Police Service of Northern Ireland

Mobile Phone Extraction (MPE)

Guidance relating to the lawful basis for conducting MPE within the PSNI

Police Service of Northern Ireland

INDEX

Table of Appendices

1. Background

In June 2020 the Information Commissioner's Office (ICO) released its investigation reports into the mobile phone extraction (MPE) conducted by police in England and Wales. In the same month, the Court of Appeal passed judgment in R v Bater-James and Mohammed (Bater-James). PSNI is party to several MPE related Judicial Reviews and in July 2021 the ICO released its MPE investigation reports for Scotland and Northern Ireland. Together these have created the requirement for PSNI to change its approach to mobile phone extraction.

The Police Service Northern Ireland (PSNI) has been required to review the lawful basis it relies on for conducting MPE. MPE needs to be viewed through the lens of a whole system approach considering not only data protection legislation (General Data Protection regulation (GDPR), Data Protection Act (DPA) 2018 and the Law enforcement regulation), but also the Criminal Procedure and Investigations Act 1996, Codes of practice and relevant statutes regarding the seizure and examination of mobile devices. Article 8, "Right to respect for private and family life", of the Human Rights Act 1998 likewise applies. The PSNI should take into account of the ICO's England and Wales report and the Court of Appeal (Criminal Division) judgment in relation to Bater-James & Anor v R [2020] EWCA Crim 790.s. and should ensure that all business processes and documentation are consistent with the findings of the review.

In respect to the investigation of suspected offences, and the seizure, retention and examination/extraction of evidence from digital devices the PSNI may rely upon, but is not limited to the following materials for example (not all of which will be engaged in every case) as providing the necessary legal basis:

a. Police (Northern Ireland) Act 1998, section 32;
b. Police and Criminal Evidence (NI) Order 1989, Articles 10, 21, 22, 24;
c. PACE Code B, para 7.14;
d. The Criminal Procedure and Investigation Act 1996, section 23 and Codes of Practice para 3.5;
e. Data Protection Act 2018, Part 3.
f. Regulation of Investigatory Powers Act 2000, section 49.
g. PSNI MPE policy 2022.

S. 32 of the Police (NI) Act 2000 provides :-

"(1) It shall be the general duty of police officers—

(a) to protect life and property;

(b) to preserve order;

(c) to prevent the commission of offences;

(d) where an offence has been committed, to take measures to bring the offender to justice."

2. Relevant Existing Disclosure Guidance

When exercising statutory powers for the purposes of preventing, detecting, investigating or prosecuting crime, officers and staff should consider responsibilities for disclosure that may arise and should be familiar with the documentation listed below. Further guidance can be found at:

- The Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland (Revised) 2005
- Further guidance on disclosure is also contained in the Public Prosecution Service Code For Prosecutors
- PPS Reasonable Line of Inquiry Guidance (RLOI)
- Attorney Generals Guidelines on Disclosure for investigators, prosecutors and defence practitioners 2020
- College of Policing Authorised Professional Practice – Extraction of Material from Digital Devices
- ICO (NI) Mobile Phone Extraction Report

3. Relevant Associated Legislation

Relevant Legislation

- Data Protection Act 2018
- Principles on the Management Of Police Information (MOPI) under Public Records Act (NI) 1923 and Disposal of Records Order (S.R. & O. 1925 No. 167)
- Section 32 of the Police Act (NI) 2000
- European Convention on Human Rights (ECHR) in particular Articles 2, 6 & 8.
- Police, Crime, Sentencing and Courts Bill

4. Categories of Device

Throughout this policy, there is reference to Mobile Phone Extraction (MPE) and particular reference is made to this as we amend policy concerning extraction of material from mobile phones.

This policy also is applicable to the extraction of digital material from other electronic devices to include laptops, in car computers, satellite navigation systems, fitness trackers and other internet-enabled devices (this list is not exhaustive).

5. Lawful basis for Examination

The provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) apply in England, Wales and Northern Ireland. Under the CPIA and its Code of Practice (Northern Ireland), police must pursue all **reasonable lines of enquiry,** whether they point towards or away from the suspect, and to gather relevant materials.

In the context of the sensitive law enforcement processing involved in MPE, the ICO previously reported that police must demonstrate that their processing is **based on law** and that:

a) the processing is **strictly necessary** for the law enforcement purpose,

b) the processing meets at least one of the conditions in Schedule 8 (see below DPA principles), and

c) at the time when the processing is carried out, the controller (Chief Constable) has an appropriate policy document in place."

This is to specifically state that the request for MPE is both a Reasonable Line of Enquiry into the offence/s under investigation, and that it is the least intrusive means of achieving the objective.

- The investigators must show justification that MPE is also necessary and proportionate in relation to the offence/s being investigated.

NB: Where investigations involve a large quantity of digital material it may be impossible for investigators to examine every item of such material individually. Therefore there should be no expectation that this should happen. Investigators and disclosure officers will need to decide how best to pursue a reasonable line of inquiry in relation to the relevant digital material, and ensure that the extent and manner of the examination are appropriate to the issues in the case. In reaching any such decisions, investigators and disclosure officers must bear in mind the overriding obligation to ensure a fair trial of any suspect who is charged

and the requirement to provide disclosure in the trial process (The Attorney Generals Guidelines for Disclosure 2020). Should the above apply prosecutorial advice can be sought from the PPS.

6. Data Protection ACT Principles

Part 3 of the DPA outlines six data protection principles which must be complied with when processing data for law enforcement purposes, including when exercising these powers, summarised below.

1. The processing of personal data for any of the law enforcement purposes must be lawful and fair.

2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

3. 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.

4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

5. Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

6. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

7. Bater-James & Anor [2020] EWCA Crim 790 Judgement

The English Court of Appeal, in the case of *Bater-James & Anor* [2020] EWCA Crim 790, provided helpful guidance on a number of issues of principle that arise frequently in the context of police investigations where complainants and other witnesses are asked by police to share the contents of their mobile telephones and similar devices:

(i) **Properly identifying when it is necessary to seek details of a witness's digital communications**.

The Court confirmed that there is no obligation on investigators to seek to review a witness's digital material without good cause. The request to inspect digital material, in every case, must have a proper basis, usually that there are reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial ("a reasonable line of inquiry"). The Court explained that "*it is not a 'reasonable' line of inquiry if the investigator pursues fanciful or inherently speculative researches. Instead there needs to be an identifiable basis that justifies taking steps in this context….there must be a reasonable foundation for the inquiry*"

(ii) **If it is a reasonable line of inquiry, how should the review of the witness's electronic communications be conducted?**

Investigators will need to adopt an incremental approach.

- ***First***, to consider with care the nature and detail of any review that is required, the particular areas that need to be looked at and whether this can happen *without recourse to the complainant's mobile telephone or other device*. It may be possible, for example, to obtain all the relevant communications from the suspect's own mobile telephone or other devices. It may also be possible to review relevant social media posts of the complainant without looking at the individual's mobile telephone, provided they are willing to provide a password.

- ***Second***, and only if it is necessary to look at the complainant's digital device or devices, an important question is whether it is sufficient simply to view limited areas (e.g. an identified string of messages/emails or particular postings on social media). In some cases, this will be achieved by simply addressing focused questions to the

witness, looking at the relevant material and taking screenshots or making some other record, without taking possession of, or copying, the device.

- ***Third***, if a more extensive enquiry is necessary, the contents of the device should be downloaded with the minimum inconvenience to the complainant and, if possible, it should be returned without any unnecessary delay. If the material is voluminous, consideration should be given to appropriately focussed enquiries using search terms, a process in which the defendant should participate.

  This process should be applied through consultation with the PPS prosecutor at an early stage and may involve the participation of the defence through the application of the Disclosure Management Document (DMD). It may be possible to apply data parameters to any search. Finally, appropriate redactions should be made to any disclosed material to avoid revealing irrelevant personal information.

(iii) **What reassurance should be provided to the complainant as to scope of the examination/review and the circumstances of any disclosure of material obtained from the device?**

It is necessary that the complainant is kept informed of proposed use to be made of the mobile telephone or other device and its contents, depending on the extent to which the witness wishes to be provided with updates.

At the outset, the complainant should be given a straightforward explanation that:

- the defendant does not have a general right to examine the contents of a witness's digital device;

- police shall only seek to examine the contents of a device when to do so is in pursuit of a reasonable line of inquiry;

- the witness is not obliged to cooperate with a police request, but if the witness fails to do so there is a risk that it may be impossible to pursue the investigation, a witness summons may be issued or any trial resulting from the investigation may be halted;

- the witness's device will only be copied (where applicable) and examined to the extent necessary to pursue the line of inquiry – irrelevant content shall not be looked at;

- only material which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused will be disclosed to the defence, and any unnecessary personal details or irrelevant information will be redacted; and

- the witness shall be kept informed as to any decisions made as to disclosure of contents of the device and the length of time it can be estimated that the investigators shall have to retain the device.

- It may be necessary to carry out sampling and searches on more than 1 occasion especially as there is a duty on the prosecutor to keep duties of disclosure under review such as an application under section 8 of the CPIA 1996 or where the defendant requests that further sampling or searches be carried out (provided it is a reasonable line of enquiry)

- In exceptional circumstances where prohibited or offensive material (IIOC) is located on a device, the device may not be returned to the owner.

8. ICO Compliance Declaration

In order for the PSNI to comply with the DPA 2018 and the Information Commissioner's Office report for Northern Ireland 2021, a declaration must be acknowledged and signed by an officer not below the rank of Inspector, prior to any application being considered for approval by the Cyber Crime Centre or Cyber Support Units. This process will be applied on a phased basis across the PSNI and further guidance can be obtained from the Cyber Crime Centre pages on Point. This ICO Compliance Declaration must be attached to the digital forensic submission form.

Authorising Inspectors must retain an evidential record of their approval. This record must include that they have considered other less intrusive methods to obtain the

information/evidence required; and the specific parameters of examination agreed with the investigating/submitting officer. The record must be made in a way to satisfy the requirements of CPIA.

9. Categorisation of MPE Suspect / Witness / Victim / Other

The PSNI needs to be clear whether it is referring to a consensual approach to engagement with a person to seek their agreement to examine their device or, alternatively, to the use of consent as a lawful basis for processing. See also "Lawful Basis for Examination".

If consent is the chosen pathway for processing data from MPE this needs to be informed consent (freely given, specifically informed and unambiguous), see Appendix A Digital Processing Notices (DPNb).

Police must therefore consider whether to take possession of the device by:

a) Consent or,

b) Using a Statutory Authority

The Status of the person will be key in this consideration and as such we must, as far as possible, make a clear distinction between different categories of individuals:

1. Those suspected of an offence;
2. Witnesses; and
3. Victims / Complainants
4. Others

SUSPECT MPE CATEGORY

The law permits police officers to seize device/s from suspects in certain circumstances. The law also provides a power of search to locate the device in certain circumstances. The

lawful powers used to search for and seize devices should be explained to suspects by the officer seizing it if practicable. Suspects are not entitled to refuse when officers are exercising their powers of search and/or seizure lawfully and by doing so they may be committing further offences.

Officers may ask suspects voluntarily to provide us with their device, even when powers of seizure are available. If agreement is forthcoming officers will take possession of the device. This may occur, for example, if suspects are suspected of committing an offence but are not being arrested.

Once in possession of the device the PSNI will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This section allows the processing of personal data when it is required for a law enforcement purpose. There are conditions attached to this. As we expect to process sensitive personal data we will only acquire data from the device when it is 'strictly necessary' to do so for that law enforcement purpose. We also need to meet one of the conditions set out in Schedule 8 DPA 2018. The most likely conditions that will be met are:

1. Necessary for judicial and statutory purposes – for reasons of substantial public interest;
2. Necessary for the administration of justice;
3. Necessary for the safeguarding of children and of individuals at risk.

(See Bater-James & Anor judgement - "*it is not a 'reasonable' line of inquiry if the investigator pursues fanciful or inherently speculative researches. Instead there needs to be an identifiable basis that justifies taking steps in this context….there must be a reasonable foundation for the inquiry")*

WITNESS /VICTIM/COMPLAINANT/OTHER MPE CATEGORY

We may take possession of devices belonging to witnesses with their agreement; often referred to as 'common law consent'. Once in possession of the device we will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This allows us to process personal data when it is required for a law enforcement purpose and to this end we must show that informed consent for processing of the device has been given (see Principle of consent and DPN documents).

There are circumstances in which a lawful power of seizure may be used to take possession of the device of a witness. For example, if the offence under investigation was felt to be sufficiently serious that police were going to continue the investigation without the victim, they may consider it necessary to obtain a warrant to obtain that evidence from a reluctant witness.

We must demonstrate that we have considered alternative, less intrusive means of achieving the same law enforcement purpose.

If officers have lawfully seized a device (e.g. during the execution of a warrant) and later find that it belongs to a witness, they should seek the agreement of the witness and complete a Digital Processing Notice (DPNa) before examining the device.

However the above may not apply where investigators have a statutory power to retain and process the device but the principle of least intrusive option and the use of informed consent remains.

DPA principles on page 13 relating to Suspect MPE also apply to Witness MPE.

10. Principle of Consent

Consent is defined in **Article 4(11) of the general data protection regulation (GDPR)** as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

In most cases a suspect's device will have been acquired using a lawful power of seizure such as those conferred under PACE, but it is also possible that their device could be acquired by asking for their informed agreement.

The investigator or police responder will consider whether the individual concerned has capacity to give informed agreement for their digital device to be taken by the police and data to be extracted. They will also consider whether their ability to understand is affected by their age or any learning impairment, injury, intoxication or trauma for example.

They will specifically consider their capacity to provide informed agreement to hand over the device where the device user is a child; an adult with cognitive impairment; a person for whom English is not their first language or the victim/witness has experienced trauma. There may be obvious and non-obvious indicators. Consider whether the individual needs independent legal support and/or time to consider their decision.

Where it is believed the device user may lack capacity or is incapacitated, the investigator will ensure steps are taken to ensure informed agreement is obtained in a way that reflects the rights of that person. For example, more time could be allowed to make the decision or investigators could ensure suitable support is available. Where appropriate, contact details may be provided so support can be obtained before informed agreement is sought, for example by an appropriate adult, guardian, advocate, interpreter or legal representative.

An individual has the right to withdraw consent for processing their data. If consent is withdrawn following completion of the data extraction process, the data may only be processed without their consent if there is a lawful basis for doing so.

11. Incremental Examination of Devices

All devices seized during an investigation that are deemed relevant and require an examination are submitted to the Cyber Support Unit (CSU) (of which there are 4) designated to service the investigation team. Only when more advanced processes / analysis is required are devices submitted to the Cyber Crime Centre (CCC). Software available across CSU and CCC is broadly similar for the majority of examinations with CCC having some additional software. CCC capability, in terms of training and analytical capability, is greater than that of CSU.

There are essentially 4 extraction types of ascending capability of data extraction and examination of mobile devices capable of being undertaken by PSNI namely:

a. *Logical Extraction* – undertaken by a PSNI Cyber Support Unit (CSUs) –. The extraction software tool, CELLEBRITE, is deployed.

b. *File System Extraction* – undertaken by a PSNI CSU –The extraction software tool, CELLEBRITE, is deployed using a deeper analysis feature of the software.

c. *Physical Extraction* – undertaken by a PSNI CSU. The extraction software tool, CELLEBRITE, is deployed. This enables making a bit-for-bit copy of the contents of the device.

d. *Full File System* – Undertaken by CSU and CCC. There are 2 extraction tools available to recover data using this method. Usually deployed to service a more immediate need or to recover specific data types.

Appendix A

Digital Processing Notice A (DPNa) – Victim/Witness

Digital Processing Notice B (DPNb) – Suspect

Digital Processing Notice C (DPNc) – Victim/Witness Further Enquiries – (New RLOI)

Digital Processing Notice D (DPNd) – Suspect Further Enquiries – (New RLOI)

Digital Processing Notice – Victim/Witness Information Notice

Digital Processing Notice – Suspect Information Notice

Digital Processing Notice - Officer Guidance