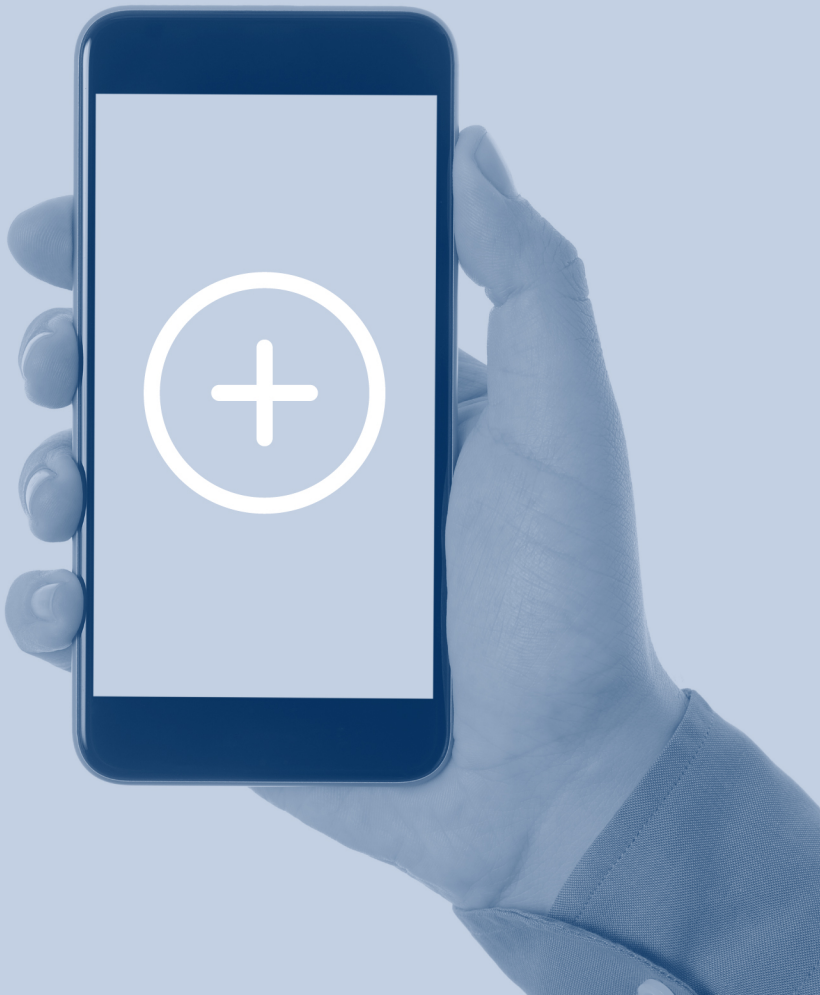
Mobile phone data extraction by police forces in England and Wales

An update on our findings

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.

The report broke new ground. It called for a change in culture to stop unnecessary processing of personal data from mobile phones where it is not fully justified. It is not okay for police forces to ask people to hand over their mobile phones without a good cause. They must only take people's data when it is strictly necessary for a specific, reasonable line of enquiry.

It has had a transformational impact. The Court of Appeal issued a judgment that reinforced our report's findings and recommendations. The Attorney General has revised his guidelines on disclosure, stressing the message that it is not always necessary to obtain digital materials. And the College of Policing has issued operational guidance to police forces, emphasising the need to consider alternatives to the examination of mobile phones and to extract only the minimum amount of data strictly necessary.

Further work is needed.

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

That investigation shows a fragmented response to my 2020 report. The need for reform is widely recognised, but the operational changes required are still to take place, and there is a lack of national coordination. I have continued to press

the case with stakeholders for the code of practice I called for in 2020, to improve current practice and build in adequate safeguards.

Despite our efforts, this is yet to be actioned.

This report is published alongside reports covering my office's findings in Northern Ireland and in Scotland. The ICO continues to support police forces and prosecutors to understand and implement the changes required. We are encouraged by the consensus across the UK regions that action is needed, but more progress is needed.

People are right to expect that police forces will treat their personal information fairly, transparently, and lawfully, and that only data that is necessary will be taken. The ICO will continue to engage with those responsible for these critical changes, and push for an urgent change in culture.

Elizabeth Denham CBE
UK Information Commissioner

Contents

Executive summary

In June 2020, the Information Commissioner's Office (ICO) reported on its investigation into mobile phone extraction (MPE) by police forces in England and Wales when conducting criminal investigations. That report made a number of wide-ranging recommendations.

The report, along with the Court of Appeal judgment in Bater-James & Anor v R [2020] EWCA Crim 790, began work to reform how police forces consider the extent to which they need to obtain digital data from mobile phones.

The significant risks associated with highly intrusive processing of intimate data from mobile phones are now widely accepted. Consequently, police forces should only do this type of processing after considering other, more privacy-friendly, means of achieving the same investigative objective. In data protection legislation, this means that police forces must demonstrate strict necessity (with other associated conditions) for such processing to be lawful.

Recent changes to the Attorney General's Guidelines on Disclosure, and the Criminal Procedure and Investigations Act 1996 Code of Practice, recognise the need for better engagement between organisations involved in the criminal justice system. This assists police forces in being more specific about their requirements for digital materials.

More recently, the ICO completed its investigation into MPE by looking into practices in Northern Ireland and Scotland. We are publishing our findings alongside this report. Both reports make specific recommendations to police in those devolved administrations.

It is clear that our June 2020 report made a significant impact, with many stakeholders across the criminal justice landscape acknowledging the need for significant change. New legislation is being introduced and there have been significant judicial findings alongside changes to national guidance. However, this is just the start. Legislation needs to have safeguards written into it, police forces need to adopt appropriate processes and procedures and roll out training that fosters behaviours to reflect these changes. These reforms to MPE are required to safeguard the information rights and privacy of citizens, regardless of whether a device belongs to a complainant, a witness or a suspect.

Leaders in criminal justice organisations across the UK still have a significant amount of work to do, in order to achieve this fundamental change in approach. This is essential to ensure the public has confidence in the police's ability to process and manage data professionally and in compliance with data protection legislation.

It is vital that HM Government and the devolved administrations take an holistic view of the significant challenges that remain and set out comprehensive roadmaps to demonstrate how and by whom these are addressed.

Looking to the future, as broadband and mobile network bandwidth increases and cloud-based storage becomes more prevalent, new challenges emerge in relation to acquiring digital data in criminal investigations. Device users may not necessarily be aware of where their device stores their data, as it is not relevant to them. Organisations need to apply the same data protection considerations to off-device as on-device material. Practitioners need to do more work to apply the principles developed in this investigation to law enforcement processing of personal data accessed through digital devices but stored elsewhere.

1. Introduction

1.1 Background

In June 2020, the Information Commissioner's Office (ICO) published a report[1] following its investigation into how police forces in England and Wales use mobile phone extraction (MPE) in the context of criminal investigations. In this update report, we refer to the previous publication as "our June 2020 report".

The report made 13 recommendations relating to work required to improve the consistency of the police forces' approach in those areas. It contained a commitment from the Information Commissioner to work with police, government and criminal justice organisations to develop their understanding of the investigative findings and to implement measures to address these. It also contained a commitment to examine and report on MPE practices in the devolved administrations of Northern Ireland and Scotland.

This report reflects on the impact of our June 2020 report and the consequential developments. It also takes into account our investigative findings in Northern Ireland and Scotland that we are publishing alongside this report. Following publication of our June 2020 report, ICO officers gained a significant amount of detailed insight through engagement with a wide range of stakeholder groups. This report draws upon the benefit gained from that work.

1.2 The nature of mobile phones and digital materials

Our June 2020 report set out in detail a number of the characteristics of modern mobile phones and the material they commonly hold. We summarise these below.

First, many people consider themselves inseparable from their mobile phones and conduct the majority of their daily lives online. This means that a substantial body of material relating to finances, relationships, intimate feelings and many other areas builds up on the device and is available for scrutiny when extracted or otherwise interrogated.

The data a device contains does not just relate to the device's regular user; it often has personal data relating to many other people. These 'third parties' have the same rights under privacy and data protection legislation as those directly involved in the investigation. Their data may be as simple as basic contact details (eg one or more telephone numbers or email addresses). However, it may also relate to what they may reasonably believe were private, possibly

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

intimate, communications with the device's user. Amongst other things, these may be:

- text messages;
- images;
- audio files; or
- videos.

Another important characteristic of a mobile phone is that it is often generating and storing data of its own volition, without the knowledge of its user. Data such as:

- location history;
- browsing history;
- cookies; and
- usage of apps

is often being generated but is not readily visible to the user.

An overarching, central point to the ICO's position on MPE is that the data a mobile phone holds cannot simply be 'given away' to a controller (in this case a law enforcement agency) by the device owner. Police forces need a good cause, based in law, to do this, as it includes data about other people and not just the device owner.

As a consequence, the practice of MPE needs controls that apply in order to protect the information rights and privacy of citizens. They need to apply regardless of whether a device is taken from a complainant, a witness or a suspect.

1.3 Processing data from mobile phones lawfully

Our June 2020 report set out a framework for the consideration of MPE. It includes two distinct but mutually dependent activities, which are:

- the acquisition of the device; and
- processing data from the device.

The means by which police forces may legitimately acquire devices vary in detail across the UK. There are a range of statutory and common law powers enabling officers to seize or take possession of devices where they reasonably believe they are of evidential value.

When considering the circumstances of a case, it may be appropriate to adopt a consensual approach to acquiring the device, by asking a person to co-operate with the investigation and be willing to allow someone to examine their device. Police do not have to use statutory powers in such circumstances.

However, a person's willingness to offer their device for examination is not, in itself, a sufficient lawful basis for processing information from it.

Processing of personal data for law enforcement purposes comes under Part 3 of the Data Protection Act 2018 (DPA 2018)[2]. This sets out the conditions required for lawful and fair processing.

The DPA 2018 sets out six principles that apply to all processing for law enforcement purposes. In summary:

- First principle: The processing must be lawful and fair.
- Second principle: The processing must be limited to a specified, explicit and legitimate purpose, and it must not be processed in a manner that is incompatible with the purpose for which it was collected.
- Third principle: The data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Fourth principle: The data must be accurate and, where necessary, kept up to date. 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. In addition, as far as possible, a clear distinction must be made between different categories of individuals – those suspected of an offence, those convicted, witnesses and complainants. Personal data based on fact must, as far as possible, be distinguished from personal data based on personal assessments.
- Fifth principle: Data should be stored for no longer than is necessary, and appropriate limits must be set for periodic review of the need for continued storage.
- Sixth principle: There must be 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.

In addition, other relevant requirements for law enforcement processing include the need for controllers to:

- provide privacy information that helps people understand how their data is being processed[3];
- implement data protection by design and default[4];
- keep logs of processing operations[5]; and

[2] https://www.legislation.gov.uk/ukpga/2018/12/part/3
[3] s44(1)&(2) DPA 2018
[4] s57 DPA 2018
[5] s62 DPA 2018

- carry out data protection impact assessments (DPIAs)[6], where there is likely to be a high risk to the rights and freedoms of individuals.

Our June 2020 report provides further explanation and analysis of these general principles and requirements.

In particular, our investigation analysed the conditions associated with the first principle (ie that processing must be lawful and fair). Our report set out why the first of the two possible conditions (namely a device owner's consent) is, in itself, not an appropriate foundation for MPE. We concluded that, in order to lawfully process the type of sensitive data found on mobile phones, it is necessary for police forces to demonstrate that the 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, and
>
> (c) at the time when the processing is carried out, the controller has an appropriate policy document in place."[7]

Police forces may consider the relevant basis in law to be the statutory obligation placed on investigators by the Criminal Procedure and Investigations Act 1996 (CPIA) and its Code of Practice to:

> "pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances."[8]

In order to demonstrate strict necessity (condition (a) above), the investigator needs to demonstrate how, based on a specific and reasonable line of enquiry, they considered other (less intrusive) means of fulfilling the line of enquiry and that obtaining specific data from a particular device remains necessary.

Schedule 8 of the DPA 2018 (in condition (b) above) sets out a range of conditions. Police forces must meet at least one of these conditions in order for the sensitive processing to take place. The first of these may be applicable in relation to investigators undertaking their statutory duties under the CPIA, if the processing:

---

[6] s64 DPA 2018
[7] s35(5) DPA 2018
[8] para 3.5 CPIA Code of Practice 2020

> "(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
>
> (b) is necessary for reasons of substantial public interest."[9]

Finally, for any sensitive processing to take place under Part 3 of the DPA 2018 (condition (c) above), organisations must have an appropriate policy document in place. Organisations can find the full requirements of this document at s42 DPA 2018.

[9] Schedule 8(1) DPA 2018

2. Investigative findings and recommendations

The ICO investigation revealed a complex legislative framework around MPE, involving criminal justice and data protection law. As a consequence, the approaches police forces took to MPE across England and Wales were inconsistent.

In particular, the investigation called for a new statutory code to assist practitioners with compliance with the law, and to provide citizens with clarity and foreseeability of the law so that they could be confident their rights were being properly respected. This was the investigation's most significant recommendation.

Police forces need to fully respect the requirements associated with sensitive processing for law enforcement purposes. They should issue new documentation that reflects their revised approach.

In many cases, the lawful basis for the processing was not set out in a way that demonstrated compliance with data protection legislation. In particular, obtaining data solely with the device owner's consent is not a valid lawful basis.

Furthermore, the amount of data processed could not, in many cases, be justified even when the basis for obtaining the data was justifiable. This can lead to unnecessary intrusion into the lives of device owners and others whose data may be stored on the device.

Therefore, police forces need to introduce new, consistent standards for the authorisation of obtaining, interrogation and retention of mobile phone data.

The investigation found a low rate of compliance with the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system. The relevant police forces and other organisations must accelerate their work to ensure they meet the relevant standards for accreditation.

Many police forces do not have effective mechanisms in place to adequately manage the significant volumes of data they have, including the legislative requirement to periodically review and delete material. This particularly applies to data that police acquire through device examination but that is not relevant to investigations. As a matter of urgency, police forces need to implement suitable policies and procedures.

The engagement between prosecution and defence requires improvements to better define reasonable lines of enquiry earlier in investigations. This would help to better target enquiries and limit the amount of data required.

Police forces need to improve the quality of engagement with, and information given to, people whose phones are being examined. This helps citizens to fully understand what their rights are and what is happening to the data taken from their devices. Such an improvement is critical to improving public confidence in coming forward to report crimes and co-operate with investigations.

There was a lack of understanding of MPE's complexities across different forces. We recommend establishing a national standard for training that emphasises the legislative requirements and respects the requirement to minimise privacy intrusion.

The investigation found that the technology the police forces were using was not, in general, designed with privacy in mind. At their core, future technology projects must consider data protection issues and privacy by design and default principles.

It was clear that a number of police forces undertook technological innovation to introduce MPE technology without properly engaging with their data protection officer and without undertaking data protection impact assessments (DPIAs). This engagement and evaluation is essential going forward.

Finally, the upcoming revisions to legislation and statutory instruments should incorporate, at their core, considerations of privacy and data protection.

For ease of reference, we provide the complete text of the recommendations from our June 2020 report at Annex A.

3. Recent developments

3.1 UK General Data Protection Regulation

On 31 December 2020, at the end of the transition period following UK's exit from the European Union, the GDPR ceased to apply to UK processing. The Regulation was then implemented in UK law as the "UK GDPR". There were minor changes in this transition related to aligning UK GDPR with DPA 2018, but those aspects of the GDPR which related to MPE (eg conditions relating to consent) remain unchanged. Therefore, as the processing we are considering here relates to law enforcement processing under Part 3 of the DPA 2018, there are no material changes of relevance to MPE practice.

3.2 Court of Appeal judgment

The Court of Appeal (Criminal Division) judgment in relation to Bater-James & Anor v R [2020] EWCA Crim 790[10] has significant relevance to MPE.

The Court considered four issues of principle, the first of which was:

> "The First Issue of Principle: Identifying the circumstances when it is necessary for investigators to seek details of a witness's digital communications. These are usually, but by no means always, electronic exchanges conducted by way of multiple platforms on smart mobile telephones, tablets or computers. These platforms are so numerous that it is pointless to attempt to list examples. In essence, the question in this context is when does it become necessary to attempt to review a witness's digitally stored communications? The linked question is when is it necessary to disclose digital communications to which the investigators have access?"

The Court found that there is "no obligation on investigators to seek to review a witness's digital material without good cause"[11]. It also said there must be a proper basis, usually based on a reasonable line of enquiry, that would it would reveal relevant material. 'Fishing expeditions' are not appropriate.

Police forces must not examine digital devices simply because that forensic technique exists and they can conveniently execute it. "There is no presumption that a complainant's mobile telephone or other devices should be inspected,

[10] http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html
[11] Para 67 Bater-James & Anor v R [2020] EWCA Crim 790

retained or downloaded, any more than there is a presumption that investigators will attempt to look through material held in hard copy."[12]

The judgment reiterates the point that complainants do not waive their right to privacy under Article 8 of the ECHR. Therefore, it is only necessary to disclose that material which is reasonably capable of undermining or assisting the case for the accused.

The second issue the Court considered was:

> "The Second Issue of Principle: When it is necessary, how should the review of the witness's electronic communications be conducted?"

The Court of Appeal found that police forces must consider whether it is actually necessary to obtain the material required from a complainant's device. If it is, they also need to consider whether it is sufficient simply to view limited areas (eg particular messages or images). Wherever possible, they should use alternatives to data extraction (eg taking screenshots or making some other record) without taking possession of the device. If more extensive enquiries are necessary, police should examine the device and extract the data with the minimum of inconvenience to the complainant. They should also return the device without unnecessary delay. Forces can use incremental searching where there are large volumes of data, and the defendant should participate in this process. Finally, to avoid revealing irrelevant personal information, police should make appropriate redactions to any disclosed material.

The third issue the Court considered was:

> "The Third Issue of Principle: What reassurance should be provided to the complainant as to ambit of the review and the circumstances of any disclosure of material that is relevant to the case?"

The judgment set a range of things that the police should tell the complainant, including:

- that they would be kept informed as to decisions made about disclosure, including how long the investigators keep the device, what the police plan to extract from it and what the police examine with a view to disclosure;
- that the police would only copy or inspect any content within the device if there is no other appropriate method of discharging the prosecution's disclosure obligations; and
- the police would only provide material to the defence if it meets the strict test for disclosure, and they would serve it in a suitably redacted form so

[12] Para 77 Bater-James & Anor v R [2020] EWCA Crim 790

as to not unnecessarily reveal personal details or other irrelevant information (eg photographs, addresses or full telephone numbers).

The fourth issue the Court considered was:

> "The Fourth Issue of Principle: What is the consequence if the complainant refuses to permit access to a potentially relevant device, either by way of "downloading" the contents (in reality, copying) or permitting an officer to view parts of the device (including, *inter alia*, copying some material, for instance by taking "screen shots")? Similarly, what are the consequences if the complainant deletes relevant material?"

It is a matter for the court to consider the circumstances relating to, and implications of, a complainant refusing access to digital materials or deliberately deleting them. However, it is important that investigators explain to complainants and witnesses the procedure that the investigation follows (as above). They should also make them aware of the consequences of any decision not to allow access to the requested digital materials.

The judgment states:

> "It is important to note that a refusal by a complainant or a witness to divulge the contents of a mobile telephone or similar device clearly does not, without more, constitute bad faith or misbehaviour on the part of the police or the prosecutor."[13]

It asserts the importance of understanding any reasons for such a refusal and consideration, by the court, of the adequacy of the trial process in the absence of the device's material.

3.3 Judicial review

At the time of writing our June 2020 report, the Centre for Women's Justice (CWJ) was pursuing a judicial review, funded by the Equality and Human Rights Commission, on behalf of two women who had reported rape to the police. The women were claiming that downloading all of their personal digital data was not relevant to their allegations. The CWJ was concerned about intrusive requests for access to digital devices and the effect of these in deterring victims from pursuing allegations.

The case was settled following the publication of our June 2020 report and the Bater-James Court of Appeal judgment. As part of the settlement, the National Police Chiefs' Council (NPCC) agreed to withdraw the training materials

[13] Para 96 Bater-James & Anor v R [2020] EWCA Crim 790

("Obtaining data from digital devices during the course of an investigation") and replace the "Digital Processing Notice" that was circulated to all forces[14].

3.4 Attorney General's Guidelines on Disclosure

The Attorney General issues Guidelines for investigators, prosecutors and defence practitioners on the application of the disclosure regime contained in the Criminal Procedure and Investigations Act 1996 Code of Practice ("CPIA code").

Recommendation 13 of our June 2020 report stated:

> "Revisions to […] the Attorney General's Guidelines on Disclosure, and the Criminal Procedure and Investigations Act 1996 Code of Practice should ensure that data protection and privacy concerns are fully considered and incorporated, given their importance in a functioning criminal justice system."

The ICO issued a response[15] to a public consultation on revisions to the Guidelines and CPIA Code. This response, along with our June 2020 report, influenced the Government's review of these statutory publications.

The revised Guidelines replace the existing Attorney General's Guidelines on Disclosure issued in 2013. They now incorporate what were formerly the Supplementary Guidelines on Digital Material, also issued in 2013.

They place greater emphasis on the determination of reasonable lines of enquiry through early engagement between investigators, prosecution and defence. They also promote meaningful engagement with victims and witnesses.

The Guidelines are now clearer as to the importance of an objective assessment of whether investigators believe a device holds relevant material. They also provide more explicit recognition of the need to avoid 'fishing expeditions' into a complainant's personal life and devices.

The revised Attorney General's Guidelines on Disclosure[16] and CPIA Code[17] came into force on 31 December 2020. Whilst they apply directly to England and Wales, the principles in relation to the acquisition of digital materials are relevant across the UK.

---

[14] https://news.npcc.police.uk/releases/police-replace-processing-notice-used-to-obtain-agreement-from-victims-and-witnesses-to-search-for-relevant-material-on-digital-devices
[15] https://ico.org.uk/about-the-ico/consultations/attorney-generals-consultation-on-guidelines-on-disclosure-and-the-cpia-code-of-practice/
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946082/Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf
[17] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf

3.5 Code of Practice for Victims of Crime

The Code of Practice for Victims of Crime (the Victims' Code) is a statutory government document which sets out the minimum level of services that victims of crime in England and Wales should receive from criminal justice agencies and other organisations. It enables victims to receive the information they need about their case, the criminal justice system and the support services available. This assists them to navigate the justice process, understand their rights and make their own informed decisions about what services to access.

Following a period of public consultation, which the ICO contributed to[18], the Government published its response[19] and laid a revised Code before Parliament. It came into force on 1 April 2021.

Recommendation 13 of our June 2020 report stated:

> "Revisions to the Victims' Code […] should ensure that data protection and privacy concerns are fully considered and incorporated, given their importance in a functioning criminal justice system."

However, the revised Code did not address our points in the consultation response relating to data protection and privacy. Concerns remain that police forces pay insufficient attention to clearly explaining to victims what their information rights are and how they should expect the police to handle their data.

At the time of writing this report, the Ministry of Justice is working with criminal justice organisations to produce a memorandum of understanding (MoU). This would explain how they should collaborate to fulfil their duties in practice. It is essential that those organisations providing services to victims clearly explain their obligations to respecting the privacy of victims and others. The ICO is working with the Ministry of Justice to provide constructive input into this MoU and additional guidance to ensure that organisations fully understand their obligations when handling victims' personal data.

3.6 National guidance

As a result of our June 2020 report, the Bater-James judgment and the judicial review challenge, the NPCC withdrew its training materials and public-facing forms. Since then, it worked on revisions to the digital processing notice (DPN) forms and associated guidance.

---

[18] https://ico.org.uk/about-the-ico/consultations/ministry-of-justice-consultation-consultation-on-improving-the-victims-code/

[19] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/936059/improving-victims-code-consultation-govt-response.pdf

In November 2020, the NPCC published[20] a new, interim DPN and associated guidance for officers. By its own admission, the NPCC's publication falls short of addressing the full scale of the ICO's recommendations, and the investigation team is continuing to engage with the NPCC on further drafts.

The College of Policing issues Authorised Professional Practice (APP), which police forces in England and Wales expect their officers and staff to follow when discharging their responsibilities. In May 2021, the College published APP relating to "Extraction of material from digital devices"[21].

The APP sets out ten principles that police forces must observe in order to be fair and lawful in their MPE operations. It helpfully distinguishes between "informed agreement" of device users to surrender their device to the police, as opposed to "consent" as a lawful basis for processing. It is also supportive of the ICO's findings in reinforcing the requirement for police forces to base the need to obtain digital data on strict necessity in relation to a reasonable line of enquiry.

The ICO welcomes the introduction of this APP and the immediate adoption of its principles. We have further recommended, in our separate reports into MPE in Northern Ireland and Scotland, that the respective policing organisations use this APP as the basis for producing equivalent guidance.

3.7 The Police, Crime, Sentencing and Courts Bill

The Police, Crime, Sentencing and Courts Bill[22] was introduced to Parliament in March 2021. The Bill provides new statutory powers which permit investigators to lawfully examine mobile phones which their regular user has voluntarily provided.

The Bill also makes provision for the creation of a new Code of Practice. Investigators are required to have regard to this new code when exercising their new statutory power.

Whilst this development engages our June 2020 report's recommendation for a statutory code and for clarity around application of the Investigatory Powers Act 2016 (IPA), there are significant risks associated with this Bill. Consequently, it requires close scrutiny.

First, the powers avoid due consideration of the IPA's applicability. They provide a route that avoids the protections that the Act affords to third parties, and effectively disarms those protections. It is therefore essential that the Bill contains adequate considerations around privacy and data protection, either

[20] https://news.npcc.police.uk/releases/police-replace-processing-notice-used-to-obtain-agreement-from-victims-and-witnesses-to-search-for-relevant-material-on-digital-devices
[21] https://www.app.college.police.uk/app-content/extraction-of-material-from-digital-devices
[22] https://bills.parliament.uk/bills/2839/

through amendments to the primary legislation or via the associated Code of Practice.

Also, the Bill as drafted states that the new code only applies in the exercise of the new powers, rather than whenever police forces undertake MPE. This would not address the most significant recommendation of our June 2020 report, that required a code that was applicable to all MPE and would in fact assist in selecting the appropriate power or adopting other approaches.

There is a risk the Bill simply adds to the existing set of powers available to police. It may also leave existing practice without the benefit of the additional oversight that the law would provide through the Bill or a code.

It is unclear how the Bill's proposed code, with its UK-wide scope, impacts on the College of Policing's APP for police forces in England and Wales. Those considering the development and implementation of products and processes need to fully understand the context within which they would use them.

The Secretary of State is required to consult the Information Commissioner in developing the code that the Bill requires. This provides an opportunity for the ICO to help shape its development and ensure that the code makes appropriate progress in addressing the most significant recommendation from our June 2020 report.

We anticipate the Bill to gain Royal Assent in autumn 2021.

3.8 Dealing with legacy data

The NPCC is sponsoring a project, through its Transforming Forensics Programme, to co-ordinate a review of digital materials held by (or on behalf of) forces. Whilst this is a welcome initiative, its formation is an acknowledgement that (as found by our investigation) some police forces do not manage much of the material they obtain from analysing digital devices in accordance with the DPA 2018. It is clear that many forces are simply unaware of the nature and extent of the material they are holding, and this is a significant concern that they need to urgently address.

The ICO is providing advice to this vital project, which should aim to both capture lessons learned and put in place rigorous policy and procedures. These measures help to ensure that, going forward, police forces manage all data in accordance with the law. Timescales are currently unclear, and we remind Chief Constables that they are individually accountable for compliance with data protection legislation in their own forces. They should progress assessing what needs to be done without delay.

3.9 Local innovation

The ICO is aware that individual forces are capable of processing digital data in different ways, and some are currently considering changing how they deal with devices. Vendors offer products that allow officers to extract data from devices in the field, without the need for users to surrender their devices. These products can be very effective in taking specific evidence from a device, eg a video of someone committing a crime. However, officers could also use them to extract a much wider range of data.

Other equipment allows officers to rapidly scan (or 'triage') devices to see whether they contain material of interest, in order to determine whether to carry out data extraction. Officers can browse devices or search for particular material using keywords. Alternatively, they can use reference data sets as the basis for matching, eg known illegal images. Under proper governance, these techniques can be very effective. In other circumstances, they have the potential to be used for the type of 'fishing expedition' that the Bater-James and Anor judgment refers to.

Using triage techniques or in-field equipment could potentially increase the speed at which police can return a device to its user and reduce the requirement to extract data. However, it remains the case that officers are still processing personal data in such circumstances, and they must apply the same considerations of strict necessity for sensitive processing.

Organisations considering introducing new technology for examining digital materials or materially changing their existing processing must complete a DPIA before commencing the new processing.

3.10 Assessment of the developments

Our June 2020 report and the Court of Appeal judgment triggered a significant amount of development work. This reflects the distance between police forces' practices and compliance with the requirements of data protection legislation when engaging in MPE.

The ICO acknowledges the engagement and consultation that has taken place since the publication of our June 2020 report. Organisations have implemented a number of significant positive improvements in governance, not least the changes to the Attorney General's Guidelines.

However, much of the activity is well-meaning but is, by its very nature, tactical. It fails to address some of the most significant issues. It is understandable that the NPCC felt compelled to act quickly and modify its digital processing notices in light of the Bater-James and Anor judgment. However, doing so before resolving wider issues, such as the lawful basis for acquisition and processing, risked

compounding existing problems. Furthermore, it did not actually address many of the concerns that our June 2020 report noted.

The introduction of new statutory powers to permit data extraction from devices that complainants and witnesses use risks further embedding the existing poor practice we identified. It requires adequate safeguards, with a Code of Practice applicable to all situations where police forces may contemplate MPE.

Our investigation found that, prior to investigators acquiring any device or undertaking MPE, they should consider:

1. In the circumstances of the investigation, is the proposed line of enquiry reasonable and therefore necessary?
2. If yes, then are there means of fulfilling the line of enquiry without resorting to examining digital data?
3. If no, then are there specific devices which you believe store relevant material?
4. If yes, is it possible to acquire the material without resorting to data extraction?
5. If no, then is there a reasonable lawful means of acquiring the device(s)?
6. If yes, do the public interest benefits outweigh privacy concerns?
7. If yes, then engagement should take place with the device user and the minimum strictly necessary data set acquired.

The College of Policing APP is helpful in setting out principles to assist police officers and staff in England and Wales to understand their obligations. However, it is not clear whether equivalent guidance is being introduced in all parts of the UK. It is also not clear how the proposed new powers and, in particular, the statutory code of practice, may impact the APP.

It is clear that the experience of victims needs to improve so that complainants feel more confident that the police would respect their privacy rights the criminal justice process. However, our work reaches wider than the victim, and we are equally concerned with the privacy and information rights of every person whose data may be stored on the relevant device. The police themselves acknowledge that a significant majority of the data extracted from mobile devices is of no relevance to criminal investigations. Similarly, many forces do not have in place effective ways of handling these vast amounts of data in accordance with data processing legislation.

4. Conclusions and further work required

Using MPE in situations where it is not justified or fully explained has a significant impact on the confidence of both victims and witnesses to report crime and to sustain engagement through the criminal justice process. We are not questioning the value of MPE as an essential tool in the investigation and prosecution of crime. However, it is essential that police forces deploy the technique in compliance with data protection legislation, to ensure its use is lawful and fair.

A great deal of work needs to be urgently done to address a range of areas of significant non-compliance. Not all of the changes proposed at a national level are necessarily consistent with the cultural change the ICO and other stakeholders representing victims are calling for.

The ICO continues to engage with and assist those responsible for these important changes. Some of the tactical responses required sit logically within particular organisations or agencies. However, this is not the case with some of the more fundamental overarching issues.

They require a change in culture as a matter of urgency. They need a strategic, co-ordinated approach, involving action by all parties involved, to deliver this. The ICO welcomes the formation of a steering group, jointly chaired by the Home Office and the NPCC, which aims to provide this leadership. This group should adopt a programme-based approach and make public a time-based plan to address the response to the ICO's recommendations and other recent changes (including the Attorney General's Guidelines and the Court of Appeal judgment). This group should also drive the progress against this plan, ensuring the consistency of all products with the overarching aims.

The ICO recognises the scale and complexity of change that it requires, which encompasses the whole criminal justice system. Some changes to legislation and national guidance are underway that ultimately determine what needs to take place within individual police forces. However, forces should be looking to see what they can achieve now. At this stage, the ICO is continuing to engage, influence and encourage systemic change at a national level, but it would consider the use of enforcement powers with individual controllers where appropriate.

Finally, there is an emerging trend of individuals using a variety of digital devices which perform similar functions. It is not uncommon for desktop and laptop computers, tablets, mobile phones, smart watches and other voice-operated digital devices to offer similar functionality. In addition, the proliferation of smart 'internet of things' devices continues. With increasing availability of fixed and mobile broadband services, there is a trend to store the

type of data involved in MPE off-device ('in the cloud'). The user can access this data regardless of which device they happen to be using at the time.

From a privacy and data protection perspective, there is no difference between sensitive data a physical end-user device (such as a mobile phone) holds and that which is held elsewhere (for example in the cloud) but the user accesses via a digital device. As investigators recognise changing investigative opportunities, it is essential that those considering these challenges at a national level shift their focus from the physical device to the material itself. This helps to ensure that changes the forces implement are not quickly outdated.

List of abbreviations

AGO ..... Attorney General's Office

APP ..... Authorised Professional Practice

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

CPS ..... Crown Prosecution Service

DPA 2018 ..... Data Protection Act 2018

DPIA ..... Data protection impact assessment

ECHR ..... European Convention on Human Rights

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

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

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

Annex A – Previous recommendations

Recommendation 1

> "The Government should strengthen the current legislative framework by producing a statutory code or other equivalent measure to ensure the law is sufficiently clear and foreseeable. The following information, which is not exhaustive, should be set out with sufficient detail to ensure that interference with the rights of individuals is not arbitrary and is in accordance with the law:
>
> - under what circumstances mobile phone extraction is permitted and why (including for which categories of offence under investigation);
> - the options available for lawfully obtaining devices and examining their contents, including the circumstances in which consent or coercive powers should be used;
> - how lines of enquiry relate to requirements for mobile phone data;
> - which categories of individual are liable to have their mobile devices examined (eg suspects, witnesses, third parties);
> - the nature of the material to be examined;
> - the time limits on the period of examination; and
> - the procedure to be followed for authorising, examining, using and storing the data obtained."

Recommendation 2

> "Police forces should:
>
> - consider the lawful basis being relied upon to process personal data extracted from mobile phones (under Part 3 of the DPA 2018) to ensure compliance with all aspects of s35, in particular the requirements relating to sensitive processing;
> - consider the applicability of the Investigatory Powers Act 2016 in relation to their MPE practice; and
> - withdraw the existing NPCC advice and template documentation, and produce new materials that reflect the findings of this report."

Recommendation 3

> "Action is required (in line with the Attorney General's recommendations in his review of disclosure and the recent HMCPSI report) to reduce the excessive processing of personal data extracted by MPE at the outset of an investigation. Consistent standards for the authorisation of obtaining, interrogation and retention of mobile data

should be developed in conjunction with the Crown Prosecution Service and Attorney General's Office and implemented across England and Wales. These should include the requirement to keep records that detail:

- the line of enquiry being pursued;
- justification for the **strict necessity** and proportionality of the processing;
- the specific extraction/search/analysis to be undertaken;
- consideration of the level of collateral intrusion and steps taken to mitigate it;
- details of the senior officer providing authorisation; and
- confirmation that the action will be compliant with the relevant legislation.

In order to reduce excessive personal data being processed, this must be repeated for the initial and any subsequent actions in a phased approach."

Recommendation 4

"Police forces should complete their 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, in order to provide assurance around the integrity of the data extraction processes they use."

Recommendation 5

"Where data is extracted but not relevant to an investigation (eg because of limitations with the extraction technology or because the prosecuting authorities have initially asked for a broad range of data to be downloaded), there should be an agreed minimum standard in place that ensures such data:

- is not processed further;
- cannot be inappropriately accessed, reviewed or disseminated; and
- has clear retention and deletion policies in place.

Police forces should put in place appropriate independent oversight and governance of these arrangements."

Recommendation 6

"The Crown Prosecution Service should ensure that recommendations made by the Attorney General regarding early engagement between the prosecution and defence to determine reasonable lines of enquiry

> are fully embedded in operational practice. This will help to limit (where possible) the amount of personal data disclosed."

Recommendation 7

> "Police forces should review the retention and review periods for personal data extracted from mobile phones and introduce effective processes to ensure that personal data is not kept for longer than necessary, in compliance with s39 DPA 2018."

Recommendation 8

> "Police forces must engage effectively with, and provide detailed privacy information to, all individuals whose devices are to be subject to MPE, to ensure that they are fully informed about the processing of their data, in compliance with s44 DPA 2018. Mobile phone extraction is an intrusive activity and, as such, is a specific case where police forces should provide more detailed and meaningful privacy information to the individual, including their rights under data protection legislation. Where police find it appropriate to apply exemptions to the provision of information, they must comply fully with the requirements set out in s44(4)-(7) DPA 2018."

Recommendation 9

> "A national training standard for all aspects of mobile phone extraction activity should be considered for investigating officers and decision makers to ensure consistency of approach. Any training must include (but not be limited to) the requirements of data protection law with a view to minimising privacy intrusion where possible:
>
> - the lawful basis for processing (including sensitive processing);
> - the requirements of s44 DPA 2018;
> - the requirements of Chapter 2 Part 3 DPA 2018;
> - the requirements of HRA and the Investigatory Powers Act 2016;
> - the authorisation process for search and extraction and how this is strictly necessary, proportionate, justified and relevant to a reasonable line of enquiry; and
> - the recording of authorisation decisions."

Recommendation 10

> "Police forces should:
>
> - keep the software they use for mobile phone extraction under review;

- ensure they maintain a privacy by design and default approach; and
- build in privacy safeguards to any new procurement or upgrade."

Recommendation 11

"Chief Officers should ensure that Data Protection Officers are engaged in, and consulted on, any new projects involving the use of new technologies for processing personal data."

Recommendation 12

"Police forces should undertake data protection impact assessments (DPIAs) prior to the procurement or roll-out of new hardware or software for mobile phone extraction and processing, including any analytical capabilities, to ensure compliance with data protection requirements, where appropriate engaging the ICO consultation mechanism. In addition, they should carry out a review to ensure DPIAs exist for all relevant current processing and that they are up-to-date and compliant with DPA 2018 requirements."

Recommendation 13

"Revisions to the Victims' Code, the Attorney General's Guidelines on Disclosure, and the Criminal Procedure and Investigations Act 1996 Code of Practice should ensure that data protection and privacy concerns are fully considered and incorporated, given their importance in a functioning criminal justice system."