Information Commissioner's Office

Mobile phone data extraction by police in Northern Ireland

Investigation report

June 2021

ico.
Information Commissioner's Office

Foreword

Mobile phones often store large amounts of highly sensitive data, reflecting not only our most private thoughts, feelings and movements, but also those of our friends and family.

From biometric, financial and medical data, to personal information that reveals our location, political or religious beliefs, sexual orientation, and ethnic origin, mobile phones are powerful repositories of our daily lives.

When my office investigated the concerns about the potential for excessive processing of personal data extracted from mobile phones by police forces, in a process known as mobile phone extraction, we found it to be a complex area, covered by a broad range of legislation relating to criminal justice and data protection.

I published a report in June 2020, explaining the issues at play in England and Wales. That report recommended several measures aimed at regaining public confidence that may have been lost through previous poor practice by police forces. These measures included calling for a new code of practice to be implemented across law enforcement to improve compliance with data protection law.

After a pause in our investigative work due to the impact of the COVID-19 pandemic, we broadened our area of interest to consider the issue of mobile phone extraction in the criminal justice system across the UK.

Data protection legislation is consistent across the UK, but we found that police data extraction practices vary, with huge amounts of personal data often being extracted and stored without an appropriate basis in data protection law. Many investigators and prosecutors were not clear with people on how their data was going to be used, potentially dissuading citizens from reporting crime and victims being deterred from assisting police.

This new report outlines concerns around the Police Service of Northern Ireland's compliance with data protection legislation, and requires an urgent response. Recommendations include carrying out a data protection impact assessment, clarifying their lawful basis for processing, improving their policies and training for staff, and improving transparency.

The PSNI has begun work to address ICO concerns. That work must continue, and I will be expecting the organisation to provide evidence of its compliance with the law in the coming months.

This new report is published alongside a similar report covering Scotland, and an updated report covering England and Wales. We are encouraged by the

consensus across the UK regions that action is needed, but there is further work to be done.

We have seen a broad range of positive changes to governance in response to my 2020 report elsewhere in the UK, including publications by the Attorney General and the College of Policing. The principles established are applicable UK-wide, and I would recommend the PSNI considers this wider work in formulating its own response.

People are right to expect that the police will treat their personal information fairly, transparently, and lawfully, and that only data that is necessary will be taken. The ICO will continue to push for critical changes to ensure compliance with the law.

Elizabeth Denham CBE
UK Information Commissioner

Contents

Executive summary

Background

In its role as the UK regulator of data protection legislation, the Information Commissioner's Office (ICO) completed an investigation into the police practice of mobile phone extraction (MPE) when conducting criminal investigations.

In June 2020, the ICO published a report on its findings relating to police forces in England and Wales (hereafter referred to as "the England and Wales report"), in which it made a number of wide-ranging recommendations.

The ICO subsequently engaged with the Police Service of Northern Ireland (PSNI) in order to assess the extent to which the organisation complies with data protection legislation in undertaking its MPE operations.

The investigation found that the PSNI falls short of compliance in a number of areas and the organisation should address these issues as a matter of urgency.

Recommendations

Recommendation 1: The PSNI should urgently undertake a data protection impact assessment (DPIA) that covers all of the MPE activity it carries out, as per the requirement of s62 DPA 2018.

The organisation should keep the DPIA under regular review and update it prior to any further innovation or procurement in MPE capability.

Recommendation 2: The PSNI should review the lawful basis it relies on for conducting MPE, taking 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. It should ensure that all business processes and documentation are consistent with the findings of the review.

When considering this recommendation, the PSNI should engage with and have regard to the work the NPCC is undertaking in relation to recommendation 2 of the England and Wales report.

Recommendation 3: The PSNI should review its policy and produce operational guidance that ensures:

- investigators only seek to acquire digital data in circumstances when they determine that less intrusive means are not sufficient to satisfy the reasonable line of enquiry;
- approach oversight and approval processes are in operation; and
- investigators acquire only the minimum data strictly necessary.

It should modify internal systems to be supportive of the guidance and log all relevant decisions and processing operations.

The organisation should put training in place to ensure that all officers and staff are aware of the operational guidance and are clear about their personal obligations.

It should review the Authorised Professional Practice produced by the College of Policing for police in England and Wales, and prepare similar guidance for use in Northern Ireland.

Recommendation 4: The PSNI should review its published privacy information and the information it provides to individuals when acquiring their device. The organisation should ensure it supplements this with information relating to processing as a result of MPE, including information on privacy and information rights.

When considering this recommendation, the PSNI should engage with and adopt the work the NPCC is undertaking in relation to digital processing notices, as a response to recommendation 2 of the England and Wales report.

Recommendation 5: The PSNI should update its data retention policy to include the specifics of managing data it acquires through MPE, consistent with s39 DPA 2018, and operationalise:

- regular reviews and deletion of data if it cannot justify ongoing retention; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that it is not processed further and so officers cannot inappropriately access, review or disseminate the data.

Recommendation 6: As far as legislative differences and devolved administration factors allow, the PSNI should engage with work the UK Government, the NPCC and the College of Policing are undertaking. This work includes:

- the statutory power and code of practice being introduced through the Police, Crime, Sentencing and Courts Bill;
- police guidance on the considerations and processes involved in MPE; and
- privacy information officers provide to people whose devices are taken for examination.

Recommendation 7: In order to provide assurance around the integrity of the data extraction processes, the PSNI should accelerate its work to implement and maintain the standards set out in the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

Other work

In parallel with this investigation, the ICO engaged with Police Scotland and the Crown Office and Procurator Fiscal Service to examine MPE operations in Scotland. We published a separate report with these findings alongside this one.

The ICO also published a further report ("Mobile phone data extraction by police forces in England and Wales – An update on our findings") that reflects on the impact of the England and Wales report and discusses the subsequent developments.

We encourage you to familiarise yourself with both the England and Wales report and its recent update in order to fully appreciate the context of this report's findings.

Next steps

The ICO acknowledges the commitment already expressed by senior leadership of the PSNI to improving the organisation's approach to MPE. The PSNI needs to take urgent action to address the recommendations we make in this report, in collaboration with other policing colleagues represented by the NPCC.

We acknowledge the complexity of the matters we are discussing and the diversity of interested stakeholders. The ICO therefore remains committed to working with all parties to assist them in understanding and implementing these recommendations.

1. Introduction

1.1 Background

The Information Commissioner's Office (ICO) is the UK's data protection regulator. It completed a UK-wide investigation into the practice of mobile phone extraction (MPE) that police use in criminal investigations.

The aim of the investigation was to develop a detailed understanding of the legislative frameworks, governance arrangements, operating practices and challenges faced by those undertaking or affected by MPE. It also aimed to provide further clarity about data protection law for those responsible for processing personal data in this context.

In June 2020, the ICO published a report[1] that contained the findings relating to police forces in England and Wales (hereafter referred to as "the England and Wales report"). It detailed concerns relating to MPE practice and made a number of wide-ranging recommendations for improvements that we require from the UK Government, criminal justice organisations and police forces. These improvements aimed to ensure that police forces process people's data fairly and lawfully, with due consideration of privacy issues. In short, it recognised significant issues with the ways in which police forces were taking the most sensitive of data from mobile devices. It called for a transformation in both the acquisition of digital devices and the subsequent processing of extracted data.

Since the publication of that report, the ICO engaged with senior stakeholders involved with business change, and we prepared a further report which reflects on progress and makes additional recommendations. In addition, the ICO completed the first phase of its enquiries into MPE practice in Northern Ireland and Scotland.

The ICO is therefore publishing three new reports:

- Mobile phone data extraction by police forces in England and Wales – An update on our findings;
- Mobile phone data extraction by police in Northern Ireland (this report); and
- Mobile phone data extraction by police in Scotland.

[1] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

1.2 Investigative approach

The ICO aimed to understand the MPE practices that the Northern Irish policing and justice sector currently employ. This was in order to assess compliance with data protection legislation and make recommendations for any required improvements. To do this effectively, it was necessary to first examine the applicable criminal justice and law enforcement legislation in Northern Ireland.

We completed the England and Wales phase of the investigation just prior to the national COVID-19 emergency. We published the report in June 2020. We could not conduct the next phase of the investigation as planned, involving enquiries into MPE in Northern Ireland, due to the ongoing impact of the pandemic on policing operations, travel and social distancing restrictions.

The investigation team benefitted from a significant amount of MPE knowledge acquired during the England and Wales investigation, including direct observation of live operations. ICO investigators further enhanced this knowledge through substantial engagement conducted across the criminal justice community, following publication of the England and Wales report. We could therefore adopt a more targeted approach in Northern Ireland, based on specific lines of enquiry.

However, due to the COVID-19 pandemic restrictions, the team was unable to directly observe the use of MPE in live investigations in Northern Ireland. We therefore acknowledge that a limitation of this report is its reliance on policy statements and other documentation that the Police Service of Northern Ireland (PSNI) provided and notes the investigation team took during engagement with senior officers and operational staff.

We are grateful for the PSNI's willingness to engage with the investigation and for the openness and candour with which it conducted the engagement. This significantly assisted the investigation, in light of the COVID-19 pandemic restrictions.

1.3 Regulatory approach

Whilst time has elapsed between the England and Wales report's publication and this one, the investigation always intended to cover the UK as a whole. The ICO was therefore keen to apply the same approach to the engagement with all police organisations so as to not disproportionately impact any of the organisations involved. We explained in the England and Wales report that the investigation was a review of practice across the 43 police forces in England and Wales, rather than a more traditional investigation into a particular controller (an individual organisation), which might lead to enforcement action. Whilst the PSNI and Police Scotland are single organisations, the ICO adopted a similar fact-finding stance to Northern Ireland and Scotland respectively. This approach

recognises the complexity of and focuses on understanding and articulating the systemic change that we require, rather than targeting individual organisations.

1.4 Structure of this report

This introductory section of the report set the scene by describing the approach to this phase of the investigation and in the context of work carried out previously in England and Wales.

The next section summarises the MPE practice of the PSNI and analyses the extent to which the organisation complies with data protection legislation.

Finally, the report sets out a number of recommendations that aim to assist the police and other criminal justice organisations in Northern Ireland to improve their compliance with data protection law.

We recommend you familiarise yourself with the content of the related "Mobile phone data extraction by police forces in England and Wales – An update on our findings" report. This should aid understanding of the key principles involved and the resulting points covered at a summary level in this current report.

2. Current practice

2.1 Overview

The PSNI has a Cyber Support Unit (CSU) that provides the forensic MPE capability within the organisation.

The CSU has up to 60 full-time trained operators across four sites in Northern Ireland. These operators perform extractions, review the results and generate reports for the officer in charge (OIC) of the investigation to review.

If the CSU is unable to fulfil the OIC's requirements, investigators may submit a device to a Cyber Crime Centre (CCC). Here, a smaller number of officers are trained to a higher level and can handle more complex requirements.

Unlike some policing organisations, the PSNI does not triage devices using kiosk technology for its core MPE work.

However, the organisation's Public Protection Branch (PPB) procured a small number of 'in-field kits'[2] which non-specialist users can use outside of the CSU environment. The CSU is also trialling the use of one of these kits, which it could deploy should there be an urgent requirement. However, it is unclear when it would be appropriate for such a deployment, and whether the right governance, guidance and training are in place for this.

The PSNI contracts out some MPE operations to Forensic Service Northern Ireland (FSNI), but this only relates to a small proportion of MPE cases where the internal capability or capacity is under pressure.

We are significantly concerned that the PSNI does not have an overarching policy in relation to its use of MPE technology. As a result, the information we obtained during this investigation was as a result of the investigation team engaging in dialogue with the organisation's officers.

2.2 Process

The MPE process begins with the OIC completing a request using the PSNI submission portal. This is an online, form-based system which facilitates requests to the CCC and the CSU.

The OIC completes a standardised request which includes, but is not limited to, information regarding:

- the device owner;

[2] Cellebrite Responder devices

- date and time of seizure;
- location of seizure; and
- the owner's primary offence.

There is a free-text section which the OIC can use to outline the circumstances of the offence and the rationale for requesting a device examination.

The OIC's supervising officer reviews the submission to ensure it is both complete and valid. The submission portal facilitates the authorisation or rejection of requests.

The portal records a risk/harm matrix score for each authorised request, which dictates the examination's priority. The authorised request is then passed to the CCC and the CSU, and the examination of each device begins depending on its order of priority rank.

The submitting officer receives a response to their request via the portal, including the reason for a rejection. The submitting officer can then reconsider the requirement and, where appropriate, submit a revised application.

The CCC and CSU accept approved requests, process them and carry out the data extraction. The standard procedure is for an officer to attempt a full physical examination of the device and to extract all data.

The CSU officer creates a report of findings from the examination. This is peer-reviewed before a senior officer (usually a Detective Sergeant) carries out a supervisor review to verify the findings. The portal facilitates this, and this system records the outcomes of the various decision points.

The portal sends the OIC an automated email to inform them the examination is completed and that they may access the report via the portal system.

Only officers involved in the case can access the data extraction reports. The portal logs all actions and these are auditable.

2.3 Compliance with data protection principles

Part 3 of the DPA 2018 sets out the requirements[3] which apply to the processing of personal data for law enforcement purposes. We assess the level of the PSNI's compliance in relation to each of the data processing principles below.

2.3.1 First principle: lawful and fair

The first principle is that the processing must be lawful and fair. Critical to compliance with this principle is identifying an appropriate lawful basis for the processing.

[3] Further detailed explanation is available in the England and Wales report.

The ICO previously reported on the requirement to appreciate the different bases for the initial acquisition of a device and for the subsequent extraction and processing of data from it.

The PSNI has a range of legal powers to allow device seizure from people who have either been arrested or where officers reasonably believe that their device is of evidential value. Officers may also rely upon common law in their engagement with citizens for policing purposes.

We do not detail the powers available to the PNSI here, as their specifics are not relevant to this investigation. The key point is that officers must obtain the device lawfully.

At the time of writing, the UK Parliament is considering the Police, Crime, Sentencing and Courts Bill. If this Bill becomes law, this may provide a further statutory basis for PSNI officers to extract data from devices that complainants and witnesses provide voluntarily.

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[4], and
>
> (c) at the time when the processing is carried out, the controller has an appropriate policy document in place."[5]

The CPIA may meet the 'based on law' requirement for processing for the law enforcement purpose. Investigators need to document this and, in each case, before they consider using MPE, they must demonstrate that they have evidenced meeting these criteria.

The PSNI does not offer a compelling case that it gives explicit consideration to the lawful basis for processing mobile phone data. In the absence of an overarching MPE policy or a relevant data protection impact assessment (DPIA)

[4] Schedule 8 DPA 2018 details the conditions for sensitive processing under Part 3 DPA 2018
[5] s35(5) DPA 2018

(see section 2.7) there are ambiguities as to which lawful basis the PSNI is basing extractions. It appears that much rests on the individual officer's assessment as to what is appropriate in the circumstances of the case. There can be no confidence that, in all cases, a reasonable line of enquiry is the justification for an extraction request. This calls into question whether the PSNI has adequate protections in place to safeguard privacy.

Whilst we accept that officers can state a reason why they require an extraction, the system does not have the rigour of asking for either:

- specific justification for the processing; or
- documentation of matters such as providing confirmation that they considered less intrusive means of achieving the objective.

In describing engagement with complainants and witnesses, the PSNI refers to relying on consent as the lawful basis for processing and this "being recorded when freely given". However, it also makes reference to relying on necessity for law enforcement purposes in the absence of consent. Therefore, the data processing condition the PSNI relies on remains ambiguous.

The ICO understands that the PPB of the PSNI is developing guidance on the use of consent in relation to obtaining third party material.

For the avoidance of doubt, the organisation 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. The ICO previously explained how, in itself, consent is not an appropriate lawful basis for this level of intrusion into the privacy of others. This is particularly relevant here since, by default, the PSNI takes all available data.

The PSNI clearly needs to do further work to demonstrate compliance with this principle.

2.3.2 Second principle: limited purpose

The second principle states that the processing must be limited to a specified, explicit and legitimate purpose. Organisations must not process data in a manner that is incompatible with the purpose for which they collected it.

The PSNI restricts access to the data relating to extractions so that only officers working on the case in question can access it. An information system facilitates this access. This is a reassuring security measure, though the practice is not compliant due to the lack of specificity when extracting data (ie the default is to extract all data that the tool being used can obtain from the device).

The ICO is not aware of any processing for secondary purposes. However, it is difficult for the ICO to be confident in the PSNI's compliance with this principle

because it is unable to provide clear evidence of justifying the original extraction.

2.3.3 Third principle: adequate, relevant and not excessive

According to the third principle, the data must be adequate, relevant and not excessive for the purpose for which it is processed.

The PSNI stated its default policy position for MPE is the extraction of all available data from devices authorised for examination. This applies whether the CCC or CSU carry out the examination internally or whether the FSNI examines it externally. The PSNI could not demonstrate any policy, technical or practical attempt to reduce the excessiveness of extraction and subsequent processing.

Given the findings of the England and Wales report, the revisions to the Attorney General's Guidelines[6] and the Court of Appeal's judgment in Bater-James & Anor v R [2020] EWCA Crim 790[7], it is difficult to envisage how this could be a defensible position going forward.

2.3.4 Fourth principle: accuracy

The fourth principle states that data must be accurate and, where necessary, kept up to date. Controllers must take every reasonable step to ensure that they erase or rectify inaccurate personal data without delay, having regard to the law enforcement purpose for which they process it. In addition, as far as possible, they must make a clear distinction between different categories of individuals:

- those suspected of an offence;
- those convicted;
- witnesses; and
- complainants.

Organisations must, as far as possible, distinguish personal data based on fact (eg a court conviction) from personal data based on personal opinion (eg communications between individuals).

Organisations engaging in forensic examinations must comply with standards set by the Forensic Science Regulator. These standards are mandated in England and Wales, but authorities in Northern Ireland and Scotland agreed to adopt and apply relevant standards that apply to their work.

In the context of MPE in the criminal justice sector, it is important that the methods the PSNI uses to interrogate devices and extract data from them are

---

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946082/Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf

[7] http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html

accurate and reliable. The relevant accreditation for policing organisations is certification to the ISO/IEC17025 international laboratory standard.

The PSNI is yet to achieve this accreditation, and the ICO understands that there are no plans to achieve this status before 2022. Therefore, in the interim, the PSNI cannot demonstrate it is using extraction methods that provide results to an independently regulated standard.

The PSNI also disclosed that it does not categorise or actively manage data it acquires from MPE operations.

Therefore, due to all the factors we describe above, the organisation is not demonstrating compliance with this data protection principle.

2.3.5 Fifth principle: storage limitation

According to the fifth principle, organisations should not store law enforcement data for longer than is necessary. They must set appropriate limits to periodically review the need for continued storage.

The PSNI did not provide any evidence of systematic review or deletion of materials obtained through MPE. Whilst the CPIA requires the retention of relevant materials for periods depending on the circumstances of the case, this does not apply to non-relevant materials. It also does not overturn the DPA 18 requirements for periodic review of the need for continued retention.

The CSU retains material until it receives feedback from the OIC that it is no longer required and a direction to delete. However, the PSNI acknowledges that it could make improvements to this process.

The organisation stated that it updated its Review, Retention and Disposal Schedule in November 2020. It has not yet published this document and the ICO has not seen the draft, so it is not clear whether it applies to all digital forensic material.

2.3.6 Sixth principle: security

The sixth principle states that organisations must have adequate measures in place to ensure the appropriate security of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The PSNI benefits from having a bureau-style operation in which all requests for MPE go to a specialist unit that the CCC oversees and which is staffed by specially trained officers. The PSNI stores the digital materials centrally on secure replicated servers, with officers having access through a secure portal.

In situations where reports based on digital extractions need to be extracted from the secure environment, we understand the organisation conveys these on encrypted media.

Therefore, we have a reasonable level of assurance around the security of data in the core operational environment.

However, the PSNI was less clear about the security of data it captures outside of the forensic environments, using the 'in-field' equipment.

2.4 Privacy information

Controllers engaging in law enforcement processing must provide privacy information that helps people understand how organisations are processing their data[8].

Whilst the PSNI has an Adult Privacy Notice[9], this almost exclusively references processing the organisation undertakes under the GDPR (now UK GDPR), rather than under Part 3 of the DPA 2018, for the purposes of law enforcement. It does not cover MPE practices for criminal investigations.

The privacy notice contains the statement:

> "This privacy notice serves as an overarching document for PSNI. Additional privacy notices exist which are specific to certain processes and procedures within PSNI. Explicit lawful processing conditions will be set out in these tailored documents, for example, a witness statement."

However, the PSNI was unable to offer any documentation containing privacy information it routinely provides to people whose devices it had taken for examination[10].

The organisation is therefore not complying with its duties to provide adequate privacy information.

2.5 Data protection by design and default

Law enforcement controllers have an obligation to implement data protection by design and default[11]. This requires them to introduce appropriate technical and organisational measures which are designed to apply the data protection

[8] s44(1)&(2) DPA 2018
[9] https://www.psni.police.uk/advice_information/information-about-yourself/adultprivacynoticepage/
[10] A form CCC67, used when requiring a person to reveal their device access credentials, was disclosed to the investigation team, but this does not fulfil any of the requirements required by the DPA 2018.
[11] s57 DPA 2018

principles in an effective manner, and to integrate the safeguards necessary for that purpose into the processing itself.

The investigation team were unable to fully investigate the technologies in use by the PSNI, noting the importance of understanding the specific characteristics of particular implementations. However, the investigation team noted the following:

- The absence of specific internal policy and process documentation;
- In the majority of cases, the default of extracting from devices as much data is available; and
- A lack of privacy information.

When considered as a whole, this provides sufficient grounds to conclude that the PSNI did not design its MPE operations with data protection as a significant consideration.

2.6 Logging

Organisations have an obligation to maintain logs of processing operations[12], including the:

- collection;
- alteration;
- consultation;
- disclosure;
- combination; and
- erasure

of data.

We saw evidence that the PSNI portal system logs user actions relating to the data extracted from digital devices. This indicates some level of compliance. However, it was beyond the investigation's scope to examine whether the PSNI logs activities in circumstances where the extracted data is being processed further in other technical environments.

We remind the PSNI of the requirement[13] for controllers to maintain logs that they can make available to the Information Commissioner on request.

2.7 Data protection impact assessments

Organisations are required to undertake a data protection impact assessment (DPIA) when designing processing that might result in a high risk to

[12] s62 DPA 2018
[13] s62(5) DPA 2018

the rights and freedoms of individuals[14]. This is particularly important in the case of MPE, due to the likelihood of sensitive processing and the intrusion of a nature likely to impact on the rights that Article 8 ECHR provides. The organisation must carry out and document the assessment prior to any processing taking place.

The PSNI does not currently have a DPIA in place, but the organisation is developing one.

We are significantly concerned about:

- the absence of a clear articulation of the nature of the processing;
- the lack of evaluation of the risks associated with it; and
- missing documentation of the safeguards that mitigate the risks.

It signifies that the PSNI has, to date, failed to demonstrate that it has considered the impact of its processing activities in this area. The organisation has also not documented how the processing is in compliance with data protection legislation.

[14] s64 DPA 2018

3. Key findings and recommendations

It is clear from the assessment this report sets out that there are a number of areas in which the PSNI currently falls significantly short of the requirements set out in the DPA 2018.

The ICO has significant concerns regarding how processing is taking place and how this impacts on the privacy and data protection rights of people in Northern Ireland. The lack of a clearly articulated legal basis for the processing represents a fundamental principle which the PSNI is currently not observing. Basic data protection documentation is not available, leading to a lack of clarity for those affected by the processing and a lack of evidence that the PSNI is considering privacy and information rights.

However, the ICO acknowledges and is reassured by the candour of senior leaders within the PSNI who self-identified and openly declared their own concerns during the investigative engagement with ICO investigators. They indicated that they had plans in place, overseen by a senior officer, to address a number of concerns that they felt this report would raise.

The PSNI benefits from being able to learn from the substantial amount of work taking place across the UK following the publication of the ICO's England and Wales. The majority of this is directly relevant to Northern Ireland. We therefore encourage the PSNI to collaborate with those organisations leading work in other jurisdictions, so that they can both feed into and (to the greatest extent possible) implement the outputs from their work.

In particular, as a member of the NPCC, the PSNI should benefit from the NPCC-led work on the provision of privacy information through its digital processing notices and associated guidance.

Also, whilst the PSNI does not usually come under the auspices of the College of Policing guidance[15], it would significantly benefit from reviewing the Authorised Professional Practice (APP) and preparing similar guidance for use in Northern Ireland. This would assist in providing consistent standards of compliance with data protection legislation and respect for the information rights of citizens regardless of where they are in the UK.

3.1 Data protection impact assessment

The PSNI does not have a current DPIA in place for its MPE operations. S62 DPA 2018 requires controllers to carry out a DPIA prior to commencing

[15] The College of Policing is the professional body for those who work in police forces in England and Wales, and it produces Authorised Professional Practice for those forces.

processing that is likely to result in a high risk to the rights and freedoms of individuals. Whilst the PSNI is already carrying out the processing in question, it should remedy the absence of a DPIA at the earliest opportunity. The DPIA should cover all aspects of MPE, including the core activities (carried out internally by the CCC, the CSU or contracted to the FSNI) and use of in-field mobile equipment. In addition to complying with the legislative requirement, this should assist the organisation in clearly setting out the lawful basis for the processing and demonstrating consideration and mitigation of all relevant risks to the greatest extent possible.

Recommendation 1

The PSNI should urgently undertake a data protection impact assessment (DPIA) that covers all of the MPE activity it carries out, as per the requirement of s62 DPA 2018.

The organisation should keep the DPIA under regular review and update it prior to any further innovation or procurement in MPE capability.

3.2 Lawful basis

Following engagement subsequent to the England and Wales report and the Court of Appeal (Criminal Division) judgment in relation to Bater-James & Anor v R [2020] EWCA Crim 790, the NPCC accepted that consent, per s35(2)(a) DPA 2018, is not an appropriate lawful basis for processing data from mobile devices.

When MPE takes place, there is a high likelihood that it processes sensitive personal data, and police should proceed on that basis. The law requires that this type of processing needs to meet a higher threshold of strict necessity. The processing is permitted only if:

> "(a) the processing is strictly necessary for the law enforcement purpose,
>
> (b) the processing meets at least one of the conditions in Schedule 8, and
>
> (c) at the time when the processing is carried out, the controller has an appropriate policy document in place."[16]

[16] s35(5) DPA 2018

The investigation found that the PSNI was not evidencing that it was meeting these conditions in processing data from mobile phones, for the following reasons:

- The absence of a DPIA or privacy information containing explicit statements around the lawful basis they were relying on.
- The response provided to the investigation team that it processes complainants' and witnesses' devices on the basis of consent, which would not be an appropriate basis.
- The default position of extracting all available data from devices.

Recommendation 2

The PSNI should review the lawful basis it relies on for conducting MPE, taking 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. It should ensure that all business processes and documentation are consistent with the findings of the review.

When considering this recommendation, the PSNI should engage with and have regard to the work the NPCC is undertaking in relation to recommendation 2 of the England and Wales report.

3.3 Excessive processing

Taking account of the s37 DPA 2018 requirement for data to be adequate, relevant and not excessive, the PSNI's 'blanket' policy of extracting all available data from devices is unlikely to comply with data protection legislation, given the nature of the data on such devices and the wide range of data subjects it impacts. This concern is compounded by the lack of systematic management of retained data or processes to delete non-relevant data.

This leaves people unsure of their rights and is likely to contribute to further attrition in engagement with the criminal justice system.

Recommendation 3

The PSNI should review its policy and produce operational guidance that ensures:

- investigators only seek to acquire digital data in circumstances when they determine that less intrusive means are not sufficient to satisfy the reasonable line of enquiry;
- approach oversight and approval processes are in operation; and

- investigators acquire only the minimum data strictly necessary.

It should modify internal systems to be supportive of the guidance and log all relevant decisions and processing operations.

The organisation should put training in place to ensure that all officers and staff are aware of the operational guidance and are clear about their personal obligations.

It should review the Authorised Professional Practice produced by the College of Policing for police in England and Wales, and prepare similar guidance for use in Northern Ireland.

3.4 Privacy information

There is an absence of standard information required by s44 DPA 2018 that officers provide to people whose devices the PSNI takes for examination. This leaves people unsure of their rights and is likely to contribute to further attrition in engagement with the criminal justice system.

Recommendation 4

The PSNI should review its published privacy information and the information it provides to people when acquiring their device. The organisation should ensure it supplements this with information relating to processing as a result of MPE, including information on privacy and information rights.

When considering this recommendation, the PSNI should engage with and adopt the work the NPCC is undertaking in relation to digital processing notices, as a response to recommendation 2 of the England and Wales report.

3.5 Data management

The investigation found a lack of rigour in managing the personal data the PSNI acquires through MPE. In particular, there is little evidence of the regular review and, where appropriate, deletion of data once there is no longer a lawful justification for its retention, in accordance with s39 DPA 2018.

Recommendation 5

The PSNI should update its data retention policy to include the specifics of managing data it acquires through MPE, consistent with s39 DPA 2018, and operationalise:

- regular reviews and deletion of data if it cannot justify ongoing retention; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that it is not processed further and so officers cannot inappropriately access, review or disseminate the data.

3.6 Consistency of approach

Each Chief Constable is accountable for the processing that takes place within their organisation, as a competent authority under the DPA 2018. However, there are clear benefits to adopting consistent standards in policing across the UK, to the greatest extent possible. This approach is likely to increase public confidence in engaging with the police and the public's understanding of the police's resulting actions.

Recommendation 6

As far as legislative differences and devolved administration factors allow, the PSNI should engage with work the UK Government, the NPCC and the College of Policing are undertaking. This work includes:

- the statutory power and code of practice being introduced through the Police, Crime, Sentencing and Courts Bill;
- police guidance on the considerations and processes involved in MPE; and
- privacy information officers provide to people whose devices are taken for examination.

3.7 Standards and accreditation

The investigation found that PSNI was yet meet the requirement of the Forensic Science Regulator to achieve certification to the ISO/IEC17025 international laboratory standard. This means that there is a lack of confidence in the integrity (and hence accuracy) of the data extracted from devices.

Recommendation 7

In order to provide assurance around the integrity of the data extraction processes, the PSNI should accelerate its work to implement and maintain the standards set out in the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

4. Conclusions

The unjustified use of MPE or failure to fully explain why it is being used can significantly impact the confidence of victims and witnesses to report crime and to sustain engagement with the criminal justice process. We are not questioning the value of MPE as an essential tool in combatting crime, but it is essential that the police conduct any such operations in compliance with data protection legislation to ensure they are lawful and fair.

This investigation found that the PSNI has a number of areas in which it needs to have greater consideration of data protection and privacy issues.

Senior PSNI leaders reassured the ICO investigation team that they were familiar with the ICO's England and Wales report and understood the judgment in the Court of Appeal case of Bater-James & Anor v R [2020] EWCA Crim 790[17]. Having now engaged directly with ICO investigators, they indicated they are committed to a change in culture in the organisation and have already started making improvements.

Whilst this report makes a number of recommendations that apply specifically to the PSNI, we make them at a time when there is considerable activity taking place across the UK to address the findings of:

- the ICO's England and Wales report[18];
- a discontinued judicial review[19]; and
- the recently published Attorney General's Guidelines on Disclosure[20] and CPIA Code[21].

All of these developmental activities are directly relevant to considerations in Northern Ireland. We therefore encourage the PSNI to engage with NPCC colleagues and the College of Policing to ensure an efficient and consistent response.

---

[17] http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html
[18] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[19] A claim for judicial review was established on behalf of two women who had reported rape to the police and were claiming that the downloading of the whole of their personal digital data was not relevant to the allegations they had made.
[20] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946082/Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf
[21] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf

The ICO is committed to assisting stakeholders in understanding these recommendations and would be very happy to continue engagement with the PSNI and others in ensuring they embed the necessary changes into practice.

List of abbreviations

APP ..... Authorised Professional Practice

CCC ..... Cyber Crime Centre

CSU ..... Cyber Support Unit

CPIA ..... Criminal Procedure and Investigations Act 1996

DPA 2018 ..... Data Protection Act 2018

DPIA ..... Data protection impact assessment

ECHR ..... European Convention on Human Rights

FSNI ..... Forensic Science Northern Ireland

GDPR ..... General Data Protection Regulation 2018 (now UK GDPR)

HRA ..... Human Rights Act 1998

ICO ..... Information Commissioner's Office

IPA ..... Investigatory Powers Act 2016

MPE ..... Mobile phone (data) extraction

NPCC ..... National Police Chiefs' Council

OIC ..... Officer in charge

PPB ..... Public Protection Branch

PSNI ..... Police Service of Northern Ireland

S ..... Section (when referring to a section number within an Act)

UK GDPR ..... UK General Data Protection Regulation 2018