined by other law. This will provide the required legal precision and necessary oversight under human rights law when a measure is highly intrusive of a fundamental right. As general rule and subject to the exceptions, Police Scotland will require a judicial warrant to enter and search property. In view of the recognition that MPB is capable of being at least as intrusive of Article 8 rights as searches of homes, the rationale for requiring warrants for searches of premises apply equally to mobile device examination.”

(emphasis added)

- 6.11 On the basis that the search of a mobile phone will reveal more than a search of an individual’s home and person, **Privacy International believe that in order to extract data, a warrant must be obtained.** Whilst the use of parameters has been discussed when using cyber kiosks, we note that that may not always be the case and it is unclear how limited or indeed how broad a search of a phone using cyber kiosks could go. We note that as cited above, at the 13 September 2018 hearing DS Burnett stated that:

“On the point that Mr Johnson made, because of the huge amount of data on a phone, the search parameters are there to make sure that, if we are looking for a text within a specific timeframe, we can do so. **Can I guarantee that that will be done on every occasion? No, because the data that would potentially be pertinent to an inquiry depends on what is under investigation.**”

[emphasis added]

- 6.12 In some cases, mobile phones may also contain material that is legally privileged, confidential journalistic material and material likely to identify journalistic sources.
- 6.13 We note the Information Commissioner’s Office submissions^{cviii} (notably made following review of the legal advice from Senior Counsel to the Chief Constable), that:

“We understand that the examination of digital devices is often a necessary intrusion for suspects, victims or third parties in order to conduct relevant investigative lines of enquiry and can be a justified interference with right to privacy under Article 8 of the European Convention on Human Rights. As such the ‘in accordance with the law’ requirement must be sufficiently circumscribed and provide adequate safeguards against abuse.

We question whether common law powers, or any other existing provisions, are sufficient to give members of the public an adequate indication of when and how their data will be processed by the police, and satisfy the ‘in accordance with the law’ requirement under Article 8 of the ECHR.”

(emphasis added)

- 6.14 The written submissions of the Scottish Human Rights Commission^{cix} dated 7 June 2019 following review of legal opinion provided by Police Scotland state:

“We have considered both the response to the letter of the Justice Minister on digital device triage systems (cyber kiosks) and the Legal Opinion provided by Police Scotland. **The Commission is still not satisfied that the use of this technology by Police Scotland complies with the requirements of Article 8 of the European Convention on Human Rights. This is because the law surrounding the use of cyber kiosks lacks sufficient quality to be accessible and foreseeable.** In addition, there are no adequate safeguards in place as the legislature (when enacted) did not consider situations of seizure and search in this particular contest. Therefore, the current framework or lack of it does not provide sufficient and robust safeguards for people’s privacy rights in this context.”

“Our view remains that way forward is the enactment of legislation in relation to all digital forensics and statutory guidance (e.g. a code of practice) covering the browsing and extraction of data from digital devices that integrate Article 8 requirements. We also favour the requirement of a judicial warrant for any search of mobile phones (and digital media), unless it is explicitly and clearly defined by law.”

(emphasis added)

POLICE SCOTLAND'S POSITION ON LAWFULNESS

- 6.15 Our understanding of Police Scotland's position is that under common law they are entitled to seize anything it is reasonably believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even though, in their words, the statute contravened makes no provision for seizure.
- 6.16 In correspondence with Police Scotland, the Crown Office Procurator Fiscal Service broadly categorised the legal basis^{cx} relied upon by Police Scotland, to allow Police Officers to seize an item as:
- Where an individual has been arrested
 - Where there is a statutory power of search of an individual or their property without the need for a search warrant
 - Where a search warrant has been granted either under legislative powers or the common law
 - Where the owner has given consent
 - Where there is common law power
 - Where there is urgency.
- 6.17 On 10 May 2018 at the Sub-Committee^{cx} the following exchange took place:

The Convener: Under what authority can you take possession of a phone, interrogate it and retain its data? Who has access to that data? How would it be disposed of?

Detective Superintendent Burnett: On the first point, there are, in general terms, four legal frameworks – for want of a better phrase – under which we could bring a device into lawful custody. That, of course, would be required to be for a policing purpose. There are powers under common law...

The Convener: Are you saying that anyone who is arrested under common law could have their phone taken into possession?

Detective Superintendent Burnett: Yes, or –

The Convener: Would that include for breach of the peace?

Detective Superintendent Burnett: Police could seize a person's mobile phone or other device if the person is under arrest...We also have powers that exist under warrant. We could be provided with a warrant under the Misuse of Drugs Act 1971, for example, that would give us the relevant powers. The third element is statutory powers... The fourth element is when, for example, a victim of crime ... provides their device voluntarily for examination and there might be information that is pertinent to the inquiry on that phone.

(emphasis added)

RELIANCE ON JL & EI V HMA AND HMA V ROLLO

6.18 Police Scotland set out in written submissions dated 12 November 2018^{cxii} that:

“Where a lawful power of search exists that power of search enables a police officer to search for an item, seize it, and examine it. That is the position as set out in the case of J.L. & E.I -v- HMA. In that case the court observed that no speciality is introduced simply because what is found is an electronic device such as the electronic memo-master discussed in HMA v Rollo. HMA v Rollo explored the admissibility of evidence contained in a password protected electronic device. This articulated that the ‘means or surface’ for recording information did not deprive such stores of information from qualifying as a document which could be subject to examination. The J.L. and E.I. -v- HMA case concerned the examination of an iPhone and, more particularly, information contained within the phone in digital format (namely text messages) and that was deemed to be lawful.”

6.19 Privacy International have previously argued to the Sub-Committee^{cxiii} that, we do not believe that the cases cited are sufficiently analogous, nor do they give full consideration to the matter in question both in terms of the technology and that our devices are becoming ever more personal and pervasive in our lives with more and more data.

6.20 We note the response of the Scottish Criminal Bar Association to the Sub-Committee^{cxiv} which stated that:

“As per Assistant Chief Constable Steve Johnson’s letter to Andrew Laing of COPFS dated 15 October 2018, Police Scotland appears to found much of its purported legal authority or its ‘...understanding of the existing legal framework...’ for the use of these devices on the basis of the decisions in Rollo v HMA 1996 JC 23 and JL & EI v HMA 2014 JC 199.

In this connection, the SCBA would observe that:-

(i) That Rollo was a decision dealing particularly and discretely with the issue as to whether an electronic notepad or diary fell within the meaning of a ‘document’ for the purpose of a search specifically carried out in terms of s.23(3)(b) of the Misuse of Drugs Act 1971.

It is not readily apparent that the decision in Rollo can be read so as to provide the blanket approval of the use of such devices.

Furthermore, in Rollo, the search clearly proceeded under the authority of a judicial warrant. It is not clear what assistance the decision provides in relation to searches that are not carried out under the auspices of any warrant;

(ii) That JL & EL was a decision dealing particularly with police powers of search in relation to persons detained under the now repealed provisions of s.14 of the Criminal Procedure (Scotland) Act 1995. Those powers of detention and subsequent search only applied where the police had reason to suspect that a person had committed an offence punishable by imprisonment.

This would indicate the engagement of a degree of proportionality in that the offence in question had to be sufficiently serious so as to be punishable by imprisonment before the detention and search provisions under s.14 applied.

Indeed, in JL & EL, the crime in question was an assault to injury and permanent disfigurement - in other words, a serious offence indeed punishable by imprisonment.

By contrast, the replacement detention and search provisions introduced by s.1 of the Criminal Justice (Scotland) Act 2016 can also apply to offences not punishable by imprisonment in terms of s.1(2) and (3) of the 2016 Act.

It cannot therefore be assumed, as Police Scotland appear to assume, that the decision in JL&EL will necessarily apply in relation to different legislative provisions (i.e. s.1 of the Criminal Justice (Scotland) Act 2016) where the same degree of proportionality as obtained in relation to the provisions under consideration in JL & EL (i.e. the provisions of s.14 of the Criminal Procedure (Scotland) Act 1995) does not seem to apply.

6.21 We note the submissions by Open Rights Group on Police Scotland's reliance on *Rollo v. HMA* and *JL & EL v HMA* which further illustrate the inadequacies of reliance on these cases.^{cxv}

LEGAL OPINION OBTAINED BY POLICE SCOTLAND

6.22 Police Scotland received legal advice from Senior Counsel upon which they rely. We note the submissions^{cxvi} of the Information Commissioner's office dated 10 June 2019, which highlight that the focus of the advice was on warrantless searches of arrested persons, despite the ICO consistently asking Police Scotland for a full assessment of the legal position in respect of each category of data subject, including victims, witnesses and third parties. The ICO further stated:

"We question whether common law powers, or any other existing provisions, are sufficient to give members of the public an adequate indication of when and how their data will be processed by the police, and satisfy the 'in accordance with the law' requirement under article 8 of the ECHR."

- 6.23 We are further concerned that as noted^{cxvii} by the Scottish Human Rights Commission in their letter of 7 June 2019 that “both Police Scotland and the Scottish Police Authority recent statements do not fairly represent the advice of counsel”.

“The Legal Opinion is cautious and qualified in relation to the legal basis rather than ‘clear and unambiguous’. This is based on several recommendations within the advice given to strengthen the legal basis and the acknowledgment of a very limited legal analysis of this area of law in Scotland [Para 10]. The legal authority relied upon seems to offer a wide discretion by the police conducting the examination and not directly analogous for comparison. On the contrary, the existing legal analysis in other national and international courts stress the requirement of lawfulness and need of clear procedural safeguards to avoid arbitrary use of power and overuse of discretion.

The Legal Opinion also recognises the merits of developing a legislative framework fit for the digital age and echoes our call for a statutory code of practice to cover the use of this kind of technology as the more appropriate option [Para 32 and 33]. The Legal Opinion points out the need for accessibility and foreseeability of the law and a further detailed consideration of the law to take place for example by the Scottish Law Commission [Para 31].”

- 6.24 Police Scotland’s Legal Opinion states^{cxviii}:

[31]the wider debate arising from this fast-developing area might benefit from further detailed consideration. As discussed above, there are widespread and sincerely held concerns about the investigation of cyber-crime. Reference has been made to the involvement by the Scottish Law Commission....

[32] ...it might be thought better to involve the Government in bringing forward legislation to underpin the use of cyber kiosks and cybercrime hub. The consultation process would inform Parliament and, hopefully, lead to a proper legislative framework fit for the digital age. It is possible that a working group, drawn from across the criminal justice network, could be set up to examine the issue in detail.

[33] ... It seems to me that there might be merit in at least considering a code of practice, underpinned by statute, covering the seizure and examination of ICT devices and any other relevant digital equipment.

POLICE SCOTLAND’S HUMAN RIGHTS IMPACT ASSESSMENT

- 6.25 At the Sub-Committee hearing on 13 September 2018^{cxix} Diego Quiroz (Scottish Human Rights Commission) commented on the human rights impact assessment noting a number of concerns.

“First the document conflates certain legislative protections with human rights protections. Because of the time constraints, I will focus on only one of those. The analysis of article 8 relies heavily on data protection requirements. It reads: “this article will be heavily protected due to the documents compliance with GDPR.” The data protection framework, which is about data processing, is separate from the human rights framework, and compliance with that framework, although necessary, is not sufficient by itself to meet human rights requirements. That is a crucial point, and it requires further analysis by the police. I do not think that only a bit of tweaking or analysis is needed; it requires much more further analysis because the distinction between privacy and data protection is fundamental to understanding how they interact and complement each other.

Privacy concerns arise when personally identifiable information is collected, stored and used – which is not the case here, although it is the case with hubs – and the legal question focuses on whether there is justified or unjustified interference. Data protection is about securing data against unauthorised access – it is a technical question about the conditions that are required to facilitate full and lawful protection of data. We are worried that those two distinct issues are being treated as the same and synonymous in the human rights impact assessment. Data protection is an expression of the right to privacy but does not address the same issue as is addressed under the ECHR.”

POLICE SCOTLAND’S DATA PROTECTION IMPACT ASSESSMENT

- 6.26 As we stated above, we are concerned about Police Scotland’s comparison with briefcases and filing cabinets. In the DPIA version 0.14 Police Scotland sate that:

“The common law of Scotland operates no differently in relation to the seizure of a digital device by a police officer in the course of an investigation to any other item which is reasonably suspected to be evidence in a police investigation or incident.”

“In like terms, the same applies (broadly) when it comes to examination of the ‘contents’ of any such device. In that connection, a digital deice can be regarded as being the electronic equivalent of a brief case or filing cabinet, where the device is protected by some sort of barrier or lock which requires a PIN or password to access its ‘contents’.

Therefore, if a police officer in the execution of a lawful power, seizes a digital device, the law allows for the examination of that device for information held within.”

“It is not possible to foresee what the common law will or will not permit in every circumstance regarding seizure and examination of devices.”

6.27 The Legal Opinion obtained by Police Scotland stated:

[7] The common law power to search, seize and examine following arrest was succinctly summarised in the case of *JL v HM Advocate*.

“A power of “search” of the person comprehends looking for an item (going through pockets, for example: *Bell v Leadbetter* at 1934 J.C., p.77) seizing it and examining it. Accordingly, if a police officer has lawfully arrested a person, that officer may in exercise of the common law power of search following an arrest take possession of the person’s jacket or handbag, look inside the jacket pocket or handbag and, on finding, for example, a diary, examine the entries made in that diary with a view to these entries forming a basis for a further inquiry or being admitted as evidence in future criminal proceedings.”

6.28 As noted above, we believe such a comparison is flawed.

SCOTTISH GOVERNMENT POSITION

6.29 The Cabinet Secretary for Justice has also addressed the Sub-Committee and made written submissions. His position can be summarised, as set out in his letter dated 3 June 2019^{cxix} that:

“It is, of course, for the SPA and Police Scotland to ensure that they exercise their powers in accordance with the law, and that there is a legal basis for any particular use of the technology as it stands. It is of course open to anyone who believes that a particular course of conduct is not lawful to challenge it in the courts. I am not aware of any such challenge; and the Sub-Committee will have noted the opinion given by Murdo Macleod QC...”

6.30 The Cabinet Secretary confirmed at his evidence session 13 June 2019^{cxix} that:

“On the overarching legal framework and the particular issue of digital device triage systems, or cyberkiosks, Police Scotland and the Scottish Police Authority have to satisfy themselves about the legal advice that they have received before proceeding and obviously, from the evidence, they believe that they have the legal basis to proceed.

...

Ultimately, if there is a difference in opinion in relation to the law, it would be up to the courts to make a determination – I am not advocating that approach, but that is the case.

6.31 The Cabinet Secretary, acknowledging the importance of these issues stated:

“Because of my commitment to the legal, ethical and proportionate use of new technologies, which I believe is shared by the sub-committee, I plan to form an independently chaired reference group to scope the possible legal and ethical issues arising from emerging technological developments. The overall aim is to ensure that Police Scotland can continue to have not only the power to keep our communities safe but, crucially, the right safeguards to protect the rights of the individual...at present, simply a policy intention, I am unable to go into much detail...”

It is to be seen if this materialises and whether this will have any impact on the issues raised in relation to cybercrime kiosks and hubs.

INTERNATIONAL JUDICIAL DECISIONS

6.32 We note that police access to mobile phones has received judicial attention at the highest level in both the US and Canada.

6.33 Although the English courts have not thus far been called upon to consider directly mobile phone extraction by the police, in *Beghal v DPP* [2016] AC 88, Lord Hughes JSC stated (at [57]) that:

“[T]he retention of [data obtained from a mobile phone under of Schedule 7 to the Terrorism Act 2000] (see below) is a considerable intrusion into the private life of the subject, particularly given the volume and content of personal material which is kept nowadays on mobile telephones or portable computers.”

6.34 As noted by Diego Quiroz from the Scottish Human Rights Commission:

“The differences are particularly clear when we are talking about electronic devices, which goes back to the point about the Canadian Supreme Court and US Supreme Court cases. They clearly state that searches and examinations of mobile phones should be done within the legal framework of a warrant. In the case of Canada, there are only very narrow circumstances in which those searches can be done without a warrant and it depends on the criminal offence and the immediacy of the circumstances. Certainly, the Canadian Supreme Court is quite clear that minor offences will not allow the use of mobile extraction or browsing without a warrant.”

6.35 In the US Supreme Court’s judgment in the seminal case of *Riley v California* (2014) 134 S.Ct. 2473, which concerned a search of mobile phone incident to an arrest, Chief Justice Roberts provided a detailed analysis of the scope of information contained on mobile phones, which included the following observations:

“...Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person. The term “cell phone” is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. ..Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read – nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant ...”

- 6.36 Yet more powerful observations have emerged from the Canadian Supreme Court. In the case of *R v Morelli* [2010] 1 S.C.R 253 the Court observed (at 2) that:

“It is difficult to imagine a search more intrusive, extensive, or invasive of one’s privacy than the search and seizure of a personal computer.”

There is no doubt that this reasoning applies mutatis mutandis to smart phones.

- 6.37 In the Canadian Supreme Court Case of *R v Fearon* [2014] 3 S.C.R 621 (concerning the manual browsing of a mobile phone by police officers following an arrest), Karakatsanis J, made a number of powerful remarks about mobile phones and the privacy implications of access to them by the police:

“[Mobile phones] generate immense stores of data about our movements and our lives. Ever-improving GPS technology even allows these devices to track the locations of their owners. Private digital devices record not only our core biographical information but our conversations, photos, browsing interests, purchase records, and leisure pursuits. Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. Our digital devices are windows to our inner private lives.” (at [101]).

“The incredible and unique power of modern digital communications devices as portals to vast stores of information – and their ability to expose our private lives – means that they can be even more threatening to our privacy than the search of our homes” [134]. “Particularly for the ‘digital generation’, these devices contain far more information, and information far more personal, than does a private home. These devices provide a window not just into the owner’s most intimate actions and communications, but into his mind, demonstrating private, even uncommunicated, interests, thoughts and feelings” (at [152]).”

COMMUNICATIONS DATA

6.38 Whilst there has been a lack of consideration specifically on mobile phone extraction in the United Kingdom, mobile phones necessarily contain significant amounts of communications data. This is a category of information which has received considerable judicial attention in recent years. In *Digital Rights Ireland v Ireland Minister for Communications, Marine and Natural Resources* [2015] QB 127 (at [27]) the Court of Justice of the European Union (“CJEU”) said the following about communications data^{cxixii}:

“Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.”

6.39 In *Tele2 Sverige Ab v Post -oct telestyrelsen* [2017] QB 771 the CJEU went on to note that such data “provides the means ... of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications” (at [99]). These observations were made in the context of cases about the retention of communications data by service providers and access to such data by the state, but they apply to communications data generally.

6.40 The police would ordinarily obtain communications data through the issuing of notices to communication services providers to provide such data, the direct acquisition of the data or in the context of and incidental to the interception of communications. As set out in the Communications Data, Standard Operating Procedure for Police Scotland^{cxixiii} the Regulation of Investigatory Powers Act 2000 provided a legal basis for the lawful access to communications data by public authorities, including police forces, in Scotland. This has been replaced by the Investigatory Powers Act 2016 which identifies Police Service of Scotland as a ‘relevant public authority’^{cxixiv}. The Regulation of Investigatory Powers (Scotland) Act 2000 remains relevant in Scotland (namely to covert surveillance and equipment interference).

6.41 Following the decision in *R (Watson) v Secretary of State for the Home Department* [2018] 2 WLR 1735 (at [9] and [27]) this framework was subject to amendment to ensure that the police can only acquire communications data from Communication Service Providers where there is a prior review by a court or independent administrative body and, in the content of law enforcement, for the purposes of preventing or detecting serious crime. Amendments were introduced via new regulations, The Data Retention and Acquisition Regulations 2018.

DATA PROTECTION

- 6.42 The Data Protection Act 2018 (“DPA 2018”) which implements the derogations for Member States in the European General Data Protection Regulations (“GDPR”) and transposes the EU Law Enforcement Directive 2016/680 in the UK in Part 3, sets out rights and responsibilities in relation to the processing of personal data for law enforcement purposes. Mobile phone extraction is undoubtedly data processing^{cxv} (which encompasses any operation(s) performed on personal data including collection, recording, storage, adaptation or alteration, retrieval, consultation and use) for the purposes of the DPA 2018. Any further use, storage or deletion of data derived from mobile phone extraction would also amount to processing.
- 6.43 The processing of personal data via cyber kiosks and hubs by Police Scotland is thus governed by Part 3 of the DPA 2018, Such processing must comply with the data protection principles in sections 35 to 40 of the DPA 2018 and Police Scotland as the data controller is responsible for demonstrating compliance with these principles (section 34(3)).
- 6.44 The first data protection principle requires that “the processing of personal data for any of the law enforcement purpose must be lawful and fair.” To be lawful, the processing must be **based on law** and the data subject (i.e. the individual’s whose personal data it is) must have consented or the processing must be necessary for the performance of a task carried out for that purpose by Police Scotland. There are further conditions for “sensitive processing” that is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data or biometric data, for the purpose of uniquely identifying an individual; health data or data concerning sex life or sexual orientation. MPE will certainly amount to “sensitive processing” , thus the first data protection principle further requires either consent and that the controller has “appropriate policy document” or that the processing is strictly necessary for law enforcement purposes and at least one of the conditions in Schedule 8 DPR 2018 e.g. Administration of justice, plus an “appropriate policy document” is in place.
- 6.45 Reliance on consent as a legal basis without an adequate basis in law, is problematic when one takes into consideration the recitals to the Law Enforcement Directive 2016/680 which Part 3 of the DPA 2018 transposes.
- 6.46 Recital 35 provides “The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. **In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679 [GDPR], should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes.** This should not preclude Member States from providing, by law, that the data subject **may agree** to the processing of his or her personal data for the purposes

of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.” *(emphasis added)*

- 6.47 Recital 37, goes on to state in relation to sensitive processing: “Such personal data should not be processed, unless processing is subject to **appropriate safeguards** for the rights and freedoms of the data subject **laid down by law and is allowed in cases authorised by law**; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should **also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.**” *(emphasis added)*
- 6.48 The Article 29 Data Protection Working Party (group of data protection authorities across the EU, which has since been replaced by the European Data Protection Board) adopted in November 2017 an “Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)”, which states:

“**The consent of the data subject can never in itself constitute a legal ground for the processing of special categories of data in the context of the Directive.** This is a major difference in comparison to the GDPR and this difference is stressed explicitly in Recital 35 which considers that Member States may provide by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive

In the light of this, the WP29 concludes that **voluntary agreement should only be considered as an additional safeguard under the law in cases in which processing that is particularly intrusive to him or her are envisaged by law.** Therefore, it is for the national legislator to decide whether and to what extent to allow for data processing under the precondition of the data subject’s voluntary agreement and whether to include special categories of data (see on this Recital 37).

In such cases, the data subject should be informed in a **clear and unambiguous manner by the competent authority about the voluntary nature of his/her agreement and should be given the possibility to withdraw it at any time** (for example, in the case of collection of fingerprints or biological samples).” *(emphasis added)*

- 6.49 It is clear that the circumstances in which consent can be an appropriate legal basis are limited, it is extremely difficult to gain free consent given the clear imbalance of power between individuals and the police and in any event processing must be **based on law**. Hence, why from

a data protection perspective a clear legal framework is a necessity and we question Police Scotland's reliance on consent as the sole legal basis.

- 6.50 Where sensitive processing is carried out without consent and the other safeguards set out in the DPA 2018 (of which we have our doubts as expressed above) the processing must be strictly necessary. The ICO's Guide to Law Enforcement Processing (April 2018, p.7) provides that: "strictly necessary in this context means that the processing has to relate to a pressing social need [which cannot reasonably be achieved] through less intrusive means."^{cxvii} This means that MPE (either by way of a kiosk or a hub) must be the least intrusive means of achieving the law enforcement purpose.
- 6.51 The second principle is that the law enforcement purpose for which personal data is collected must be specified, explicit, legitimate and not processed in incompatible manner with the purpose collected. The third data protection principle requires that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed. The fourth data protection principle is that data is accurate and where necessary kept up to date. This includes an obligation to make a clear distinction between personal data relating to different categories of data subject, such as persons suspected of having committed or being about to commit a criminal offence; persons convicted of a criminal offence; persons who are or may be victims of a criminal offence; and witnesses or other persons with information about offences. The fifth data protection principle requires that data is kept no longer than necessary and there are appropriate time limits for periodic review. The sixth data protection principle requires that personal data be processed in a secure manner. These are all considerations that must be taken into account by Police Scotland and as noted above, Police Scotland must be in a position to demonstrate compliance with each of these principles.
- 6.52 There are a number of other specific obligations, including a requirement to keep logs in relation to the data processing (section 62) and an obligation to carry out Data Protection Impact Assessments, section 64(1) of the DPA 2018 imposes a undertake Data Protection Impact Assessments ("DPIA") "where a type of processing is likely to result in a high risk [having regard to the nature, scope and context of the processing] to the rights and freedoms of individuals". The ICO's Detailed Guidance on DPIA's^{cxviii} provides that the processing of personal data using new technologies, or the novel application of existing technologies automatically requires a DPIA. Police Scotland's DPIAs are an important step forward from the initial trials for which no such assessment was carried out, however, the DPIA still requires further work, in particular given the concerns highlighted in this submission.
- 6.53 Privacy International submitted a complaint to the Information Commissioner's Office in March 2018 that the lack of clarity as to the legal basis for carrying out mobile phone extraction by UK police forces was potential breach of the Data Protection Act 1998 as well as Part 3 of the DPA 2018 when it was still a Bill. This is set out at length in Privacy International's complaint^{cxviii} and we do not repeat those submissions here.

6.54 The Information Commissioner's Office ("ICO") is currently reviewing data protection issues arising from the use of MPE in Scotland and the recent report by Sub-Committee highlights the potential to collect excessive amounts of data in breach of the DPA 2018.

"130. The ICO submitted that data protection law requires information to be obtained for a specific, explicit and legitimate purpose and raised a particular concern with the cyber kiosks ability to image a large amount of data, much of which could be irrelevant.

131. David Freeland from the ICO, explained why the use of cyber kiosks could lead to Police Scotland not complying with data protection law, telling the Sub-Committee that:

"If the police went through all of someone's text messages, that would potentially be an intrusion into other people's private conversations that were not relevant to the case; it would not simply be a case of focusing on the conversations between the particular persons who were already of interest...extracting everything wholesale in that way puts the police at risk of non-compliance."^{cxxix}

6.55 David Freeland, in evidence to the sub-committee on 13 September 2018 stated:

"From our perspective, data protection law is quite clear that information should be obtained for a specific explicit and legitimate purpose, which should be established at the outset. If the information were to be used for some completely different or unrelated purpose, that would not comply with data protection law.

To echo the point that has just been made, one of the principles of data protection law is that the information that is obtained must be adequate, relevant and limited to the specific purpose. In this context, that means that we should have evidence-led policing, rather than everything being obtained just in case there might be something there."

VICTIMS AND WITNESSES

6.56 As noted by the ICO, the legal basis in relation to phones of victims and witnesses is not covered in the Legal Opinion obtained by Police Scotland.

6.57 Police Scotland appear to have changed their position in relation to consent as a basis for proceeding data from the phones of victims and witnesses. In written submissions dated 12 November 2018, Police Scotland stated that:

“In respect of victims and witnesses the police will often rely upon individuals volunteering their devices and providing a level of informed consent. We recognise the importance placed upon us to properly explain how the police might handle the individual’s information. This guidance will be included within the public information leaflet as well as the supporting document sets, relied upon by our officers.”

6.58 However, in the DPIA version 0.12 it states:

“Is the processing based on consent and if so, why?”

No – not consent based – Whilst there will be occasions when a witness/member of the public provides their device to assist in a police investigation the taking possession of the device by the police is by means of seizure. There may be consent on behalf of the device owner at that time however by virtue of the fact that device is seized and may not be returned to them if it is requests, consent is not required to access the data.”

6.59 But in the DPIA version 0.14 it states that:

“Victims and witnesses

There is no clear documented basis for seizure and examination of a digital device from a victim or witness, other than by consent or by warrant. Informed consent should be obtained.

To comply with these requirements the Police Scotland – ‘Digital Examination Consent Records’ should be understood and completed by the victim / witness.’

6.60 In their letter dated 2 September to the Justice Sub-Committee on Policing, Police Scotland state that they have engaged publicly on the matter of consent and how it relates to digital forensic examination matters for victims and witnesses. They have done this via two public engagement events with the purpose of developing ‘an enhanced process for Consent Capture in support of Digital Forensic Examination’.

6.61 Police Scotland have not obtained legal advice on the reliance on consent with respect to the examination of devices of victims and witnesses. As stated above, it is clear that the circumstances in which consent can be an appropriate legal basis are limited, it is extremely difficult to gain free consent given the clear imbalance of power between individuals and the police and in any event, processing must be based on law. Hence, why from a data protection perspective a clear legal framework is a necessity and we question Police Scotland’s reliance on consent as the sole legal basis.

6.62 In relation to Article 8 European Human Rights Act, the starting point is that waiver of a Convention right is effective only if it is established in “*an unequivocal manner, and be given in full knowledge of the facts, that is to say informed consent.*” (*Pfeifer and Plankl v Austria* 25 February 1992, Series A no.227 §§37-38) Further, in the specific context of the execution of a search warrant the European Court of Human Rights has held that the fact that someone has cooperated in the context of the execution of a search warrant does not remove the

interference with their Article 8 rights; this is particularly true where the absence of such cooperation would not prevent a search being undertaken.

- 6.63 In relation to Data Protection legislation, as noted by the ICO in their written submissions dated 10 June 2019:

“The police may ask for permission to seize and interrogate a person’s mobile device. However, under state protection law, the legal basis for the subsequent processing of personal data held on the device, and any retention of personal data of evidential value, needs to be considered. That will include whether consent is a valid legal basis in this context.”

- 6.64 The Scottish Human Rights Commission notes in written submission dated 7 June 2019 that:

“Where witnesses and complainants are concerned, the analysis is also insufficient [Para 29]. There are already questions of whether consent can be valid in the case of complainants given the pressures that they face and the imbalance of power. Recent cases over the ‘mandatory examination’ of complainants’ mobile devices in sexual offence cases make clear evidence of how challenging and unwelcome this can be. It is important to note that any information arising from a cyber kiosk examination may be subject to disclosure in prosecution.”

- 6.65 We note that the use of ‘consent’ does not mean that Police Scotland cannot seize a device. They state in DPIA version 0.14 that:

“...It may therefore be the case that seizure of a device at common law from a victim / witness may be justified in certain cases, if there is adequate ‘urgency’ to justify the action. This would require due regard to the specific facts and circumstances encountered at that time.”

- 6.66 We believe that victims must have agency in whether they hand over their phones. We acknowledge that in some instances the police may seek consent from victims prior to extracting or viewing data on their phones. However, this is different to what legal basis should be in place to permit the processing of data from the phones of victims, including under Data Protection legislation which require there be a basis in law. We submit that reliance on solely consent as a legal basis to process the data of victims risks falling short of the requirements of Law Enforcement Directive thus avoiding legal protections and safeguards that must be in place for victims and witnesses if they choose to provide data from their mobile phones.

- 6.67 As noted above, whilst there may be some situations where voluntary agreement for certain forms of intrusive processing should be part of the process, this alone cannot justify the processing which must also have a basis in law and sufficient safeguards in. We are particularly concerned in context of mobile phone extraction as to whether any such consent is informed and specific enough to authorise the intrusion. Furthermore, the power imbalance between the police and a member of the public, means that it is extremely difficult to gain truly ‘free’

consent. Thus any such 'voluntary agreement' must be accompanied by a strong level framework and safeguards.

- 6.68 We further note that even if victims do not consent, Police Scotland maintain (§6.63 above) that their devices may be seized. This further highlights the need for a sufficient legal basis and the false confidence that could be placed in 'consent.'

ARTICLE 8

Article 8 (right to respect for private and family life, home and correspondence) of the European Convention on Human Rights provides that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- 6.69 The UN Special Rapporteur on Privacy considers that the right to privacy is essential *‘to dignity and the free and unhindered development of one’s personality’*.^{cxxx}
- 6.70 The right to privacy supports other fundamental rights and freedoms of democratic societies including freedom of opinion, expression, peaceful assembly and association.
- 6.71 In his report ‘A Question of Trust’^{cxxxi} David Anderson QC states that *“Intrusions into privacy have been compared, compellingly, to environmental damage: individually their impact may be hard to detect, but their cumulative effect can be very significant.”* He considered four elements of privacy. That it enables expression of individuality; facilitates trust, friendship and intimacy; is necessary for the securing of other human rights; and empowers the individual against the state.
- 6.72 The right to privacy is an internationally recognised human right and enshrined in UK domestic law^{cxxxii} under Article 8 of the European Convention on Human Rights as enshrined in the Human Rights Act 1998 (“HRA”). The use of Mobile Phone Extraction by law enforcement is an interference with private life and must be “in accordance with the law” and necessary and proportionate to meet a legitimate aim.
- 6.73 There is no doubt that the use of cyber kiosks and cybercrime Hubs engage Article 8(1) of the Convention. Depending on the nature of the information extracted, it may interfere with [i] private and family life [ii] home and [iii] correspondence limbs of this Convention right. In any given case mobile phone extraction may encompass information gathering that is equivalent to obtaining of sensitive personal data, the interception of communications, equipment interference and the acquisition of communications data. These are all activities

that squarely engage Article 8. The nature and scope of the information likely to be obtained through mobile phone extraction means that the use of this technology will often amount to a very significant intrusion in Article 8 rights (and may also engage other rights including the right to freedom of expression under Article 10 and the right to freedom of association and assembly under Article 11.)

6.74 The Scottish Criminal Bar Association states in its submission to the Sub-Committee that:

“It is a statement of the obvious that the use of these devices would allow police officers to access information that may well be personal and/or sensitive, but irrelevant for the purposes of any police inquiry. In the circumstances, the individual’s common law rights to privacy and Article 8(1) ECHR right to private and family life must be very live considerations. The SCBA is concerned that the correspondence and evidence provided thus far by Police Scotland does not appear to address to any meaningful degree this issue;”

6.75 In the DPIA version 0.14 there is reference to intelligence gathering. On this point we again note the submission of the Scottish Criminal Bar Association which states that Police Scotland does not appear to address to any meaningful degree the issue as to how Scots law’s general prohibition on searches amounting to ‘fishing exercises’ by the police interacts with the proposed use of these devices.

6.76 The European Court of Human Rights jurisprudence^{cxxxiii cxxxiv} on surveillance makes it clear that Article 8 is engaged by the collection of information falling within its ambit regardless of whether or not the state ultimately view that information. Moreover, the Court has emphasised that correspondence (which would encompass various categories of information on a mobile phone) is protected regardless of the nature of the information contained therein.

427. The right to respect for “correspondence” within the meaning of Article 8 § 1 aims to protect the confidentiality of communications in a wide range of different situations. This concept obviously covers letters of a private or professional nature (*Niemietz v. Germany*, § 32 *in fine*), including where the sender or recipient is a prisoner (*Silver and Others v. the United Kingdom*, § 84; *Mehmet Nuri Özen and Others v. Turkey*, § 41), but also packages seized by customs officers (*X v. the United Kingdom*, Commission decision). It also covers telephone conversations between family members (*Margareta and Roger Andersson v. Sweden*, § 72), or with others (*Lüdi v. Switzerland*, §§ 38-39; *Klass and Others v. Germany*, §§ 21 and 41; *Malone v. the United Kingdom*, § 64), telephone calls from private or business premises (*Amann v. Switzerland* [GC], § 44; *Halford v. the United Kingdom*, §§ 44-46; *Copland v. the United Kingdom*, § 41; *Kopp v. Switzerland*, § 50) and from a prison (*Petrov v. Bulgaria*, § 51), and the “interception” of information relating to such conversations (date, duration, numbers dialled) (*P.G. and J.H. v. the United Kingdom*, § 42). 428. Technologies also come within the scope of Article 8, in particular electronic messages (emails) (*Copland v. the United Kingdom*, § 41; *Bărbulescu v. Romania* [GC], § 72), Internet use (*Copland v. the United Kingdom*, §§ 41-42), and data stored on computer servers (*Wieser and Bicos Beteiligungen GmbH v. Austria*, § 45),

including hard drives (*Petri Sallinen and Others v. Finland*, § 71) and floppy disks (*Iliya Stefanov v. Bulgaria*, § 42).

Examples of “interference”

430. The content and form of the correspondence is irrelevant to the question of interference (*A. v. France*, §§ 35-37; *Frérot v. France*, § 54). For instance, opening and reading a folded piece of paper on which a lawyer had written a message and handed it to his clients is considered an “interference” (*Laurent v. France*, § 36). There is no de minimis principle for interference to occur: opening one letter is enough (*Narinen v. Finland*, § 32; *Idalov v. Russia* [GC], § 197). 431. All forms of censorship, interception, monitoring, seizure and other hindrances come within the scope of Article 8.

- 6.77 It is not only the extraction of data that engages Article 8. It is well established that the storage and/or further use of information gathered by a state agency constitute further, and discrete, interferences with privacy rights.
- 6.78 It is apparent from the hearings of the Justice Sub-Committee and the content of the Police Scotland impact assessments that there are a wide range of references to different legal bases for conducting mobile phone extraction. Two things are apparent, first, there is manifest lack of clarity as to the legal basis for undertaking mobile phone extraction; and second there is a very wide range of statutory powers and contexts in which the police consider they can use cyber kiosks (and cybercrime hubs).
- 6.79 At the Sub-Committee hearing on 13 September 2018 Diego Quiroz (Scottish Human Rights Commission) commented:

“...I would like to roll back a bit to the question about legality, which is very important under human rights and the rule of law. There are two aspects, one of which is the existence of a legal framework. Some of that has been expressed by Police Scotland. Once there is a legal framework, the question is about its quality.

Accessing sensitive and personal data certainly engages article 8 of the European convention on human rights. A cluster of cases from the European Court of Human Rights in Strasbourg – everything from *Copland v United Kingdom* to *Kennedy v United Kingdom* and *S and Marper v United Kingdom* – confirms that. That is quite clear.

We know that cyberkiosks can access private data – everything from texts to photos and web browsing – and even more sensitive data, such as biometric data. My phone has my fingerprints and my voice, for example. In a criminal law context there can even be information about journalistic material or legally privileged information. That is incredibly sensitive data, so the framework and its legality are important.

It is possible to find more private information in a mobile phone than in a bedroom or a house. Let us keep with that metaphor. The police need a warrant to search a house. That being the case, a more or equally intrusive digital measure will certainly require a similar safeguard. However, this is the first time I have heard the police mentioning the idea of using warrants. I think that the Commission would not be satisfied if there was no similar legal safeguard to that which there is when a house is searched in Scotland.”

“The second point is that a warrant must be specific. A warrant by itself could be unlawful...It must be specific enough to cover the reference that is mentioned; it cannot be about all the data in the mobile phone. The information in question must be relevant to the case, otherwise the taking of it would be unlawful. The issue is more nuanced than just involving a warrant.”

- 6.80 At the Sub-Committee hearing on 15 November 2018 Diego Quiroz emphasised the believe of the Scottish Human Rights Commission that there is no legal basis outside the context of a warrant, and that is because it entails a significant interference with rights under Article 8 of the European Convention on Human Rights. He stated the techniques lack legal certainty and adequate safeguards against abuse and arbitrariness.

“The legal basis for the techniques argued by the police appears to be founded on a number of contexts and statutory provisions arising in many different circumstances. That makes their legality highly fact dependent, and it seems quite reasonable to say that we therefore do not have a legal basis for such examinations of mobile phones.”

“...it is an incredibly complex framework which applies in different circumstances. It is therefore difficult, if not impossible, to discern the legal powers that the police have to use that technique by just applying logic, as was said. There is a lack of specificity in the current law, which is something that we think is required in the framework.”

- 6.81 Clare Connelly, Faculty of Advocates stated at the same hearing that:

“The fact that Police Scotland representatives have returned a number of times without the clear legal framework that you are looking for reflects the complexity of that challenge. So far in case law, we have seen that, when it comes to examining mobile devices, the Scottish courts rely on the traditional legal approach. In my respectful submission, that traditional legal approach is not fit for purpose, and that is a matter that needs to be looked at again.”

“The 2016 act certainly empowers police officers to stop and search, but that does not necessarily give the Article 8 protections that are clearly of concern to the panel and to you. For that reason, I would say that we do not have a fit for purpose legal framework in place at the moment to allow the roll-out of the policy and the use of cyber kiosks without interfering with the Article 8 rights of individuals.

6.82 In written submissions dated 2 November 2018 the Scottish Human Rights Commission stated that:

“MPB [Mobile Phone Browsing] is highly intrusive of the right to privacy, home and correspondence. We consider that there are considerable difficulties when considering the legal basis of this technique. The Commission is of the view that there is a lack of clarity as to the precise legal basis for the use of this technique as well as an absence of sufficient oversight safeguards. MPB appears to be founded on seizure powers (rather than examination powers) arising in many different policing contexts. While the legality if fact dependent, it is reasonably foreseeable that there could be instances where the legal basis for a such searches does not meet the ‘quality of the law’ requirement in Article 8 of the ECHR. This is likely to be the case where it is deployed outside of the context of judicial warrants.

Furthermore, there is a lack of bespoke domestic law governing this issue, which means the legal tests of foreseeability and accessibility test are unlikely to be met in some instances. Serious consideration should also be given to the issue of independent oversight for the use of MPB, which seems unsuitable at the moment.

An adequate legal and policy framework requires both the sufficient precision to enable any individual (if need be with appropriate advice) to regulate his conduct and adequate safeguards to guarantee against the risk of abuse and arbitrary interference.”

6.83 On the point of ‘seizure’ rather than examination powers, Stewart Stevenson MSP, raised question about the law applicable to seizing of a phone as opposed to the subsequent searching. At the 15 November 2018 hearing Stewart Stevenson MSP stated that:

“I wonder whether the complexities might be susceptible to trying to granularize the issue. I want to do that in a particular way.

Is there a different set of law that applies to the seizing of a phone as opposed to the subsequent searching? I can see – this is not a legal statement – that it makes logical sense to seize a phone to protect is because it would be interfered with in some circumstances, even if there might have to be legal process to allow the searching of that phone, just as the police might secure premises but not have the right to enter and search them. Is it reasonable to look at the problem not as a single problem but as a sequence of different legal competences or questions that need to be asked? I think that “Seizing” and “Searching” sound like two useful headings. Am I right or wrong in looking at the matter in that way?”

6.84 Diego Quiroz picked upon this point and stated:

“The point about the seizure of evidence from a human rights perspective is that the powers that traditionally allow the police to seize items cannot be considered and applied in the case of mobile phones. There are no separate powers for the examination of seized items and most

of the provisions that were referred to are parasitic on other powers. That means that they have different meanings and different purposes.”

- 6.85 It is also noted with interest that Police Scotland are open to distinguishing the legal basis for seizure and examination in relation to the phones of victims. However, they have not been willing to do more broadly.

“Absence of documented ‘legal basis’ does not mean that seizure of devices for victims or witnesses would be inadmissible. The admissibility of evidence is a matter for the court to decide having considered the evidence, and the specific facts and circumstances in which the device was seized with due regard to the public interest and fairness to the accused.

This power of seizure at common law as outlined above is distinct from any subsequent examination of a device. Whilst ‘urgency’ may apply to the seizure of the device, circumstances were that urgency could be applied to subsequent examination is much less common. A warrant may be required for such an examination. Where a device is seized in the above circumstance (urgency applies) COPFS should be contacted and a warrant should be considered for any subsequent examination of the device data.”

- 6.86 Whilst it is not specific to the position under Scots Law, we note Privacy International’s submission to the Law Commission of England and Wales Consultation on search warrants (copy attached). The Law Commission has stated that search warrants are “among the most intrusive powers that investigators can exercise.”

- 6.87 In written submissions Open Rights Group on 13 November 2018 emphasised the need for clear, foreseeable and adequately accessible national law. They highlighted Police Scotland’s Human Rights Impact Assessment at page 6 which states:

“The police are entitled at common law to seize anything it is reasonably believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure.” “All seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision.”

- 6.88 On 7 June 2019 the Scottish Human Rights Commission wrote to the Sub-Committee stating that having considered the response to the letter of the Justice Minister on digital device triage systems and the Legal Opinion provide by Police Scotland, they were still not satisfied the use of cyber kiosks by Police Scotland complies with the requirements of Article 8 of the European Convention on Human Rights:

“This is because the law surrounding the use of cyber kiosks lacks sufficient quality to be accessible and foreseeable. In addition, there are no adequate safeguards in place as the legislature (when enacted) did not consider situations of seizure and search in this particular

context. Therefore the current framework or the lack of it does not provide sufficient and robust safeguards for people's privacy rights in this context."

6.89 We believe that:

- A search of a person's phone can be more invasive than a search of their home, not only for the quantity and detail of information but also the historical nature. The state should not have unfettered access to the totality of someone's life and the use of Mobile Phone Extraction requires the strictest of protections.
- The police must have a warrant issued on the basis of reasonable suspicion by a judge before forensically examining any suspect's smartphone, or otherwise accessing any content or communications data stored on the phone.
- A clear legal basis must be in place to inspect, collect, store and analyse data from devices. It must be considered whether such intrusive technology should only be used in serious crimes.
- Reliance on consent is fundamentally problematic given the power imbalance inherent in the relationship between an individual and the police. Reliance on consent as the sole legal basis falls short of the requirements of the Law Enforcement Directive and there must be a basis in law.
- There must be adequate safeguards to ensure intrusive powers are only used when necessary and proportionate. If law enforcement are to use vulnerabilities that constitute hacking, given the risk to device security, it needs to be considered whether this is ever proportionate.
- The analysis of necessity and proportionality should include any effect the police action may have on the security and integrity of the mobile phone examined, or mobile devices more generally.
- The owner and user(s) of any phone examined should be notified that the examination has taken place.
- Anyone who has had their phone examined should have access to an effective remedy where any concerns regarding lawfulness can be raised.
- There must be independent oversight of the compliance by the police of the lawful use of these powers.

7. RECOMMENDATIONS

Recommendations regarding deployment of cyber kiosks

- The deployment of cyber kiosks should not take place unless and until there is a clear legal basis.
- A warrant issued on the basis of reasonable suspicion by a judge should be acquired by examining any suspect's phone.
- It is not appropriate to rely solely on consent to extract data from the phones of victims and witnesses, there must be a clear legal basis.

Recommendations regarding functionality of cyber kiosks

- Clarification is necessary in relation to whether:
 - (a) Cellebrite devices to be used in the cyber kiosks have the capability to extract and store data;
 - (b) Whether there is any future intention that data be downloaded at the kiosk; and
 - (c) If this is the case, what procedure the police intend to adopt in relation to impact assessments, public and parliamentary consultation.

Recommendations regarding cybercrime hubs

- Police Scotland should respond to the questions of the Sub-Committee regarding hubs.
- Police Scotland should provide clarity on the legality of cyber crime hubs and the safeguards in place.
- Police Scotland should provide information regarding the use of cloud analytics and artificial intelligence techniques in relation to cyber crime hubs.

Recommendations regarding audit

- Independent audits should be regularly carried out to:
 - Ensure that cyber kiosks are not used for fishing expeditions.
 - Review the necessity and proportionality of use of cyber kiosks and cybercrime hubs.
 - Review statistics on the use of cyber kiosks and cybercrime hubs.
- Annual reports and statistics regarding the use of cyber kiosks and cyber crime hubs should be publicly available.

Recommendations regarding devices

- Cyber security standards should be agreed and circulated, specifying how data must be stored, when it must be deleted, and who can access.
- All authorities who use these powers must purchase relevant tools through procurement channels in the public domain and regularly update a register of what tools they have purchased, including details on what tools they have, the commercial manufacturer, and expenditure amounts.

- Technical standards must be created and followed to ensure there is a particular way of obtaining data that is repeatable and reproducible, to ensure verification and validation. This should be accompanied, for example, by a clearly documented process.
- Technical skill is required as with this unprecedented amount of electronic evidence comes the need for highly skilled mobile forensic investigators. Consideration must be given to the risk of miscarriages of justice.
- The testing, trialling and deployment of new forms of highly intrusive technology must be accompanied by impact assessments, adequate safeguards and engagement with the public and civil society.

General recommendations regarding legality

- A search of a person's phone can be more invasive than a search of their home, not only for the quantity and detail of information but also the historical nature. The state should not have unfettered access to the totality of someone's life and the use of mobile phone extraction requires the strictest of protections.
- The police must have a warrant issued on the basis of reasonable suspicion by a judge before forensically examining a suspect's smartphone, or otherwise accessing any content or communications data stored on the phone, whether by cyber kiosk or cybercrime hub.
- A clear legal basis must be in place to inspect, collect, store, analyse data from devices.
- Reliance on consent is fundamentally problematic given the power imbalance inherent in the relationship between an individual and the police. Reliance on consent as the sole legal basis falls short of the requirements of the Law Enforcement Directive and there must be a basis in law.
- There must be adequate safeguards to ensure intrusive powers are only used when necessary and proportionate.
- If law enforcement are to use vulnerabilities that constitute hacking, particularly with respect to cybercrime hubs, it needs to be considered whether this is ever proportionate.
- The analysis of necessity and proportionality should include any effect the police action may have on the security and integrity of the mobile phone examined, or mobile devices more generally.
- The owner and user(s) of any phone examined should be notified that the examination has taken place.
- Anyone who has their phone examined should have access to an effective remedy where any concerns regarding lawfulness can be raised.
- There must be independent oversight of the compliance by the police of the lawful use of these powers.

CONCLUSION

The situation in Scotland regarding the use of mobile phone extraction has come a long way since the secret trials were exposed. The inquiry by the Justice Sub-Committee has brought much needed transparency and has interrogated the use of cyber kiosks prior to their deployment. Without this inquiry, impact assessments would have not necessarily been carried out, the deficiencies in the legal basis would not have been exposed and the public would have less knowledge about the use of highly intrusive technology.

Yet in many respects the inquiry has led to more questions than have been answered. The use of cyber crime hubs remains opaque, the kiosks have capabilities that could be used but have not been sufficiently clarified and given that, as explored above, cyber kiosks can be used without search parameters (DS Burnett §3.25) and used as ‘intelligence’ (DPIA version 0.14) the use of kiosks for fishing expeditions remains a live issue, in the opinion of Privacy International.

The key question is whether there is lawful basis for Police Scotland to use cyber kiosks. The resounding outcome of the Justice Sub-Committee’s inquiry and the submissions from the External Reference Group is that the legal basis upon which Police Scotland seek to rely is deficient. In this context it is deeply regrettable that the Cabinet Secretary for Justice is not willing to take a more proactive role or instigate any actions by the Scottish Government to tackle this issue. On the one hand we have Police Scotland who believe they have legal basis but equally have no law-making powers and on the other, the Government which could push for sound legal basis appear prepared to leave resolution of the issue to the Courts – a time consuming and costly exercise which is not to the benefit of any of the parties which have been willing to engage in an open and constructive dialogue through the Committee inquiry and the External Reference Group.

Privacy International believe that not only do we need transparency and accountability, but in order to protect the public we need robust safeguards. In particular, Privacy International believe that consideration of the need for a warrant is of the utmost importance. Unfortunately, we are yet to see adequate safeguards put in place.

References

ⁱ Marx, Gary T. *Privacy in the Modern Age. The Search for Solutions*, New York, The New Press, 2015, p.xi

ⁱⁱ Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.1

ⁱⁱⁱ Whilst this report is focussed on England and Wales, the findings also merit consideration in Scotland: <https://publications.parliament.uk/pa/ld201719/ldselect/ldscitech/333/333.pdf>

^{iv} <https://www.bbc.co.uk/news/uk-48086244> & <https://www.theguardian.com/commentisfree/2019/apr/30/rape-victims-mobile-phones-trial-women-sexually-assaulted-scrutiny-consequences-rapist>

^v Scottish Police Authority, SPA Strategy, Policy and Performance Committee, 8 May 2019, https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190503SPAreport_on_cyber_kiosks.pdf

^{vi} Letter from Police Scotland to Justice Sub-Committee on Policy, 2 September 2019 https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/cyber.pdf

^{vii} <https://privacyinternational.org/press-release/1755/press-release-privacy-international-issues-complaint-uk-information-commissioner>

^{viii} Letter from Police Scotland to Justice Sub-Committee on Policing, 2 September 2019 https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/cyber.pdf

^{ix} Privacy International Press Release, 26 April 2018 <https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile>

^x The Herald, Police Scotland in secret phone hack operation, 1 April 2018 <https://www.heraldscotland.com/news/16130745.police-scotland-in-secret-phone-hack-operation/>

^{xi} As reported by the Scottish Justice Sub Committee on Policing “In its letter of 6 June 2018 Police Scotland confirmed that only data on the number of devices examined had been collated. Adding that: “Further data in terms of nature of seizure, specific lawful policing purpose under which the device was seized and subsequently examined and the evidential efficacy of those examination in supporting a prosecution were not collated. The reason for this being that this was not the purpose of the trial.” https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-DigitalDeviceTriageSystems.pdf

^{xii} Police Scotland submission to Justice Sub-Committee on Policing, 30 April 2018, https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS.pdf

^{xiii} Justice Sub-Committee on Policing, Official Report, 10 May 2018, <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526&i=104575>

^{xiv} Report on Police Scotland’s proposal to introduce the use of digital device triage systems (cyber kiosks) 8 April 2019 <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{xv} Report on Police Scotland’s proposal to introduce the use of digital device triage systems (cyber kiosks) 8 April 2019 <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{xvi} Written submission from Police Scotland, 30 April 2018, https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS.pdf

^{xvii} Justice Sub-Committee on Policing, Official Report, 13 September 2018 <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&i=105715>

^{xviii} Report on Police Scotland’s proposal to introduce the use of digital device triage systems (cyber kiosks) 8 April 2019 <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{xix} Justice Sub-Committee on Policing, Official Report, 9 May 2019 <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=12093>

^{xx} Written submission from Open Rights Group, 13 November 2018

https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ORG-CyberKiosks.pdf

^{xxi} Seizing the Future, Seeking clarity of law in the seizure and search of mobile devices in Scotland, Matthew Rice,

https://www.openrightsgroup.org/assets/files/pdfs/Scotland/Seizing%20the%20future_%20Seeking%20clarity%20of%20law%20in%20the%20search%20and%20seizure%20of%20mobile%20devices%20-%20Open%20Rights%20Group.pdf

^{xxii} Justice Sub-Committee on Policing, Official Report, 13 September 2018, page 9

<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&mode=pdf>

^{xxiii} Justice Sub-Committee on Policing, Official Report, 10 May 2018

<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526>

^{xxiv} Justice Sub-Committee on Policing, Official Report, 10 May 2018

<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526>

^{xxv} Justice Sub-Committee on Policing, Official Report, 10 May 2018

<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526> &
<https://www.parliament.scot/msps/currentmsps/daniel-johnson-msp.aspx>

^{xxvi} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.10

^{xxvii} Cellebrite, (2019) Smarter Forensics [ONLINE] Available at: <https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf> [Accessed on 23 March 2019]

^{xxviii} McQuaid, J, (2018) Magnet Forensics [ONLINE] Available at:

<https://www.magnetforensics.com/resources/recorded-webinar-an-in-depth-look-at-different-password-bypass-options-2/?submission=https://go.magnetforensics.com/l/52162/2018-11-14/jxklfj> [Accessed on 24 March 2019]

^{xxxix} Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.63

^{xxx} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.17

^{xxxii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.2

^{xxxiii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019

^{xxxiii} Justice Sub-Committee on Policing, Official Report, 13 September 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&mode=pdf>

^{xxxiv} Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.143

^{xxxv} Privacy International, What types of data can law enforcement extract from my phone?
<https://privacyinternational.org/news-analysis/2840/what-types-data-can-law-enforcement-extract-my-phone>

^{xxxvi} Justice Sub-Committee on Policing, Official Report, 15 November 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11785>

^{xxxvii} Justice Sub-Committee on Policing, Official Report, 13 June 2019
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=12191>

^{xxxviii} Cellebrite (2019) [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 30 March 2019]

^{xxxix} Cellebrite webinar (December 2018) [ONLINE] Available at: <https://www.cellebrite.com/en/webinars/building-an-investigation-using-social-media/> [Accessed on 20 December 2018]

^{xl} Cellebrite webinar (December 2018) [ONLINE] Available at: <https://www.cellebrite.com/en/webinars/building-an-investigation-using-social-media/> [Accessed on 20 December 2018]

^{xli} Cellebrite (2019) Cellebrite [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 12 March 2019]

^{xlii} Cellebrite Product Release Notes <https://www.cellebrite.com/en/support/product-releases/>

^{xliii} Goldberg, M (March 2018) Cellebrite webinar [ONLINE] *Leverage the IoT to close cases faster* Available at: <https://www.cellebrite.com/en/webinars/leverage-the-iot-to-close-cases-faster/> [Accessed on 19 September 2018]

^{xliv} Goldberg, M (March 2018) Cellebrite webinar [ONLINE] *Leverage the IoT to close cases faster* Available at: <https://www.cellebrite.com/en/webinars/leverage-the-iot-to-close-cases-faster/> [Accessed on 19 September 2018]

^{xlv} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.81

^{xlvi} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/12/ReleaseNotes_UFEDCloudAnalyzer_7.6.pdf [Accessed on 4 February 2019]

^{xlvii} The Statistics Portal [ONLINE] Available at: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

^{xlviii} Smith, C (April 2019) DMR [ONLINE] Available at: <https://expandedramblings.com/index.php/amazon-statistics/> [Accessed on 25 April 2019]

^{xlix} Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>

ⁱ Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>

ⁱⁱ Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>

ⁱⁱⁱ Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/12/ReleaseNotes_UFEDCloudAnalyzer_7.6.pdf [Accessed on 4 February 2019]

ⁱⁱⁱⁱ ibid

^{liv} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2019/08/ReleaseNotes_CA_7.9-web.pdf [Accessed on 4 February 2019]

^{lv} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78-80

^{lvi} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]

^{lvii} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]

^{lviii} ibid

^{lix} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]

^{lx} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31 March 2019]

^{lxi} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31 March 2019]

^{lxii} Cellebrite Release Notes, Release Version 7.6: UFED Cloud Analyzer, (January 2019) Cellebrite [ONLINE] <https://www.cellebrite.com/en/support/product-releases/> [Accessed on 31 March 2019]

^{lxiii} Cellebrite Release Notes, Release Version 7.6: UFED Cloud Analyzer, (January 2019) Cellebrite [ONLINE] <https://www.cellebrite.com/en/support/product-releases/> [Accessed on 31 March 2019]

^{lxiv} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/12/ReleaseNotes_UFEDCloudAnalyzer_7.6.pdf [Accessed on 4 February 2019]

^{lxv} Cellebrite Cloud Analytics (2019) Cellebrite [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 20 December 2019]

^{lxvi} Cellebrite (2019) [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 2 May 2019]

^{lxvii} Release Notes (March 2018) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/03/UFEDCA7.1_ReleaseNotes.pdf [Accessed on 20 April 2019]

^{lxviii} The Guardian 'Police trial AI software to help process mobile phone evidence', Owen Bowcott and Hannah Devlin, 27 May 2018, <https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence>

^{lxix} Cellebrite (2018) White Paper *Digital Forensics is changing how law enforcement prevents and responds to terrorism* Available at: <https://www.cellebrite.com/en/whitepapers/digital-forensics-is-changing-how-law-enforcement-prevents-and-responds-to-terrorism/>

^{lxx} Professor Peter Sommer (September 2018) [ONLINE] Available at: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/92608.html> [Accessed on 23 March 2019]

^{lxxi} Professor Peter Sommer (September 2018) [ONLINE] Available at: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/92608.html> [Accessed on 23 March 2019]

^{lxxii} House of Lords, Science and Technology Select Committee, 3rd Report of Session 2017-2019 'Forensic science and the criminal justice system: a blueprint for change' 2 April 2019, <https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf>

^{lxxiii} Science and Tech Committee (November 2018) UK Parliament [ONLINE] Available on: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html> [Accessed on 23 March 2019]

^{lxxiv} Science and Tech Committee (November 2018) UK Parliament [ONLINE] Available on: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html> [Accessed on 23 March 2019]

^{lxxv} Justice Sub-Committee on Policing, 'Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks), 8 April 2019 <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{lxxvi} Supplementary written submission from Police Scotland, 14 November 2018 https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS-CyberKiosks3.pdf

^{lxxvii} Justice Sub-Committee on Policing, Official Report, 10 May 2018 <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526>

^{lxxviii} Open Rights Group, Seizing the Future, Seeking clarity of law in the seizure and search of mobile devices in Scotland, Matthew Rice, https://www.openrightsgroup.org/assets/files/pdfs/Scotland/Seizing%20the%20future_%20Seeking%20clarity%20of%20law%20in%20the%20search%20and%20seizure%20of%20mobile%20devices%20-%20Open%20Rights%20Group.pdf

^{lxxix} Justice Sub-Committee on Policing, Official Report, 9 May 2019 <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=12093>

^{lxxx} Justice Sub-Committee on Policing, Official Report, 10 May 2018 <http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526>

^{lxxxix} Justice Sub-Committee on Policing , Official Report, 13 September 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670>

^{lxxxix} Justice Sub-Committee on Policing , Official Report, 13 September 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670>

^{lxxxix} Written submission from Police Scotland, 7 September 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS-CyberKiosks.pdf

^{lxxxix} Written submission from Open Rights Group, 13 November 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ORG-CyberKiosks.pdf

^{lxxxix} Open Rights Group, Seizing the Future, Seeking clarity of law in the seizure and search of mobile devices in Scotland, Matthew Rice,
https://www.openrightsgroup.org/assets/files/pdfs/Scotland/Seizing%20the%20future_%20Seeking%20clarity%20of%20law%20in%20the%20search%20and%20seizure%20of%20mobile%20devices%20-%20Open%20Rights%20Group.pdf

^{lxxxix} Open Rights Group written submission 13 November 2018 “Further and more importantly, while the reference group was formed to specifically consider the roll-out of cyber kiosks in triage context, Open Rights Group considers that the best solution for a clear legal basis is to establish a holistic framework that covers (a) lawful bases for seizure, or surrender with informed consent, of devices (b) preliminary examination and selection (triage) that the kiosks will perform and (c) the operation and oversight of the pre-existing Cybercrime Hubs when triage results in the device being subjected to further, Hub, examination.”
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ORG-CyberKiosks.pdf

^{lxxxix} <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{lxxxix} Justice Sub-Committee on Policing, ‘Report on Police Scotland’s proposal to introduce the use of digital device triage systems (cyber kiosks), 8 April 2019 <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{lxxxix} Pidd, H, May 2017, The Guardian [ONLINE] Available at: <https://www.theguardian.com/uk-news/2017/may/04/greater-manchester-police-fined-victim-interviews-lost-in-post> [Accessed on 21 April 2019]

^{xc} Cofield, G, March 2019, The Register [ONLINE] Available at: https://www.theregister.co.uk/2019/03/21/police_federation_ransomware_attack/ [Accessed on 21 April 2019]

^{xci} NCSC (September 2018) National Cyber Security Centre [ONLINE] Available at: <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data> [Accessed on: 18 March 2019]

^{xcii} <https://www.northyorkshire-pfcc.gov.uk/content/uploads/2016/10/7ae-Mobile-Phone-Examination.pdf>

^{xciii} Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.151

^{xciv} Dr Jan Collie (27 November 2018) Evidence to Select Committee on Science and Technology Available at: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html> [Accessed on 5 March 2019]

^{xcv} New Features (April 2017) Magnet Forensics [ONLINE] Available at: <https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/> [Accessed on 23 March 2019]

^{xcvi} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.2

^{xcvii} Q.209 Dr Gillian Tully 22 January 2019 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/95512.html>

^{xcviii} Marshall,A (September 2018) Science and Technology Committee, UK Parliament [ONLINE]
Available at: [Accessed on 26 April 2019]
<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/89341.html>

^{xcix} Marshall, Angus.M, Paige, R, *Requirements in digital forensics method definition: Observations from a UK Study*, Digital Investigation 27(2018) 23-29, 20 September 2018,

^c Written submission from Police Scotland, 7 September 2018,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS-CyberKiosks.pdf

^{ci} Written submission from Police Scotland, 7 September 2018,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS-CyberKiosks.pdf

^{cii} Letter from Police Scotland to Justice Sub-Committee on Policing, 2 September 2019
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/cyber.pdf

^{ciii} Privacy Statement (2019) Celebrite [ONLINE] Available at: <https://www.cellebrite.com/fr/privacy-statement/> [Accessed on 12 April 2019]

^{civ} Open Rights Group written submissions 13 November 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ORG-CyberKiosks.pdf

^{cv} Response from the Information Commissioner's Office,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICO_Cyber_Kiosks.pdf

^{cvi} Justice Sub-Committee on Policing, 'Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks), 8 April 2019 <https://sp-bpr-en-prod-cdnet.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf>

^{cvi} Written submission from the Scottish Human Rights Commission, 2 November 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-SHRC.pdf

^{cviii} Response from the Information Commissioner's Office,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICO_Cyber_Kiosks.pdf

^{cxix} Response from the Information Commissioner's Office,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICO_Cyber_Kiosks.pdf

^{cx} Letter from Crown Office and Procurator Fiscal Service to Police Scotland, 30 January 2019,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190130COPFStoPS-CyberKiosks.pdf.

^{cx}_i Justice Sub-Committee on Policing, Official Report, 10 May 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526>

^{cxii} Supplementary written submission from Police Scotland, 12 November 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS-CyberKiosks2.pdf

^{cxiii} Supplementary written submission from Police Scotland, 11 June 2018
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PSsupplementary2.pdf

^{cxiv} Scottish Criminal Bar Association Response to the Scottish Parliament Justice Sub-Committee on Policing https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-SCBA-CyberKiosks.pdf

^{cxv} Open Rights Group, Seizing the Future, Seeking clarity of law in the seizure and search of mobile devices in Scotland, Matthew Rice
https://www.openrightsgroup.org/assets/files/pdfs/Scotland/Seizing%20the%20future_%20Seeking%20clarity%20of%20law%20in%20the%20search%20and%20seizure%20of%20mobile%20devices%20-%20Open%20Rights%20Group.pdf

^{cxvi} Response from the Information Commissioner's Office
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICO_Cyber_Kiosks.pdf

^{cxvii} Submission from the Scottish Human Rights Commission,
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-SHRC-CyberKiosks.pdf

^{cxviii} <http://www.spa.police.uk/assets/126884/532470/532474/552201/552457>

^{cxix} Justice Sub-Committee on Policing , Official Report, 13 September 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670>

^{cxx} Letter from Humza Yousaf, Cabinet Secretary for Justice, Scottish Government to Justice Sub-Committee on Policing, 3 June 2019
https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/General%20Documents/Scot_Gov_response_to_JSCoP_Digital_Device_Triage_report_20190603.pdf

^{cxxi} Justice Sub-Committee on Policing, Official Report, 13 September 2018
<http://www.parliament.scot/parliamentarybusiness/report.aspx?r=12191&mode=pdf>

^{cxxii} The communications data in question included: data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

^{cxxiii} Police Scotland, Communications Data, Standard Operating Procedure,
<https://www.scotland.police.uk/assets/pdf/151934/184779/communications-data-sop>

^{cxxiv} Investigatory Powers Act 2016
http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf

^{cxxv} European Commission, (2019) [ONLINE] Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [Accessed on 23 March 2019]

^{cxxvi} Guide to Data Protection (2019) Information Commissioner's Office [ONLINE] Available via: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/> [Accessed on 23 March 2019]

^{cxvii} DPIA (2019) Information Commissioner’s Office [ONLINE] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/> [Accessed on 27 March 2019]

^{cxviii} Camilla Graham Wood (April 2018) Privacy International [ONLINE] Available at: <https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf> [Accessed on 15 March 2019]

^{cxix} Justice Sub-Committee (April 2019) The Scottish Parliament [ONLINE] Available at: <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf> p.23 [Accessed on 20 March 2019]

^{cxx} Cannataci, J (March 2016) United Nations [ONLINE] Available at: <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21248&LangID=E> [Accessed on 20 April 2019]

^{cxixi} Anderson, David Q.C., (June 2015) *A Question of Trust, Report of the Investigatory Powers Review, Independent Reviewer of Terrorism Legislation*, p.27

^{cxixii} Article 17 of the International Covenant on Civil and Political Rights (ICCPR) to which the UK is a state party, provides that ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence’, and that ‘Everyone has the right to the protection of the law against such interference or attacks.’

The right to privacy is also guaranteed by Article 8 of the European Convention on Human Rights, which is incorporated into UK domestic law through the Human Rights Act 1998. Article 8 confers on everyone a right to ‘respect for his private and family life, his home and his correspondence’.

^{cxixiii} European Court of Human Rights, ‘Factsheet – Mass surveillance’ July 2019 https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

^{cxixiv} European Court of Human Rights, ‘Factsheet – Mass surveillance’ July 2019 https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf