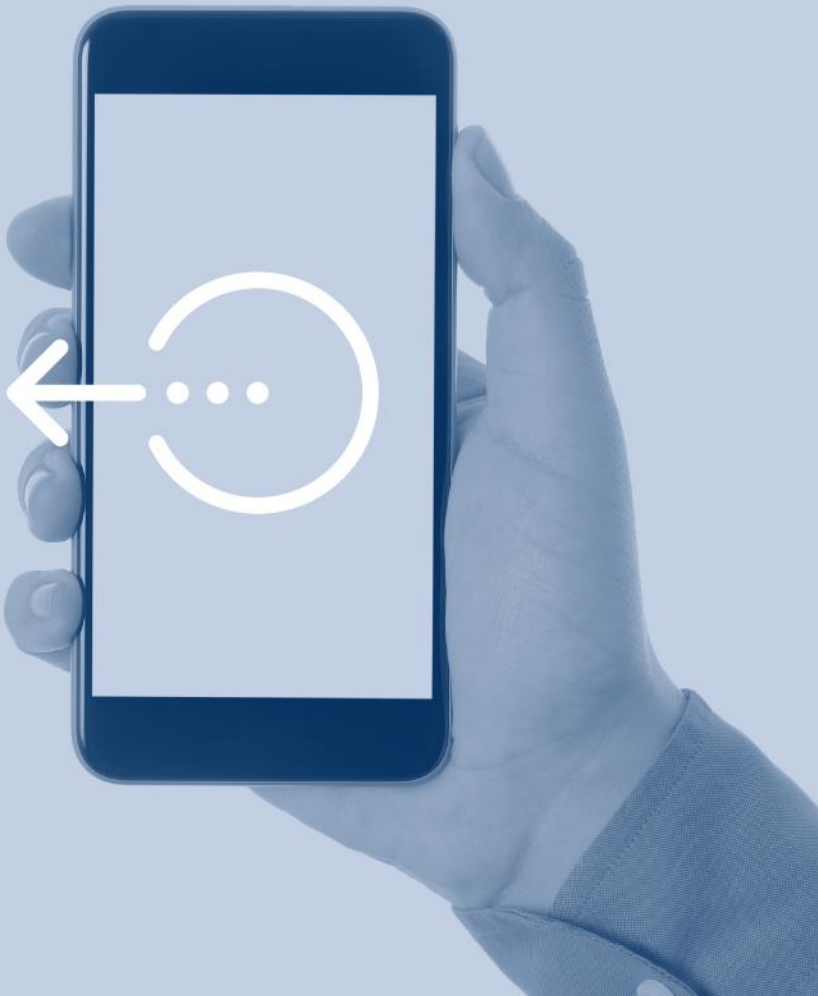
Mobile phone data extraction by police forces in England and Wales

Investigation report

June 2020

Version 1.1



Information Commissioner's Office

Foreword

There can be few other areas of our lives where our wider human rights and our information rights come together so vitally than in the area of criminal justice.

When concerns arose about the potential for excessive processing of personal data extracted from mobile phones, in a process known as mobile phone extraction, I resolved to inquire into and understand the privacy and data protection risks. Many of our laws were enacted before the phone technology that we use today was even thought about. The existing laws that apply in this area are a combination of common law, statute law and statutory codes of practice. I found that the picture is complex and cannot be viewed solely through the lens of data protection. As this report makes clear, a whole-of-system approach is needed to improve privacy protection whilst achieving legitimate criminal justice objectives.

Our smart phones are powerful repositories of highly sensitive personal information, including our intimate conversations, family photographs, location history, browsing history, biometric, medical, and financial data. They reveal patterns of our daily personal and professional lives and enable penetrative insights into our actions, behaviour, beliefs, and state of mind. It is no exaggeration to say that the personal data found in our mobile phones richly depict our lives.

Those working in the criminal justice system recognise, as I do, the value of mobile phone data for achieving appropriate criminal justice outcomes, as well as the challenges that the high volumes of data can bring, given the proliferation of digital information being created and stored through the widespread use of mobile phones.

This report explains how current mobile phone extraction practices and rules risk negatively affecting public confidence in our criminal justice system. Of particular concern is my finding that police data extraction practices vary across the country, with excessive amounts of personal data often being extracted, stored, and made available to others, without an appropriate basis in existing data protection law.

In reaching this conclusion, my report examines the relevant data protection rules in some detail. It explains the significant requirements that an organisation must meet to rely on the legal basis of consent for data extraction. The report also describes an alternative condition for processing: where it is necessary for the performance of a task carried out for a law enforcement purpose by a competent authority.

Central to either approach is communication and meaningful engagement with complainants and witnesses. People expect to understand how their personal data is being used, regardless of the legal basis for processing. My concern is that an approach that does not seek this engagement risks dissuading citizens from reporting crime, and victims may be deterred from assisting police.

I am therefore calling on government to introduce modern rules, through a code of practice that improves data extraction practices. This will build public confidence, notably the confidence of victims of crime and witnesses in permitting extraction of their sensitive personal data. It will also better support police and prosecutors in their vital work. I propose the creation of a national consortium of relevant public agencies and organisations to work collaboratively to help construct such a code.

In conducting this investigation, I listened intently to a range of views from within the criminal justice sector and across civil society and victims' groups. I am grateful for the time stakeholders have taken to assist this investigation and for the valuable insights provided.

I am encouraged by the consensus across all stakeholders that more needs to be done to govern mobile phone extraction practices while increasing public confidence. This report offers a detailed technical analysis of data protection law, but the implications for individuals' privacy are abundantly clear, as is the need for significant reform and improvements in practice.

While the work needed to implement my recommendations must not fall by the wayside, I am acutely aware that this report is issued at a time of unprecedented challenges flowing from the COVID-19 pandemic. I therefore acknowledge that the timeline for change will be longer than usual, but I am keen that we begin to make progress as soon as practicable, and I am committed to supporting that work at all stages.

Elizabeth Denham CBE
Information Commissioner

Contents

Executive summary

Mobile phone extraction in policing

The Information Commissioner has investigated the process known as Mobile Phone Extraction (MPE), used by police forces when conducting criminal investigations in England and Wales. This followed concerns that:

- forces were inconsistent in their approach;
- there were poor practices in information handling, including an overly wide approach to extracting data; and
- a reliance on consent as the basis for undertaking this task in circumstances where it was not appropriate.

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.

The investigation and its findings call into question the appropriateness of some of the current police practices in MPE. This report recommends that a number of measures are implemented across law enforcement in order to improve compliance with data protection law and regain some public confidence that may have been lost.

The original policing principles[1] set out in 1829 by Sir Robert Peel intended to define an ethical police force and are still relevant and continue to underpin policing today. One of these principles is:

> "to recognise always that to secure and maintain the respect and approval of the public means also the securing of the willing co-operation of the public in the task of securing observance of laws."

The way that people use their phones today could not have been envisaged at the time that key criminal justice legislation was formulated. Today, people see mobile phones as extensions of themselves; they have become unique repositories of our personal information, generating huge amounts of data and often hold the most intimate and private details of our everyday lives. Mobile phone usage continues to grow exponentially with all generations routinely interacting through phones and applications. Mobile phones are used in such a

[1] https://www.gov.uk/government/publications/policing-by-consent

range of activities that even a cursory analysis of their contents can reveal detailed insights into thoughts, movements and personal preferences.

Such is the richness of information contained on, and accessed by, mobile phones that they are increasingly a key source of evidence in criminal investigations. Recognising this, and the Peel principles, means that MPE in the policing context needs to take proper account of data protection and privacy quite apart from what the law strictly requires. Without doing so, the confidence of complainants[2] and witnesses could be undermined to the detriment of the police's ability to do their important work.

Whilst the investigation observed practice in only a limited number of police forces, it gathered sufficient evidence to conclude that there are inconsistent approaches and standards of compliance by forces. This raises concerns that there is no systematic approach to justifying privacy intrusion and demonstrating that it is balanced against legitimate law enforcement purposes. Given the sensitive data processing involved, the observed police practices increase the risk of arbitrary intrusion and impact standards of compliance when processing personal data extracted from mobile devices. This increases the risk that public confidence could be undermined.

The investigation also found that the ways the different laws governing data protection, police investigation and evidence gathering intersect in MPE operations provide additional challenges to police forces in achieving consistent and compliant practice.

The Commissioner recognises the absolute right to a fair trial and the important part that relevant mobile phone data might play in criminal investigations and fair proceedings. The Commissioner recommends, however, that further improvements are introduced to demonstrate that the processing involved is in accordance with the law and to ensure that there are sufficient safeguards in place and routinely applied to guard against arbitrary interference with individuals' rights.

It is acknowledged that this is a complex area, engaging not just data protection law but also criminal justice and human rights legislation. Whilst the primary focus of the investigation was data protection, it would have been remiss not to consider the end-to-end process from identification of a requirement for the data, through its extraction and use, to its ultimate deletion. The investigation therefore examined the key parts of relevant law in order to explain how different legislation intersects and how these laws need to be applied to MPE.

[2] For convenience and brevity, we use the term "complainant", without prejudice or disrespect, to refer generically to a person who has made a report of being the victim of a criminal offence, recognising that such a person may be referred to as a "victim" or "survivor".

The Commissioner's findings also address the nature of the engagement with owners of phones and provide clear direction about the sensitive nature of data processed through mobile phone extraction and the higher thresholds that must be met for this to be lawful and justifiable. In particular, a default position of, in some cases, extracting as much data as is available (as opposed to seeking specific data) is challenged.

Recommendations

Recommendation 1: Given the complexity of this area, the Commissioner is calling for the introduction of better rules, ideally set out in a statutory code of practice, that will provide greater clarity and foreseeability about when, why and how the police and other law enforcement agencies use mobile phone extraction.

Recommendation 2: Police should revisit and clarify the lawful basis they rely upon to process data extracted from mobile phones. This should include whether or not the Investigatory Powers Act 2016 is engaged by any aspects of the MPE they are conducting. The report focuses on two conditions for law enforcement processing that data protection legislation provides: the Consent[3] of the data subject or, where Consent is not appropriate, the processing is strictly necessary to carry out the law enforcement task. From the perspective of the data protection regulator, the report makes clear that in the context of law enforcement processing, including MPE, achieving the standards of Consent (in data protection terms) is deliberately challenging. This is to ensure that the individual has meaningful choice and control over how their data is used. The investigation found that the practices being adopted presently did not always demonstrate the conditions needed for Consent to be valid. If opting to rely on Consent, the police must ensure that they are meeting these high standards.

The investigation concludes that this alternative condition for processing (strictly necessary for a law enforcement purpose) is more appropriate and the police should carry it out with clear communication with the owner of the phone and, wherever possible, their co-operation. In other words, this alternative should not be regarded as simply a coercive option invariably imposed upon complainants and witnesses. With either condition, there are clear obligations on the police to meet the requirements for sensitive processing and uphold the safeguards that the law requires for this type of processing. Given the number of different agencies and organisations involved in making such an arrangement work, an overarching code of practice covering the relevant parts of the criminal justice system may also provide the opportunity to clarify the role consent has in MPE.

Recommendation 3: The police, the Crown Prosecution Service and the Attorney General's Office should collaborate to improve the consistency of

[3] Consent in data protection law has a specific meaning and is represented throughout this report as "Consent" (with upper case C) to distinguish it from the general definition of consent.

authorising data extracts. This should be implemented across England and Wales, to increase public confidence in the accountability of the police and the criminal justice process when undertaking these intrusive actions.

Recommendation 4: Police should complete their work to ensure that they are conforming to the standards underpinning the integrity of MPE, as required by the Forensic Science Regulator.

Recommendation 5: Police forces should put in place more robust policies and procedures to ensure the appropriate handling and deletion of data that has been extracted but that is not relevant to a particular investigation.

Recommendation 6: Early engagement between the police and the Crown Prosecution Service should be improved as envisaged in the Attorney General's report[4] in order to allow the extraction, further processing and disclosure of mobile phone data to be more targeted such that privacy intrusion is minimised.

Recommendation 7: Police forces should implement measures to ensure that mobile phone data is managed in accordance with data protection legislation and retained no longer than necessary.

Recommendation 8: To meet the standards required for fair processing, police forces should make improvements to their engagement with individuals whose phones are to be examined, to ensure they fully inform those individuals about what is being proposed and what their rights are. This will involve providing detailed privacy information and working to improve the current notices given to those whose phones are to be examined.

Recommendation 9: A national training standard should be introduced to ensure all those involved in mobile phone extraction are aware of their legal obligations.

Recommendation 10: The technology used by police forces in extracting data should be updated and future procurements should take account of privacy by design principles to ensure it supports the forces in complying with their legal obligations.

Recommendation 11: Chief officers should ensure that data protection officers are involved 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 to ensure compliance with

[4] https://www.gov.uk/government/publications/review-of-the-efficiency-and-effectiveness-of-disclosure-in-the-criminal-justice-system

data protection requirements. They should also ensure that up-to-date DPIAs exist for all relevant current processing.

Recommendation 13: Wider work being undertaken across criminal justice, including revisions to the Victims' Code, the Attorney General's Guidelines on Disclosure and the Criminal Procedure and Investigations Act 1996 Code of Practice, should incorporate measures that address data protection and privacy concerns.

Next steps

The police and the wider criminal justice community must take action to apply these recommendations to their practice in order to provide the public with appropriate levels of reassurance. The Commissioner offers support to the National Police Chiefs' Council and College of Policing to assist with taking forward these recommendations.

This can by no means be the end of the story. Data protection and privacy is one aspect of a much broader set of issues in this space, and there are significant steps across the whole system that need to be taken to increase the public's confidence in how their personal data is used in a criminal justice context. The Commissioner therefore calls for a national consortium of relevant organisations to work together to improve the system as a whole in order to ensure public confidence in the wider process.

The Commissioner will be writing to Chief Constables and Police and Crime Commissioners, to assist in the consideration and implementation of her recommendations.

The Commissioner recognises the shared ambition across agencies and organisations to improve practice, including the National Disclosure Improvement Plan and the Attorney General's review and the Victims' Code revision already under way, and her recommendations should be seen as complementary to that work. These combined efforts will provide a catalyst for improvements in data protection and privacy issues that will in turn provide the public with greater reassurance.

1. Introduction

1.1 Background

There can be few more important areas in our lives where our information rights and our wider rights come together than in the area of criminal justice. In August 2018, the Information Commissioner launched an investigation into the use of mobile phone extraction (MPE), a practice undertaken by law enforcement agencies to extract data from electronic communication devices of complainants[5], witnesses and suspects during the course of a criminal investigation. This investigation took into consideration concerns raised with the Commissioner from individuals affected by MPE and also a complaint made by Privacy International (PI).

PI's report "Digital stop and search: how the UK police can secretly download everything from your mobile phone"[6] raised a wide range of concerns about MPE and called for an urgent review of the police's use of it.

1.2 Scale of the issue

MPE is a common feature of police[7] investigations across the country. It is clear that mobile devices have become embedded into the everyday lives of a majority of the population. Current OFCOM statistics[8] show that 78% of adults personally use smartphones. These devices are being used to process far more data than could have been envisaged when legislation underpinning criminal justice practices was drafted. Smartphone users each process around 1.9GB per month (roughly twice the contents of the Encyclopaedia Britannica). The extent to which these devices effectively record a user's everyday activities, whether it be their movements, their associations, their personal preferences, or the services they access online, is unprecedented.

1.3 Mobile phones

There can be few aspects of day-to-day life that do not involve the use of mobile devices, ranging from formal business communications to accessing sensitive financial records, recording family holiday memories, or having intimate exchanges with loved ones. The ever-expanding capacity to generate and store

[5] For convenience and brevity, we use the term "complainant", without prejudice or disrespect, to refer generically to a person who has made a report of being the victim of a criminal offence, recognising that such a person may be referred to as a "victim" or "survivor".
[6] https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile
[7] The report is equally relevant to other law enforcement agencies using MPE in criminal investigations.
[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf

data means that a significant history and amount of personal data is held on most devices, including what we might consider to be our most private and sensitive information.

Not all the processing taking place on our smartphones is initiated by its user. Much is system generated without any interaction with, or often the knowledge of, its user. Mobile apps can often record data without users being aware and this data is not always visible to them, eg geographical location history, browsing history and wifi connection history. Whilst there are a range of potentially analogous situations where the police seek personal information from complainants and witnesses, the mobile phone is unique as a repository of data with different implications for data protection and privacy.

When messaging apps such as WhatsApp[9] are used, it is common for a sender's personal data (photos, videos or other personal information) to be placed onto the recipient's device, without the recipient's knowledge or explicit acceptance. These communications could contain private or sensitive information and the sender may have a reasonable expectation that the recipient will keep the contents private.

Finally, given the ubiquitous nature of data storage systems, the apps on the device and the credentials stored on them may facilitate access to personal data stored in the cloud. This means the device is not just a repository of evidence in its own right, but it is also a key to wider personal information about the individual.

There are therefore a number of factors that police investigators need to carefully consider when assessing whether they need to access and extract data from a mobile phone, particularly a smartphone, because:

- they often contain intimate details of individuals' private lives;
- they contain data about a significant number of identifiable individuals;
- there is likely to be a very large volume of personal data, potentially relating to significant periods of time;
- much of the data will often be of no relevance to the investigation;
- the individuals (both the user and their contacts) whose personal data is stored on the device have a reasonable expectation of privacy; and
- the owner (or user) of the device may have limited control and knowledge of what is stored on it or accessible via it.

[9] WhatsApp Messenger is a freeware, cross-platform messaging and 'Voice over IP' service owned by Facebook.

This is quite different to the case of a diary, for example, in which its owner has full control and knowledge of its contents, the nature of sensitive data about others is much more limited, and it is not a gateway to wider data.

1.4 Requirement for the data

Data extracted from mobile phones can assist the police in acquiring evidence in support of a criminal investigation, including providing details of individuals' actions, movements and state of mind.

Whilst the benefit of MPE as a rich source of evidence is understood, its use by the police must take into account individuals' human rights and comply with laws governing police investigatory powers and the use of personal data. The level of intrusion into individuals' privacy must be necessary and proportionate to the matter being investigated. Data protection legislation applies equally to all individuals, but other legislation requires the police to treat different categories of person in particular ways during the investigative process, and this extends to the status of the holder of the device, whether they are a complainant, witness or suspect.

This investigation considers, **from a data protection and privacy perspective**, concerns expressed by civil society groups about police accessing very private information on a routine basis in criminal investigations, and the tendency toward accessing large volumes of ultimately irrelevant but no less sensitive personal information. Many of the data protection issues identified as part of this investigation may be felt most acutely by complainants and witnesses whose devices are subject to MPE.

1.5 Challenges and concerns

The right to a fair trial is an absolute right, and the right to privacy and the protection of personal data have to be considered in this context. For the public to have confidence in the criminal justice process, it is important that a public authority gives due deference and proper weight to individuals' right to privacy.

The Commissioner recognises the challenges faced by the police and prosecuting authorities operating in a digital age. These challenges include the substantial volume of data available, the nature of the data, the complexity of criminal cases and the need to identify reasonable lines of enquiry, whether these point towards or away from a suspect. This creates a tension between balancing the obligation on the police and prosecutors to identify all reasonable lines of enquiry and acquire evidence, against the intrusion that their activities may have on the privacy of the holder of the device being examined, as well as other individuals whose personal data is accessible through the device. The Commissioner also notes the challenges faced by the public in understanding what happens to data

extracted from mobile devices in the course of an investigation and how personal data is managed from the point of collection through to disposal.

The availability and volume of data on digital devices has a practical impact on the majority of criminal investigations, and has increased both the resources necessary and the length of time taken to review the material. In its report of its 2019 rape review, HM Crown Prosecution Service Inspectorate (HMCPSI):

> "saw requests for forensic examination of phones taking up to 11 months to complete."[10]

As the volume of data held on devices continues to increase, police can potentially identify and obtain greater volumes of data in the course of an investigation. Once obtained, police need to review the data held as part of the investigation. Situations can quickly arise where there is more data held by the police than can realistically be viewed, affecting timescales for an investigation and for criminal justice outcomes. Other techniques are therefore required to interrogate the data, such as keyword searches or, once there is a sufficient level of maturity and confidence in them, potentially artificial intelligence-based technologies.

There has been widespread concern resulting from a number of high-profile cases where it has been found that materials obtained from mobile phones were not used properly. This is most notably set out in the Joint Review by the Crown Prosecution Service and Metropolitan Police Service of the disclosure process in the case of *R v Allan*[11].

Large volumes of data are likely to include intimate details of the private lives of not only device owners but also third parties (eg their family and friends). In other words, it is not just the privacy of the device owner that is affected, but all individuals that have communicated digitally with that person or whose contact details have been added by the owner. This presents considerable risks to privacy through excessive processing of data held on or accessed through the phone.

Left unexplained, or in cases where it is not necessary or justified, this intrusion into individuals' privacy presents a risk of undermining confidence in the criminal justice system. People may feel less inclined to assist the police as witnesses or to come forward as a victim, if they are concerned that their and their friends' and families' private lives will be open to police scrutiny without proper safeguards. The 2019 HMCPSI inspection observed that requests from the CPS were not being sufficiently specific about the data required (leading to the

[10] paragraph 1.20 https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf
[11] https://www.cps.gov.uk/publication/joint-review-disclosure-process-case-r-v-allan

default position of trying to extract as much as possible). The report of that inspection states that:

> "lawyers' and managers' comments frequently referenced heightened concerns about privacy as causes for less co-operation, but also referenced misunderstandings about what would happen to the material, adverse media coverage, and CPS requests not restricting the request by the proper use of parameters."[12]

We assess there is a connection between the willingness of victims and witnesses to come forward and report serious crime in circumstances where:

- the advice provided to them about what happens to personal data held on their mobile device is inadequate;
- the grounds for processing it are unclear; or
- they believe that no distinction is made between what is relevant and what is simply available for downloading.

Risk related to diminishing confidence is likely to increase if there is a lack of governance and oversight of the processing being carried out or there are weaknesses and inconsistencies in practices for retention, disclosure and security of the data extracted.

It is also critically important that individuals who have been a victim of or witness to crime do not suffer further distress due to unnecessary intrusion into areas of their life they have a reasonable expectation would be kept private. The criminal justice system should support the autonomy and agency of victims to the greatest extent possible. All of this needs to happen without any risk to a fair trial, whilst considering the balance between the trust and co-operation of the public against the wider public interest in reducing crime and protecting the public.

1.6 Public interest

Law and order are fundamental to the maintenance of a civil society, and there is therefore significant public interest in the ability of citizens to report crime and in the police being able to investigate crimes effectively.

There are substantial concerns across society, government and the police and justice sector, about the increases in the number of cases of rape or serious sexual assault being reported, in the reduction in the numbers of charges and convictions, and the potential link between these and the processing of sensitive

[12] paragraph 7.16 https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf

personal information and associated privacy intrusion[13]. There has also been extensive media coverage highlighting concerns where the management of data extracted from mobile phones has undermined the progression of cases through the criminal justice process.

Through this investigation, we have seen a broad consensus across the criminal justice sector, police, government, the public and civil society groups that more needs to be done to ensure public confidence in the criminal justice process, whilst adapting to the challenges of digital disclosure. The high level of interest will continue with advances in Artificial Intelligence (AI) and the way AI, including machine learning, is used in the justice sector[14].

1.7 Reports and inquiries

PI published a report calling for an urgent review of the use of MPE by the police, ("Digital stop and search: how the UK police can secretly download everything from your mobile phone"[15]). It raised questions over the lawful bases for carrying out extractions, the lack of national and local guidance, and the authorisation process. The report also highlighted concerns over the retention of extracted data and individuals' rights to access it, as well as over security measures which are in place to protect data that has been acquired. PI were also concerned that the use of MPE kiosks ('self-service' devices used by police forces to download and analyse the contents of individuals' mobile phones) is becoming more common and forming part of 'business as usual' for officers, despite a lack of governance, oversight and accountability in their use.

The House of Commons Justice Select Committee conducted an inquiry into the disclosure of evidence in criminal cases[16], which came about following the high-profile collapse of a number of cases in 2017 and 2018. In addition, in November 2018, the Attorney General's Office (AGO) published the government's review of the efficiency and effectiveness of disclosure in the criminal justice system[17]. The official reports of these governmental reviews reflect on previous criminal justice failings and highlight the need to consider the requirements for disclosure of materials to the defence, from the point at which an allegation is made. They point to challenges associated with the management of large volumes of digital material and express concern that confidence in the administration of criminal justice may be being undermined by cases collapsing

[13] https://www.london.gov.uk/sites/default/files/vcl_rape_review_-_final_-_31st_july_2019.pdf
[14] https://www.lawsociety.org.uk/news/documents/horizon-scanning-artificial-intelligence-and-the-legal-profession/
[15] https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile
[16] https://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2017/disclosure-criminal-cases-17-19/
[17] https://www.gov.uk/government/publications/review-of-the-efficiency-and-effectiveness-of-disclosure-in-the-criminal-justice-system

or being stayed due to deficiencies in the management of materials relevant to the case.

There have been developments in guidance and practice in England and Wales in conjunction with the official inquiries, including the CPS 'Disclosure – A guide to "reasonable lines of enquiry" and communications evidence'[18] guidance.

The Information Commissioner's Office (ICO) investigation also coincided with the Scottish Parliament's Justice Sub-Committee on Policing's inquiry into Police Scotland's Digital, Data and Information and Communications Technology (ICT) strategy. The ICO provided evidence to that inquiry. Police Scotland's strategy included a plan to roll out 'cyber kiosks' to frontline police officers. This meant they would be able to browse the contents of phones as a form of triage to determine whether further examination (including data extraction) was required by a specialist digital forensics unit. The inquiry concluded with a Scottish Parliament report[19] into this proposal. The ICO is continuing to engage with Police Scotland about the issues arising from this report.

1.8 Investigative methodology

This investigation was driven by an aim to improve compliance with data protection legislation, upholding information rights for complainants, witnesses and suspects, and other affected parties, when MPE is used in police investigations, whilst recognising the legislative requirements relating to criminal justice. It sought to develop a detailed understanding of the legislative frameworks, governance arrangements, business practices and challenges faced by those undertaking or affected by MPE and to provide further clarity for those responsible for processing personal data in this context.

In order to achieve this, a number of key stakeholder organisations were engaged in writing, through face-to-face meetings and round-table workshops, including government departments and official bodies, victims' commissioners, regulators and civil society groups, in order to gain an in-depth appreciation of challenges and concerns.

This was supplemented by observations of the use of MPE in live investigations in a number of police forces[20]. MPE technology vendors also assisted the investigation by providing details of the capabilities of their systems.

[18] https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence
[19] https://digitalpublications.parliament.scot/Committees/Report/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks
[20] No personal data was disclosed to ICO investigators during the field observations.

Direct engagement was supplemented with analysis of relevant legislation, guidance, training materials, and submissions, publications and official reports by civil society organisations, victims' groups and government.

The principal official bodies and stakeholder groups the ICO engaged with or consulted during the investigation include:

- Association of Police and Crime Commissioners (APCC);
- Attorney General's Office (AGO);
- College of Policing (The College/CoP);
- Crown Prosecution Service (CPS);
- Forensic Science Regulator (FSR);
- Home Office;
- Independent Office for Police Conduct (IOPC);
- Investigatory Powers Commissioner's Office (IPCO);
- Mayor's Office for Policing and Crime (MOPAC) Victims' Commissioner for London;
- National Police Chiefs' Council (NPCC);
- Victims' Commissioner for England and Wales; and
- a number of police forces and specialist units engaged in MPE.

A number of civil society organisations and victims' groups also provided representations to the investigation, including:

- Big Brother Watch;
- Centre for Women's Justice;
- End Violence Against Women;
- Liberty;
- Mayor of London's Violence Against Women and Girls Board;
- Privacy International;
- Rape Crisis England & Wales;
- Rights of Women; and
- The Survivors Trust.

As findings emerged, senior ICO representatives met with senior police, criminal justice, civil society and victims' representatives to consider the particular issues arising from consent and to understand the consequences of the recommendations that had been formulated at that stage.

1.9 Scope of the investigation

As the regulator of data protection legislation, the ICO investigation sought to understand the practices currently employed by the policing and justice sector in order to assess their compliance with that legislation. The investigation sought to understand the measures in place to review content, limit excessive processing, ensure security and provide individuals with the ability to exercise their information rights. It is clear that data protection is only one of the laws that impacts on this process and that any improvements to the application of the legislation require a whole-system approach and commitment to improve.

In line with the PI complaint, it was also important to consider the lawful basis the police rely on for extracting and processing personal data from mobile devices. In areas where the police do not normally use coercive powers (eg in relation to complainants or witnesses), this was necessary because of the threshold that needs to be met for consent (in the meaning intended under data protection law) to be a valid basis for processing.

This investigation covers the whole of the UK. However, due to the variations in criminal justice legislation relating to the countries of the UK and the significance of the Commissioner's emerging findings, it was decided that this report would focus on England and Wales and be published at the earliest opportunity. The general principles around data protection are equally applicable across all UK countries. Further reports will be published about Scotland and Northern Ireland in due course.

1.10 Structure of this report

This section of the report has set the scene about the nature of mobile phones, their use in modern society, how the data contained on them is commonly used by police as a source of evidence in criminal investigations, and concerns about how the practice of MPE impacts the privacy of those whose information may be stored on them. It explains the nature and scope of the ICO's investigation.

The report goes on to set out in one place, for the first time, all the legislation that is relevant to the extraction of mobile phone data by police in the context of criminal investigations and links that to data protection legislation. It provides an analysis of the extent to which practice complies with the legislation, before detailing the findings of the investigation and setting out recommendations for the police and others to implement in order to improve compliance.

2. Legislative framework

In order to assess the lawfulness of MPE, it is necessary to consider elements of the criminal justice framework that place obligations on the police in conjunction with the relevant data protection legislation.

2.1 Criminal justice legislation

The legal landscape around police investigatory powers is wide-ranging and complex. This section provides an overview of the legislation that is directly relevant to MPE.

2.1.1 Police and Criminal Evidence Act 1984

The Police and Criminal Evidence Act 1984 (PACE)[21] confers powers on police officers to secure evidence as part of a criminal investigation.

Part II of PACE sets out a range of powers including entry, search and seizure. In particular, s19 PACE provides the police, who are lawfully on the premises, with the power to seize anything that they reasonably believe to be evidence about an offence being investigated, if it is necessary to seize it in order to prevent the evidence being concealed, lost, altered or destroyed[22]. Sections 20 and 21 apply these powers specifically to the seizure, access and copying of computerised information (including that stored on mobile phones).

2.1.2 Criminal Justice and Police Act 2001

There is recognition that, at the point of seizure, it is not always possible or practical to separate material that can be lawfully seized from that which cannot, particularly in the case of digital data. Therefore, in order to allow investigators to sift through that material elsewhere, Part 2 of the Criminal Justice and Police Act 2001 (CJPA)[23] permits police officers to seize material which cannot be separated from any material which they have the power to seize under PACE.

2.1.3 Criminal Procedure and Investigations Act 1996

The Criminal Procedure and Investigations Act 1996 (CPIA)[24] and its code of practice[25] set out how police officers should record, retain and reveal to the

[21] https://www.legislation.gov.uk/ukpga/1984/60/contents
[22] s19(3) PACE
[23] https://www.legislation.gov.uk/ukpga/2001/16/contents
[24] https://www.legislation.gov.uk/ukpga/1996/25/contents
[25] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf

prosecutor, material obtained in a criminal investigation and which may be relevant to the investigation.

In particular, the CPIA code provides the duty for officers to pursue all **reasonable** lines of enquiry whether they point towards or away from the suspect, and to gather and retain **relevant** materials[26].

Material may be relevant to an investigation if it appears that it has some bearing on any offence under investigation or anyone being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case.[27]

The police must retain material that may be relevant to an investigation at least until the accused is acquitted or convicted, or the prosecutor decides not to proceed with the case. If the accused is convicted, they must retain the material at least until:

- the convicted individual is released from custody, or discharged from hospital, in cases where the court imposes a custodial sentence or a hospital order; or
- six months from the date of conviction, in all other cases.

If there is an appeal to the conviction, further obligations to retain data apply.

2.1.4 Investigatory Powers Act 2016

The Investigatory Powers Act 2016 (IPA)[28] makes provisions about, amongst other things, the interception of communications and how intercepted material is handled. These powers are subject to oversight by the Investigatory Powers Commissioner's Office (IPCO).

Under the IPA, an interception can occur while a communication is being transmitted or by accessing communications stored during or after transmission. Under s4(4)(b) of the IPA, accessing the contents of a communication stored in or by a telecommunication system (whether before or after its transmission) constitutes interception, irrespective of whether it has already been accessed by the intended recipient. This has significance in the context of MPE if police access "stored communications".

Section 6 of the IPA provides for "lawful authority" to carry out the interception of communications. If the interception is carried out with a targeted interception warrant[29] or, "in the case of a communication stored in or by the telecommunications system", a targeted equipment interference warrant[30], it will

[26] s3.5 CPIA Code
[27] s2.1 CPIA Code
[28] https://www.legislation.gov.uk/ukpga/2016/25/contents
[29] Part 2 IPA
[30] Part 5 IPA

be lawful for all purposes. There are a number of other circumstances covered in s6 that can provide lawful authority without a warrant. Chapter 12 of the Interception of Communications code of practice[31], issued under Schedule 7 of the IPA summarises the requirements for the lawful interception of communications without a warrant, including (but not limited to) where:

- the sender and the intended recipient have consented to the interception[32];
- either the sender or intended recipient has consented and a concurrent directed surveillance authority is in place under Part II of the Regulation of Investigatory Powers Act 2000[33];
- it takes place as a result of the exercise of a statutory power exercised for the purpose of obtaining the information[34]; or
- it is carried out in accordance with a court order[35].

The IPA makes it clear that a "telecommunications service"[36] means any service that facilitates the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system. Therefore, this includes services such as SMS messaging provided by mobiles phones.

There are a number of statutes that may be used to obtain stored communications for evidentiary purposes. Those most commonly used by law enforcement agencies include (but are not limited to):

- powers of search, seizure or production under the Police and Criminal Evidence Act 1984;
- powers to search or obtain content under the Proceeds of Crime Act 2002;
- powers to search under the Firearms Act 1968, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971;
- powers to examine imported goods under the Customs and Excise Management Act 1979 to examine imported goods; and
- powers to search or examine under Schedule 7 of the Terrorism Act 2000.

While both the monitoring of a communication simultaneously with its transmission and the interception of "stored communications" can constitute interceptions, the IPA treats the monitoring of live communications as legally distinct from the accessing of stored communications. It is essential for any

---

31 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf
32 s44(1) IPA
33 s44(2)(a)-(b) IPA
34 s6(1)(c)(ii) IPA
35 s6(1)(c)(iii) IPA
36 s4(3) IPA

person who accesses electronic data to be clear about whether they are carrying out activity that falls under the provisions of the IPA, and if so that they are doing so with lawful authority under s6 of the IPA as well as complying with the guidance contained in the codes of practice.

It is important to note that common law powers and consent from the holder of the device would not, in themselves, constitute lawful authority for interception of communications to take place, where such situations arise.[37]

2.2 Data protection legislation

In May 2018, the Data Protection Act 1998 was repealed and the European General Data Protection Regulation (GDPR)[38] came into force. At the same time, its sibling legislation relating to police use of data, the European Data Protection Law Enforcement Directive[39], was implemented in the UK through the Data Protection Act 2018 (DPA 2018)[40].

The aspects of the UK legislation most relevant to MPE are outlined in this section.

2.2.1 Data Protection Act 2018

DPA 2018 aims to protect individuals' data rights by setting out a number of principles that must be respected by controllers[41] when carrying out any processing of personal data relating to identifiable natural persons (data subjects)[42]. It confers a number of rights on those whose data is being processed.

2.2.2 Law enforcement processing

Part 3 DPA 2018 contains specific provisions relating to "competent authorities" processing data for law enforcement purposes.

A competent authority[43] is:

- an individual specified in Schedule 7 DPA 2018; or
- any other individual if, and to the extent that, they have statutory functions to exercise public authority or public powers for law enforcement purposes.

[37] S44 of the IPA sets out specific requirements that must be met in order for the retrieval of data, in a way that would constitute an interception under the IPA, to be authorised by the consent of the sender or the recipient.
[38] http://data.europa.eu/eli/reg/2016/679/2016-05-04
[39] http://data.europa.eu/eli/dir/2016/680/oj
[40] http://www.legislation.gov.uk/ukpga/2018/12/contents
[41] Article 4(7) GDPR
[42] Article 4(1) GDPR
[43] s30 and schedule 7 DPA 2018

Chief officers of police and other policing bodies are amongst those specified in Schedule 7 DPA 2018.

Law enforcement purposes[44] are defined as:

> "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

2.2.3 Data protection principles

When undertaking law enforcement processing, the DPA 2018 makes controllers responsible for, and requires that they be able to demonstrate compliance with, the following principles[45]:

- 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, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay. 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.

[44] s31 DPA 2018
[45] ss35-40 DPA 2018

2.2.4 Sensitive processing

In the context of law enforcement processing, there are additional protections where the data is considered to be 'sensitive'.

"Sensitive processing"[46] is defined as the processing of:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- data concerning health; or
- data concerning an individual's sex life or sexual orientation.

S35 DPA 2018 mandates the requirement for an appropriate policy document[47] to be in place before sensitive processing is undertaken and for this processing to be either:

- with the **consent** of the data subject (within the meaning of data processing law); or
- **strictly necessary** for the law enforcement purpose and meeting a condition in Schedule 8 DPA 2018.

2.2.5 Legal basis for processing

According to the first data protection principle[48], law enforcement processing under Part 3 DPA 2018 (as defined in section 2.2.2) must be lawful and fair.

The processing can be lawful only if and to the extent that it is **based on law** and either:

- the data subject has given consent (within the meaning of data processing law) to the processing for that purpose; or
- the processing is necessary for the performance of a task carried out for that purpose by a competent authority.[49]

In addition, as a typical mobile phone is highly likely to contain data meeting some of the criteria set out in section 2.2.4, MPE is likely to amount to sensitive processing, and therefore further conditions apply[50]:

either

[46] s35(8) DPA 2018
[47] https://ico.org.uk/media/for-organisations/documents/2616230/part-3-appropriate-policy-document.docx
[48] s35 DPA 2018
[49] s35(2)(a)&(b)
[50] s35(4)&(5)

- the data subject has given consent (within the meaning of data processing law) to the processing for the particular law enforcement purpose; and
- at the time when the processing is carried out, the controller has an appropriate policy document in place;

or

- the processing is strictly necessary for the law enforcement purpose;
- the processing meets at least one of the conditions in Schedule 8 DPA18; and
- at the time when the processing is carried out, the controller has an appropriate policy document in place.

In all cases where sensitive data may be involved, an appropriate policy document, describing how sensitive data is handled and what safeguards are applied, must be in place.

As the preceding discussion establishes, the concepts of **Consent** and **strict necessity** have great significance for MPE. Each of these is considered in turn.

Consent

There is no explicit definition of "Consent" provided in Part 3 DPA 2018. However, the EU Law Enforcement Directive (LED), upon which Part 3 DPA 2018 is based, refers to "consent of the data subject, as defined in Regulation (EU) 2016/679"[51]. Therefore, the standard for Consent to operate as the sole justification for law enforcement processing is a high bar, with the conditions being the same as those specified in the GDPR.

The definition of Consent is taken from Article 4(11) GDPR which states that:

> "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

An indication of Consent must be unambiguous and involve a clear affirmative action (an opt-in) by the data subject. It also requires distinct ('granular') Consent options for distinct processing operations. Individuals should be able to withdraw Consent at any time.

In addition, Recital 42 GDPR further specifies that:

[51] Recital 35 LED

> "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

The UK is also a signatory to the modernised version of the Council of Europe Convention 108[52] (which applies equally to law enforcement processing). It includes guidance stating that:

> "consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice."

Paragraph 45 of the accompanying explanatory report states:

> "The data subject has the right to withdraw the consent he or she gave at any time…"

And withdrawal of consent:

> "does not allow continued processing of data, unless justified by some other legitimate basis laid down by law."

Paragraph 47 explains that the prevention, investigation, detection and prosecution of criminal offences may represent such a legitimate basis.

Note that none of the above implies that any expression of agreement, in itself, renders processing fair and lawful. In order to form the sole basis of processing, such Consent would need to meet the high standards set out above.

Strictly necessary

The term "strictly necessary for the law enforcement purpose" places a high threshold for processing based on this condition. Controllers need to demonstrate that they have considered other, less privacy-intrusive means and have found that they do not meet the objective of the processing. In addition, there is a further requirement to demonstrate that the processing meets at least one of the Schedule 8 DPA 2018 conditions:

- statutory purposes;
- administration of justice;
- protecting individual's vital interests;

[52] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

- safeguarding of children and of individuals at risk;
- personal data already in the public domain;
- legal claims;
- judicial acts;
- preventing fraud; or
- archiving.

2.2.6 Privacy information

To help individuals understand how their personal data is going to be processed, controllers must make a range of information[53] available to them, including:

- the identity and the contact details of the controller;
- the contact details of the data protection officer;
- the purposes for which the controller processes personal data;
- the existence of the rights of data subjects to request from the controller:
    - access to personal data;
    - rectification of personal data; and
    - erasure of personal data or the restriction of its processing;
- the existence of the right to lodge a complaint with the ICO and the contact details of the ICO;
- information about the legal basis for the processing;
- information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;
- where applicable, information about the categories of recipients of the personal data; and
- further information as is necessary to enable the exercise of the data subject's rights under this Part 3 DPA 2018.

Any restriction to providing the information must be justified with reference to at least one condition detailed in s44(4) DPA 2018. Those conditions being that it is a necessary and proportionate measure to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or

[53] s44(1)&(2) DPA 2018

- protect the rights and freedoms of others.

2.2.7 Data protection by design and default

Controllers have a number of other obligations, notably the need to implement appropriate technical and organisational measures[54] which are designed to:

- implement the data protection principles in an effective manner; and
- integrate into the processing itself the safeguards necessary for that purpose.

These measures must ensure that, by default, only personal data which is necessary for each specific purpose is processed, and this duty applies to:

- the amount of personal data collected;
- the extent of its processing;
- the period of its storage; and
- its accessibility.

2.2.8 Logging

Controllers (or processors if they are processing personal data on behalf of the controller) must keep logs[55] for at least the following processing operations:

- collection;
- alteration;
- consultation;
- disclosure (including transfers);
- combination; or
- erasure.

The logs of consultation must make it possible to establish the justification for, and date and time of, the consultation, and so far as possible, the identity of the individual who consulted the data.

2.2.9 Data protection impact assessments (DPIAs)

Prior to commencing any type of processing likely to result in a high risk to the rights and freedoms of individuals, controllers must carry out a data protection impact assessment (DPIA)[56].

The DPIA must contain:

[54] s57 DPA 2018
[55] s62 DPA 2018
[56] s64 DPA 2018

- a general description of the envisaged processing operations;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address those risks; and
- safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Part 3 DPA 2018, taking into account the rights and legitimate interests of the data subjects and other individuals concerned.

In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, controllers must take into account the nature, scope, context and purposes of the processing. The ICO has published detailed guidance[57] on this.

2.3 Human rights legislation

The European Convention on Human Rights (ECHR)[58] has been given further effect in UK law by the Human Rights Act 1998. Article 8 of the ECHR is the right to respect for private and family life, and provides[59]:

- everyone has the right to respect for their private and family life, their home and their correspondence; and
- there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right to the protection of personal data is not an absolute right. It must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality.

In cases where a statutory power (eg PACE) has been exercised (see section 2.1), it must still meet the ECHR 'quality of law' test in that the outcome must be foreseeable and applied only when 'necessary in a democratic society'. There must therefore be sufficient safeguards to prevent abuse and ensure the power is not exercised disproportionately, eg policies and procedures that demonstrate appropriate consideration of necessity and authorisation.

[57] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
[58] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[59] Article 8 ECHR

If an interference with Article 8(1) rights (ie respect for private and family life, home and correspondence) is to be justified, it must meet the four-part test in *Bank Mellat v Her Majesty's Treasury (No 2)*[60], namely whether:

1. the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. it is rationally connected to the objective;
3. a less intrusive measure could have been used without unacceptably compromising the objective; and
4. having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

R (Bridges) v Chief Constable of South Wales[61] confirms at paragraph 136 that this is a relevant test when considering the strict necessity of law enforcement processing under Part 3 DPA 2018 (as outlined in section 2.2.5 of this report).

2.4 Application to MPE

'Processing', in relation to information, means an operation or set of operations which are performed on information, or on sets of information. This begins with collection, recording, organisation, structuring or storage[62].

The investigation determined that processing of personal data begins at the point that data stored on or accessed via the device is viewed or extracted. If no data is viewed or extracted from a device in the possession of the police, no processing has taken place.

The Chief Constable (or Commissioner) of each police force is registered as a controller and must demonstrate compliance with the relevant legislation and oversight rules in order to lawfully process any data extracted from or accessed via a device.

Whilst the police must first, of necessity, take possession of a device in order to be in a position to process any mobile phone data from it, and must comply with the relevant law regarding the acquisition of the device, this is beyond the scope of data protection legislation.

2.4.1 Taking possession of the phone

Police need to consider whether to request that a phone is handed to them with the consent of its owner or, alternatively, to exercise one of their statutory

[60] https://www.bailii.org/uk/cases/UKSC/2013/39.html
[61] https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html
[62] s3(4)(a) DPA 2018

powers. Likely considerations will include the status of the individual phone owner, ie suspect, complainant or witness.

It is important to note that the consent an individual may give for the police to take possession of their phone is entirely distinct from the definition of "Consent" relevant to the extraction and viewing of any personal data from that phone under data protection law. To conflate these two distinct concepts risks confusing which applicable standard to apply at each stage of the process. The fact that physical possession of a phone may have been achieved by consent of the owner does not mean that they necessarily give "Consent" for the purposes of data protection legislation for processing any personal data on the device. In other words, there is a legal distinction between consenting to the police taking possession of the device (under common law) and Consent to the police processing the personal data contained on it (in compliance with data protection law); one does not include or presuppose the other.

Police may consider using statutory powers (eg PACE or CJPA (see sections 2.1.1 and 2.1.2)) to seize a device with a view to examining its contents, in particular if they find a device in the possession of a suspect that they believe may contain evidence relevant to the investigation of a criminal offence.

These statutory powers may be used to obtain evidence but they do not determine appropriate lines of enquiry. This is a decision to be made under Part II of the CPIA and the code of practice issued under s23(1) of that Act.

In the case of complainants or witnesses, investigators may consider it more appropriate to request that the owner of a phone consents[63] to handing over their device to the police in order for it to be examined for evidence. As with statutory powers, this must be justified as a reasonable line of enquiry to obtain evidence.

2.4.2 Processing the data

Since police forces are competent authorities conducting MPE for law enforcement purposes (most commonly the investigation of criminal offences), Part 3 DPA 2018 applies see section 2.2.2).

As noted earlier, personal data typically contained on or accessible through modern smartphones is diverse in nature and is likely to be highly sensitive. The data typically includes intimate, private communications between individuals (as well as a host of sensitive information about individuals' movements, actions, preferences and more) and has the clear potential to meet one or more of the criteria outlined in section 2.2.4. Since police practitioners cannot be certain about the nature of the data before viewing it, **they should proceed on the**

[63] This application of the word 'consent' is intended to have the plain English meaning of agreement and should not be confused with the lawful basis of Consent for processing personal data as defined in DPA 2018.

assumption that it is sensitive and should ensure that they are complying with Part 3 DPA 2018 requirements. The police must also consider the impact on the ECHR right to respect for private and family life of both the user of the device and their contacts.

As part of their accountability obligations and to demonstrate compliance, police forces should carry out a DPIA (see section 2.2.9 above) when they design their data processing operations. This will offer evidence that they have:

- identified appropriate lawful bases for processing (section 2.2.5);
- respected the data protection principles by design (section 2.2.3);
- put in place an appropriate policy document about sensitive processing (section 2.2.4); and
- provided all required information to data subjects (section 2.2.6).

The DPIA must consider all the risks associated with the processing, including the potential impact of individuals' right to privacy, along with measures to treat these risks. If the level of risk remains high following application of these measures, then there is an obligation to consult the ICO[64] prior to commencing the processing.

Police forces must give careful consideration to the lawful basis for the processing, as this underpins all other aspects of compliance with data processing legislation.

Firstly, the processing must be **fair** and **based on law**. This is a matter for the controller to establish, but police forces may consider that this is covered, for example, by their obligation under the CPIA to pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is clear is that the DPA 2018 does not, in and of itself, provide the basis in law for the processing.

Secondly, having established the underlying basis in law, the police must consider which of two possible conditions (set out in s35(2) DPA 2018) they will rely on to ensure the processing is lawful, either:

- the data subject has given consent to the processing for the particular law enforcement purpose; or
- the processing is necessary for the performance of a task carried out for the law enforcement purpose.

Thirdly, on the basis that MPE amounts to sensitive processing, the law sets a higher bar. Sensitive processing for law enforcement purposes is only permitted in cases where either:

[64] s65 DPA 2018

- the data subject has given consent to the processing for the particular law enforcement purpose; or
- the processing is strictly necessary for the law enforcement purpose and meets at least one of the conditions in Schedule 8 DPA 2018.

In all cases of sensitive law enforcement processing, the police force must have an appropriate policy document in place.

Although asking for an individual's consent (in the general sense of the word) may be a core part of the process in order to ensure fairness, this consent alone cannot justify all of the processing without reference to the DPA 2018 strict necessity test. The key challenges when seeking to meet the high standards for Consent (in data protection terms) to be valid are:

- Mobile phones can hold vast amounts of personal data, going back many years before, or indeed after, an alleged offence. Unlike personal details contained in a personal diary or personal correspondence where the contents will be known to the author or owner, the individual may be unable to recall the details of all personal data on their phone. This is relevant when considering how fully informed an individual is to be able to Consent. The narrower the focus of the MPE extraction, the more likely an individual is to be fully informed about the data and about the implications of consenting to its processing.
- A phone is very likely to hold data about many individuals, and it would not be feasible to obtain Consent from each of these data subjects, not least since it is not possible to identify the individuals before processing has commenced. The owner of the phone cannot, under DPA 2018, provide Consent on behalf of others whose data is stored on their device.
- The police would need to show how Consent could be freely given in the context of a criminal investigation. As with many situations involving a citizen and a public authority, there is a perceived power imbalance between the state and the individual asked to provide their phone. Victims and witnesses may be concerned that a decision not to Consent to processing will impact on the progress of the case[65]. There is, in our view, a direct correlation between reasonable and proportionate enquires (with a demonstrable link between those enquiries and evidence likely to be held on a phone) and the likelihood and robustness of Consent as a valid condition for processing. Where all data is downloaded, even if this is unlikely to be relevant to reasonable lines of enquiry, this is likely to diminish the possibility of meaningful consent being given and will

[65] Paragraph 7.13 of the HMCPSI inspection report states "the lack of consent for such material played a part in the decision to take NFA [no further action] in eight of the 45 cases (17.8%), in all of which the complainant was otherwise fully engaged." - https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf

increase the concerns about arbitrary intrusion into privacy. This may result in an individual failing to come forward to report a crime in the first instance.

- Some complainants and witnesses have reported that they feel (rightly or wrongly) that their failure to co-operate with an investigation may be prejudicial to the police pursuing a successful prosecution. Following her London Rape Review, Claire Waxman, Victims' Commissioner for London wrote:

> "If victims/survivors resist, then they can feel immense pressure that the case may collapse as a result. If they comply, many feel as though the personal material is then used to undermine their credibility in charging decisions and in court, ultimately preventing justice. Police and prosecutors must follow reasonable and proportionate lines of enquiry in rape cases, being clear throughout with the victim as to the rationale for seeking access to their data."[66]

This perception of pressure to allow access can be strengthened by text in the notices some forces hand to individuals whose devices have been taken. This is evident, for example, in the case of the NPCC exemplar notice, which states:

> "If you refuse permission for the police to investigate, or for the prosecution to disclose material which would enable the defendant to have a fair trial then it may not be possible for the investigation or prosecution to continue."

- During times of high trauma (eg following a serious violent or sexual offence), studies[67] show it is unlikely that a victim will, because of trauma, be in a position to make a fully informed, freely given rational decision that amounts to Consent. It is therefore important that police consider the cognitive ability of post-trauma victims to be able to rely on Consent for processing personal data.
- In cases where previously-given Consent is withdrawn, police obligations under the CPIA to obtain and retain materials may prevent the deletion of data, regardless of the wishes of the data subject, and Convention 108 would suggest that this ongoing processing may be justified in law (see section 2.2.5 of this report).

---

[66] https://www.london.gov.uk/sites/default/files/vcl_rape_review_-_final_-_31st_july_2019.pdf (page 11)
[67] https://www.justice.gc.ca/eng/rp-pr/jr/trauma/index.html

For the alternative condition (strict necessity for the law enforcement purpose), police forces may consider that their lawful duty under the CPIA (pursuing reasonable lines of enquiry and securing relevant materials) has the potential to demonstrate "strict necessity", provided that they have given explicit consideration to less intrusive means of obtaining evidence. They must fully consider the challenge of the high threshold, ie "strictly necessary" is more than "necessary", for dealing with this highly personal, sensitive data. In terms of meeting the Schedule 8 DPA 2018 conditions, police could consider s1 ("statutory etc purposes") and/or s2 ("administration of justice") to be appropriate.

In all cases where sensitive data may be involved (regardless of the lawful basis relied upon), police forces must have in place an appropriate policy document, describing how sensitive data is handled and what safeguards are applied[68].

Finally, if the mobile device is being used to access and therefore process "stored communications", police forces must consider whether the IPA applies and satisfy the conditions relating to lawful authority.

2.4.3 Providing information to data subjects

As outlined above, there is a clear legal distinction between having a legal basis for acquiring a phone and having a legal basis for the subsequent processing of any data from it. Each must satisfy distinct legal criteria. In practical terms, it will usually be helpful to address both those issues with a complainant or witness at the same time, not least because they are likely to be intrinsically linked in the mind of the complainant or witness whose device it is.

There is an important duty under data protection law to provide fair processing information to individuals, irrespective of how that device came into the police possession. Therefore, when a phone is taken into the possession of a force, officers must provide detailed information to the individual from whom the device is taken or acquired, containing:

- facts about what is being sought from the device;
- under what lawful basis; and
- what rights the individual has in respect of that processing.

They should provide this regardless of the condition for processing (see section 2.4.2) they are relying upon or the category of individual whose device they are examining (eg complainant, witness or suspect).

This information must include, as a minimum, those items detailed in section 2.2.6.

[68] The ICO is currently reviewing its guidance in light of R (Bridges) v Chief Constable of South Wales.

3. Current practice

This section sets out the findings of the investigation based on engagement with government departments involved in developing criminal justice policy, prosecuting authorities and police practitioners, and draws on observation of MPE in practice in police forces.

3.1 Overview

The National Police Chiefs' Council (NPCC) seeks to bring consistency of standards of operation across the 45 police forces in England, Wales and Northern Ireland. It has defined a set of MPE service standards that have been adopted by forces and referenced in the Crown Prosecution Service (CPS) document 'A guide to "reasonable lines of enquiry" and Communications Evidence'[69].

Three levels of MPE are defined in that guide:

- Level 1 – a logical extraction of data, involving a data kiosk interacting with the device's own software;
- Level 2 – a physical extraction that could potentially retrieve deleted data or other data not accessible to the user;
- Level 3 – a full forensic specialist examination that may involve scientific examination of the device's physical components.

Forces have procured specialist hardware and software that they use to extract data from mobile devices. These are from three principal vendors whose products offer slightly different functionality but have similar characteristics.

Level 1 extractions are often carried out using 'kiosk' technology, where the device is connected by cable to a computer with specific software that enables extraction, and its contents interrogated. The success of this will often depend upon the specific configuration of the kiosk (including the version of software being used) and the particular model of device. This 'logical' extraction enables data accessible via the device's own software to be interrogated and extracted.

Where the data required is not directly accessible using the Level 1 technique, a device may be subjected to a Level 2 or Level 3 examination. This could be the case, for example, if there is a suspicion that some relevant material may have been deleted or the device is damaged and requires an alternative method of access.

[69] https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence

As new phones are brought to the market and older ones are updated, the extent to which all the techniques currently available capture all data on a device varies. Therefore, what is sometimes referred to as a 'full download' is somewhat of a misnomer, as the extraction or access may not be "full". This is compounded by the release of new mobile apps and by existing apps changing how data is stored. Therefore, the data able to be extracted in practice will depend on many variables, including:

- the type of device;
- its age;
- which software updates have been applied;
- the apps stored on the phone; and
- the configuration of the MPE software.

All the extractions witnessed during this investigation were carried out by forensically trained officers or staff, although it is understood that consideration is being given to rolling out kiosks that allow front-line officers to interrogate devices. Police Scotland has a formal project that involves officers using such kiosks to 'triage' devices by viewing their contents in order to make a decision on whether to submit them for data extraction by the specialist department. The aim of this is to quickly identify investigative opportunities and also manage demand on forensic departments. Whilst there may be efficiency gains in using this approach, it gives rise to concerns about opportunistic 'fishing expeditions', that circumvent due consideration of reasonable lines of enquiry and proportionality.

3.2 Process

It is common for police forces to have processes for the management of devices that have come into their possession. In general, they are booked into a property store to be held securely (as with any other evidence), and a request is made by the officer in the case (OIC) for some form of MPE to take place. The request contains an overview of the case and the specifics of what is required to be extracted from the device. The investigation identified that there was a lack of consistency between forces about the oversight arrangements, including the criteria for authorising different types of extractions and the seniority or role of the individual required to authorise them. This was evidenced by the use of locally-designed process forms in the absence of national standards.

When a request is ready to be actioned, the relevant device is booked out of the property store and processed according to the OIC's request.

The investigation also found that there were inconsistencies in approach to the forensic process of documenting the results of extractions. It was reported in one force that, while it was not the role of the forensic staff member to sift

through the information extracted, they may carry out that task if they have the time and capacity to do so. Should the information sought not be contained in the extraction, those staff would undertake a more complete download without any further authorisation. This approach, where forensic staff effectively self-task, raises concerns about the routine extraction of data without the OIC necessarily considering strict necessity and proportionality.

In another force, the forensic process was kept entirely separate so that the officers undertaking the extraction would not have any sight of the extracted material to ascertain whether relevant material had been extracted. This maintained the independence of the forensic service, and information extracted was provided to the investigation officer who would search through the material extracted and identify relevant information.

Regardless of the approach taken, the result of the extraction is documented (again either on paper or electronically), including the extent to which the extraction was successful, along with the actual data extracted. Master and working copies of the extracted data are created on digital media (usually CDs/DVDs or USB drives), secured as evidence and booked into the property store for the attention of the OIC.

Our investigation revealed that some forces were moving to secure server storage of extracted data that the OIC would be able to access through log-in credentials. This would replace the need to save information on removable devices and minimise the potential for data breaches through their loss.

Following initial review, extracted data sets can be searched according to user-input parameters (eg names, dates, phone numbers, words, phrase, etc) and the information generated from these search results can be used as relevant material through the criminal justice process. It was not clear to the investigation team whether there were policies and procedures in place that required the investigator to document how the data would be potentially relevant to particular lines of enquiry.

3.3 Compliance with data protection principles

This section considers each of the Part 3 DPA 2018 principles in turn and reflects on the extent to which the observed MPE practice meets the required standards.

3.3.1 First principle: Lawful and fair

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

Section 2.4.2 sets out the considerations that need to be made regarding lawful and fair processing. For ease, these are that having established the underlying

basis in law, the police must consider which of two possible conditions (set out in s35(2) DPA 2018) they will rely on to ensure the processing is lawful. Either:

- the data subject has given Consent to the processing for the particular law enforcement purpose; or
- the processing is necessary for the performance of a task carried out for the law enforcement purpose.

Then, having established that MPE amounts to sensitive processing, the law sets a higher bar. Sensitive processing for law enforcement purposes is only permitted in cases where either:

- the data subject has given Consent to the processing for the particular law enforcement purpose; or
- the processing is strictly necessary for the law enforcement purpose and meets at least one of the conditions in Schedule 8 DPA 2018.

In all cases of sensitive law enforcement processing, an appropriate policy document must be in place.

Digital processing notices

During the course of this investigation, the NPCC published materials ("Obtaining data from digital devices during the course of an investigation") making recommendations[70] to forces about the practice of MPE. The intention was to standardise practice across all forces. These materials focused on complainants and witnesses. It was stated that it was **not appropriate for s19 PACE to be used** in such circumstances, and that **consent must be the basis for obtaining devices and extracting their data**. Also circulated was a "Digital Processing Notice" that police forces were to brand individually and provide to individuals whose devices they were taking.

The NPCC-circulated digital consent forms or digital processing notices do not currently make clear what the underpinning lawful basis for an extraction is, nor the specific condition being relied upon for processing. They do not specifically distinguish, for the complainant or witness, between their agreement to hand over the phone (which is not a data processing matter) and Consent to process the personal data on the phone. The notice makes an assumption about Consent as the appropriate condition for processing without clearly setting out the justification for this or evidencing how the high standards that need to be met for Consent to be used as the condition for processing will be met. In the view of the ICO, they do not accurately reflect to either the police officer, the complainant or witness the standards that need to be met for Consent to be valid and meaningful. Nor does the notice acknowledge that the data processing that will be undertaken through MPE should be assumed to amount to sensitive

[70] The NPCC is not constituted to produce practice guidance; the College of Policing does this.

processing (within the meaning of DPA 2018) and what steps will be taken to ensure that appropriate safeguards are in place.

It should be noted that, whilst the NPCC advice was intended to encourage a standardisation of approach, the evidence from enquiries with a number of forces shows that they do not all agree with the NPCC's interpretation of the law (in relation to applicability of PACE to complainants and witnesses and the use of Consent as the condition for processing personal data). The level of adoption of the lawful basis and associated documentation is unclear and, despite the positive intent, this situation continues to contribute to a lack of consistency, nationally, in the application of individuals' information rights and in how MPE is authorised and managed.

The Commissioner's view is that the forms should be withdrawn and re- drafted to ensure that these fundamental principles are locked into the process and that any notice that emerges is in line with the findings detailed in this report.

Even if the alternative 'strict necessity' condition[71] had been relied upon by forces to justify the processing, no evidence was presented to the investigation to suggest that alternatives to MPE were routinely considered and documented, nor were appropriate policy documents for sensitive processing seen. There was inconsistency in record-keeping for decisions made about powers for obtaining devices and lawful bases used for processing personal data. This implies a lack of consistency in the interpretation and application of data processing legislation. Considerations of necessity, proportionality and collateral intrusion were not, based on what we saw, sufficiently or routinely documented.

Furthermore, it was not clear that forces had policies and procedures to ensure that privacy and the ECHR right to private and family life were key factors when they were considering the need to extract mobile phone data in each investigation.

In our view, the approach based on relying solely on Consent for processing complainants' and witnesses' data has fundamental issues in many circumstances. Therefore, the police forces should not use the forms as currently drafted, nor should they form the sole justification for processing.

It is clear from our engagement with stakeholders that consent as an expression of free will, choice and control is viewed as central to the interests of witnesses and complainants when faced with MPE. The high standards that data protection law sets for Consent to be an appropriate condition for processing sensitive personal data are clearly and purposefully aimed at supporting an individual's autonomy and agency. The fact remains that these high standards need to be met if Consent is to be the condition relied upon for processing. These standards are, in our view, difficult to achieve in most cases where MPE is used – though

[71] s35(5) DPA 2018

there may be some limited instances where Consent could be possible. However, the Commissioner agrees that a consensual approach to dealing with complainants and witnesses is essential and acknowledges the very clear views expressed to her during the course of this investigation about consent. A consensual approach is not incompatible with processing under the alternative 'strict necessity' condition. On the contrary, such an approach can directly contribute towards meeting both the 'lawful' and 'fair' requirements.

Under either approach, police should have clear communication and meaningful engagement with complainants and witnesses about:

- the data the police need to extract and process;
- how the data will be kept secure;
- what will be done with the data after the case has been considered; and
- the individuals' information rights and support to use them.

When engaging the strict necessity condition for sensitive law enforcement processing, the 'Bank Mellat test' (set out in section 2.3 of this report) may be helpful. It is reproduced here for convenience:

1. whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. whether it is rationally connected to the objective;
3. whether a less intrusive measure could have been used without unacceptably compromising the objective; and
4. whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

Applying these questions in the context of MPE, an investigator's considerations would include:

- the extent to which there is a justifiable, reasonable line of enquiry that involves interrogation of sensitive digital data;
- whether and why MPE is required to satisfy the line of enquiry;
- what other, non-forensic means are available, and why they are not sufficient in this case; and
- whether the importance of the line of enquiry, in the context of the seriousness of the matter being investigated and its wider impact, justifies the impact on the privacy of the owner of the phone and others whose data will be processed from the phone.

Even acting under the 'strict necessity' condition, it would be a mistake to proceed simply as if the power should be used coercively without seeking to fully engage with the complainant or witness. Good communication and co-operation

with the user of the phone is likely to be highly significant for two reasons. First, in order assess the impact of MPE on the phone's owner and others whose data is stored on it, it is important to know the type of data that is likely to be on the phone and the data subjects' relationships with it. Informed communication and discussion is likely to be invaluable in making that assessment. Second, as a matter of good practice, those conducting MPE should seek to act with the willing co-operation and full understanding of the data subject.

The Commissioner therefore considers that a co-operative and informed approach which aligns, if possible, with the wishes of the data subject, can and should be part of good practice, even when it has been established that MPE is strictly necessary and proportionate for law enforcement purposes.

3.3.2 Second principle: Limited purpose

The second principle relating to law enforcement processing states that the processing must be limited to a specified, explicit and legitimate purpose, and data must not be processed in a manner that is incompatible with the purpose for which it was collected.

Some forces are innovating with analytical tools that allow rapid searching, visualisation and analysis of data extracted from a single device or multiple devices. The reason given for this is that it is difficult (or sometimes impossible) for a human to manually review very large volumes of data to identify relevant materials to be used in evidence, and some form of analytical tool may assist in ensuring no relevant evidence is missed.

Whilst we saw no evidence of this, there is clearly the potential for this data to be merged and cross-analysed with other datasets held by police. Such further processing would raise significant privacy concerns, especially where data relating to third parties is used for this purpose. Where data obtained by mobile phone extraction is used for a separate policing purpose, this would require additional justification and safeguards as well as further consideration about the lawful basis for that additional processing. The police would also need to consider who the data subject was in each case along with ensuring compliance with the other principles in Part 3 DPA 2018.

3.3.3 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.

Under the CPIA, police have an obligation to pursue reasonable lines of enquiry, whether these point towards or away from a suspect, and to secure materials in order to prevent them from being destroyed, altered or lost.

Lines of enquiry should establish what data is sought. It is expected that decisions and justifications about the level and type of data processed should be

documented by the investigator to show necessity and justification, and ensure data obtained is adequate, relevant and not excessive.

The CPS document 'A guide to "reasonable lines of enquiry" and Communications Evidence'[72] reminds police and prosecutors that there "will be cases where there is no requirement for the police to take the media devices of a victim or others at all, and thus no requirement for even a level 1 examination to be undertaken"[73]. It also suggests that, where necessary to preserve evidence, it may be prudent to hold a complainant's phone until the suspect has had an opportunity to comment on the allegation. Whilst being parted from their phone will clearly be an inconvenience to the complainant, deferring a decision on the strict necessity for their device to be examined may eliminate avoidable processing (and hence intrusion).

Whilst accepting that the data processed must be adequate for the identified reasonable lines of enquiry, the Commissioner has significant concerns about the processing of potentially excessive data. For example, whilst the immediately obvious parameters around an investigation might be SMS messages between two particular individuals over a specific time period, the police will often extract much more data from the device. Two justifications were presented for this.

Firstly, many of the kiosks used in forces are configured in a way that does not allow the selection of specific data to be extracted at a very granular level. In the example above, it may only be possible to extract **all** SMS messages. Some only allowed the selection of either all standard text-based information (eg contacts, SMS, call log, etc) or all data (including multimedia and app data). The specific technology implementations therefore appeared to be driving behaviours in the situations observed during this investigation.

The second claim practitioners made to justify broad data extraction was their concerns about the potential for defence solicitors or lawyers to request mobile phone data that may not have been initially obtained by the police. This would most commonly occur when there had been little or no contact between prosecution and defence teams until some time into the investigation. Forces would therefore attempt to mitigate the risk of this by taking more data than was obviously relevant at the time of the initial extraction, in case it was needed later in the investigation.

HMCPSI noted in its 2019 rape inspection that some 40% of requests from prosecutors were not proportionate and stated "some prosecutors are still asking for a full download of a complainant's or suspect's phone. We think this may be

[72] https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence
[73] paragraph 13 CPS guidance

because of a lack of awareness of the types of download that are available, and what they can provide"[74].

This practice leads to the extracting, and therefore processing, of vast amounts of data about individuals of no relevance to investigations. There was no evidence of forces attempting to abstract and delete non-relevant sensitive personal data once it had been extracted. In all the cases observed in the investigation, the forces stated that they would retain the extracted material as a whole in its original form, citing CPIA requirements and preservation of the integrity of the extraction.

Force practitioners shared with the investigation team documents and guidance about procedural aspects of extraction and quality standards. Whilst this provides a basic level of assurance, there was no evidence of specific guidance on the formulation of a forensic investigative strategy, how this leads to reasonable lines of enquiry, and how these lines of enquiry result in MPE actions that reflect consideration of proportionality and necessity. As a result, in many cases, we saw a tendency toward a mobile extraction being the default position.

In the absence of evidence of the explicit documentation of lines of enquiry leading to the requirement for MPE to be conducted, there is a risk that the converse has been the case – that MPE has been used to formulate lines of enquiry.

The seriousness of the crime under investigation did not appear to be a key consideration in determining the extent of the extraction and therefore the level of impact on privacy. In particular, it was not clear that adequate attention was given to the use of non-forensic means (eg officer statement of what has been observed). This would avoid having to extract data and restrict the processing of sensitive data to what was strictly necessary.

The ICO accepts that different stakeholders may have conflicting views about the level of examination of mobile phone data. From the perspective of a suspect, or those representing a suspect, an examination of their phone data may identify material that either undermines or assists the case. If this is very narrowly focussed, key evidence may be missed. Conversely, from a complainant's perspective, searches beyond the bounds of identifying material about the alleged offence (a so-called 'fishing expedition') may be used as a tool to attack or undermine credibility. Ultimately, it will always be for the investigator to determine adequacy and relevance, but it is vital that the investigator's approach has the confidence of suspects, complainants and witnesses.

It is essential that all extractions and searches are **based on clear lines of enquiry**. A phased approach is suggested, where justification and authorisation

[74] Paragraphs 5.22 and 5.52 https://www.justiceinspectorates.gov.uk/hmcpsi/wp-content/uploads/sites/3/2019/12/Rape-inspection-2019-1.pdf

are documented at each stage, with clear parameters being set for searching. If further examination is considered appropriate, then this must be justified and further authorised each time.

3.3.4 Fourth principle: Accuracy

The fourth principle states that data must be accurate and, where necessary, kept up to date, and controllers must take every reasonable step to ensure that inaccurate personal data is erased or rectified without delay, having regard to the law enforcement purpose for which it is processed. 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.

It is acknowledged that granular analysis of large volumes of data taken from mobile devices poses a significant challenge to the police and prosecuting authorities. Whilst it would be possible to note at the time of extraction whether the device was taken from a complainant, witness or suspect, the investigation found that the data about all the data subjects found on the device tends to be kept together as a bulk of data and there is no categorisation within each download. Although there may be some mitigation of the associated risks whilst the data remains within the forensic environment, there is a clear risk of compliance failure if this categorisation is not completed and the data is further analysed or combined with other datasets.

The Forensic Science Regulator (FSR) mandates in her codes of practice and conduct[75] that police forces are accredited to the international laboratory standard ISO/IEC17025[76]. This standard is intended to provide reassurance about the validity of methods used, in this case, to extract data from devices, in terms of the accuracy and repeatability of the method. However, in her 2018 Annual Report[77], the FSR reported a low level of achievement of the required standard across policing. This non-conformance has to be reflected in statements to courts whenever mobile phone evidence is introduced. There is therefore a lack of certainty around the integrity of data taken from devices, particularly about its completeness. Furthermore, the accreditation only covers the forensic procedures, offering no assurance about the onward handling of digital material beyond the forensic extraction, and it is important that safeguards are in place at every stage.

[75] https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2017
[76] https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en
[77] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786137/FSRAnnual_Report_2018_v1.0.pdf

3.3.5 Fifth principle: Storage limitation

According to the fifth principle, law enforcement 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.

Requirements for the retention of data are set out in the CPIA and the College of Policing Authorised Professional Practice (APP) on management of police information (MoPI)[78]. Whilst it was clear that forces had an awareness of the rules and guidance, the absence of joined-up systems and organisational procedures introduces a risk of non-compliance.

Site visits revealed that a force could have multiple copies of the same material retained on systems which are not always interconnected, for example within the forensics department and with the other data relating to the specific investigation. Access to forensics department systems is (rightly) restricted to specialist staff, and it was not always the case that there were organisational triggers for review and potential deletion of materials across all relevant departments and systems. This lack of a joined-up approach introduces the risk of data review and retention policies not being effectively implemented, leading to lack of control over data and potentially non-compliance with legislation.

It is acknowledged that a number of forces are considering the potential for digital asset management systems that can be used to manage digital forensic assets throughout their lifetime, but their implementation across all forces is not imminent.

3.3.6 Sixth principle: Security

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, according to the sixth principle.

In order to undertake a data extraction, staff are required to identify and authenticate themselves with the extraction devices, and this provides a basic level of assurance.

However, not all of the kiosks used in Level 1 extractions had been configured to be able to encrypt data once it had been extracted and was being exported to other digital media. This risks unauthorised access or unintentional disclosure, given that, in many cases, the digital media devices (CDs, DVDs and USB drives) were conveyed by relatively insecure means (being left to be collected by couriers, for example).

[78] https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

There is the potential for kiosks to be networked and for extracted data to be transferred to a server, in which case the transfer would take place through a secure and encrypted channel. This would be positive from an information management perspective to ensure the integrity of the data, and minimise the exposure of data, notwithstanding any cyber risks that could arise.

3.4 Privacy information

Section 2.2.6 set out the information controllers are required to provide to data subjects.

The challenges in establishing, prior to processing, who data subjects are when undertaking MPE, have already been outlined in this report (see section 2.4.2). This makes it all the more important for forces to explain clearly what is involved in MPE, including the lawful basis being relied upon, the fact that this involves sensitive processing, and the specific rights of data subjects. If forces consider it is justifiable to derogate any of the Part 3 DPA 2018 rights (for example by removing the right to erasure due to the requirements of a criminal investigation), they must provide details of this and explain it clearly.

As stated in section 3.3.1, there was a lack of consistency between forces about the lawful basis being relied upon, and a considerable variation in the information provided to individuals when their phones were taken. It is essential that this information is consistent with the underlying condition for processing and that any advisory materials contain all the information set out in section 2.2.6 and can be easily accessed and clearly understood.

In addition, there are concerns about privacy information provided by individual forces. A number of forces have adopted similar wording in their privacy notice on their website. As an example, the Metropolitan Police privacy notice[79] includes:

> "Occasionally, where there are no other appropriate grounds, the Met may ask for your explicit consent in order to lawfully process your data. This will only happen in specific and limited circumstances and won't usually be relevant to law enforcement data. When we do require consent, we will explain clearly what we are asking for and how we will use it. Consent must be freely given, specific and informed and there must be a genuine choice about offering your data. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

[79] https://www.met.police.uk/privacy-notice/ (viewed on 9 December 2019)

> If we have asked you to provide your consent in order to process your personal data, you also have the right to withdraw your consent as any time. When we ask for your consent, we will tell you how we will process your data, how long we will keep it for and the steps we will take to delete it. We will also outline the steps we will take if you decide to withdraw consent."

Whilst the MPS notice, in common with other forces' privacy notices, suggests that the reliance on consent is only in specific and limited circumstances, NPCC's notice (see section 3.3.1) suggests that consent should be routine practice. Our interpretation of data protection legislation is that Consent as a condition for processing (s35(2)(a)) in MPE cases **is highly unlikely to be an appropriate condition** police can rely upon due to the standards that need to be met, as set out in data protection law and supporting conventions and recitals. It is assessed that where law enforcement seek to process data in order to prevent, investigate, detect or prosecute criminal offences, it is more appropriate to rely upon the second condition as set out in s35 (2)(b), namely strictly necessary for a law enforcement purpose.

In view of this, the notices risk misleading and confusing individuals about the basis on which their data is being processed and their ability to stop the processing by withdrawing Consent.

As above, the Commissioner's view is that even where Consent as a specific condition for processing is not applicable, the alternative condition (strictly necessary for the law enforcement purpose) should not be regarded as a coercive option and police should still rely on a consensual and informed approach. This should clearly explain to individuals:

- the processes that will be followed;
- the legal basis and justification for processing to take place;
- how their personal data will be used, secured and disposed of; and
- the rights and choices open to them.

The forms that the NPCC circulated for forces to use as exemplars of information to provide to complainants and witnesses when their devices are taken are not yet fully compliant with DPA 2018 and are in need of review and revision in light of the requirements set out in this report. Individual forces need to ensure that their notices reflect the points in this report.

3.5 Data protection by design and default

The requirements for forces to have in place appropriate technical and organisational measures designed to implement effective data protection principles and safeguards were set out in section 2.2.7.

The investigation found that the specific hardware and software tools offered by MPE vendors had capabilities designed to minimise intrusion and maximise privacy (eg by allowing focused extraction of specific pieces of data). However, the individual implementations in forces had simplified user interfaces that did not allow use of this privacy-enhancing functionality, and this has led to more data than strictly necessary being routinely extracted and processed.

This is compounded by the fact that the 'cradle to grave' handling of MPE data is not yet subject to clear policy and rigorous enforcement that would be appropriate for this highly intrusive process and the sensitive data involved.

3.6 Logging

The requirement for law enforcement processing logs to be maintained was set out in section 2.2.8.

Whilst there is assurance in audit logs which show the steps an individual officer might have taken when extracting data from a device from log-in to the end of extraction, not all forces have processes or technology to track (in particular) access to the data beyond this point. This is particularly the case where forces are yet to implement any form of digital asset management system and a number of disparate systems are used. In this case, there is a reliance on contemporaneous notes and statements made by officers. In the absence of an end to end system forces are reliant on an investigation officer's notes or records as the log. Depending on the accuracy and thoroughness of this record, it will make it more difficult for forces to demonstrate compliance with the legislation and may make it harder for data subjects to exercise their rights.

3.7 Data protection impact assessments

Section 2.2.9 of this report outlined the requirement for police forces to complete a DPIA when designing processing that might result in a high risk to the rights and freedoms of individuals. 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 Article 8 ECHR.

No DPIA applications have been submitted by police forces for "prior consultation". It is not clear whether DPIAs have been undertaken by all forces when processing extracted mobile phone data under DPA 2018. This makes it difficult to objectively assess the extent to which they have considered risks associated with the processing.

4. Key findings and recommendations

This section summarises the key findings of the investigation and sets out the ICO's recommendations for action to be taken by police forces and others to provide assurance that individuals' personal data is being processed fairly and in accordance with the law.

4.1 Legislative framework

The investigation revealed the complex interplay between human rights, criminal justice and data protection legislation. One consequence of this is a lack of agreement between different stakeholder groups and between different police forces on how to interpret and apply the law.

The Commissioner strongly believes that there should be a statutory code or equivalent measure to assist in providing greater clarity and foreseeability in order to address these and other inconsistencies. This code should cover a range of agencies and organisations to ensure the complex inter-relationships of law are fully set out.

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.

4.2 Lawful basis

The investigation uncovered an inconsistent understanding and application of data protection law across the policing community about the legal basis for processing personal data extracted from mobile electronic devices.

The advice issued by the NPCC about Consent as the lawful basis for processing is inadequate and in need of revision. A revised version must provide clarity about the underpinning lawful basis, and make clear the high standards required for Consent to be valid. Where Consent is not a valid condition, any advice to data subjects must address the strict necessity condition for sensitive processing and show consideration of any other relevant legislation, eg HRA and/or IPA.

Section 35(2)(1) of Part 3 DPA 2018 (Consent of the data subject) cannot necessarily be relied upon in any particular case as the condition the processing of personal data from mobile phone extraction. In order to comply with the law, Consent needs to be "freely given, specific, informed and unambiguous"[80]. Article 7 GDPR also sets out further conditions for Consent, with a specific provision for the right to withdraw Consent at any time. Setting aside the specific requirements of the DPA 2018, there is a fundamental issue specific to MPE in that the data subjects relating to a specific device will tend to be numerous and not always identifiable until the processing has taken place. This means it will be difficult in these circumstances to pass the threshold for Consent to be applicable.

When MPE takes place, there is a high likelihood that sensitive personal data will be processed and police should proceed on that basis. The law requires that a higher threshold of strict necessity should be met for this type of processing, but this higher threshold does not appear to be routinely considered in mobile phone extraction processes. Where Consent standards cannot be met, the processing is permitted only:

- where strictly necessary for the law enforcement purposes;
- the processing meets one of the conditions in Schedule 8; and
- at the time when the processing is carried out, the controller has an appropriate policy document in place[81].

For the avoidance of doubt, the fact that Consent in data protection law is unlikely to be the valid condition for processing does not mean that the alternative condition (strict necessity for a law enforcement purpose) should be seen as a coercive option in the case of complainants and witnesses. It is not. A consensual approach ensures the complainant or witness is clear and informed about their rights and choices, understands the lawful basis and justification for processing, how their data and privacy will be safeguarded and their rights

[80] Article 4(11) GDPR
[81] s35(5) DPA 2018

regarding objection. This seeks to ensure that the autonomy and agency of an individual is supported as far as processing in a law enforcement context allows, even where data protection Consent standards are not met.

Meaningful engagement with device owners can assist with the application of the Bank Mellat test which goes towards demonstrating the fairness and lawfulness of the processing, in particular the strict necessity to impact the right to privacy of that person and others whose data is held on the device, namely:

1. the extent to which there is a justifiable, reasonable line of enquiry that involves interrogation of sensitive digital data;
2. whether and why MPE would be required to satisfy the line of enquiry;
3. what other, non-forensic means have been considered, and why they would not be sufficient; and
4. whether the importance line of enquiry, in the context of the seriousness of the matter being investigated and its wider impact, justifies the impact on the privacy of the owner of the phone and others whose data will be processed from the phone.

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.

4.3 Necessity and proportionality

At the heart of every investigation is the obligation to pursue all reasonable lines of enquiry, whether these point towards or away from the suspect. This comes from the Criminal Procedure and Investigations Act 1996 and the relevant codes issued under and in pursuance to that Act. It is therefore accepted that investigations will frequently involve extracting a large amount of data from the mobile device in order to satisfy this obligation.

However, the investigation found that data extracted and processed from devices appeared excessive in many cases, with little or no justification or demonstration of strict necessity and proportionality. This applied equally to

extractions and subsequent searching and analysis of extracted data. There was insufficient evidence of a phased approach being taken which demonstrated the justification and authorisation at each stage, and a direct link between reasonable lines of enquiry was not evident.

Inconsistencies in the approach to what data should be extracted and used can result in a variation or unevenness in the progression and outcome of criminal investigations.

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.

4.4 Standards and accreditation

The investigation found that many forces had failed to meet the deadline set by 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 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.

4.5 Non-relevant materials

The ICO acknowledges the challenges associated with balancing the CPIA obligations to retain relevant materials against the practical difficulties in separating out material found not to be relevant to the particular investigation. This reinforces the point that sensitive processing should take place only when strictly necessary, and effective safeguards must be in place to prevent unauthorised access or disclosure (including encryption of **all** extracted data).

The investigation found that forces were not able to demonstrate that they were taking all reasonable steps through policy and technology to mitigate the risks associated with holding personal data taken from mobile phones that was not relevant to the investigation. This is of particular concern when the data relates to individuals who are not connected to the investigation.

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.

4.6 Processing limitation

Before charging decisions can be made, CPS Early Investigative Advice (EIA) and associated action plans sometimes place obligations on the police that require the extraction and search of material that falls outside what the police might

otherwise have considered to be a reasonable line of enquiry. This increases the risk of excessive data entering the criminal justice system.

The investigation found that current practices of large scale extraction and disproportionate searching result in the acquisition and retention of large amounts of excessive data. This presents further risks if there is insufficient regard given to all of the law enforcement processing principles and associated safeguards set out in DPA 2018.

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.

4.7 Retention periods

The investigation found that some police forces were yet to implement end-to-end processes and systems that linked forensic extractions and subsequent search and analytical results to investigative and criminal justice processes. These forces were not able to provide assurances that they were effectively managing their mobile phone data.

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.

4.8 Privacy information

Section 44 DPA 2018 places obligations on processors to provide a range of information to individuals to help them understand how their personal data is going to be processed. However, the investigation found that complainants, witnesses and suspects are not always provided with sufficient information to fully comply with these requirements, subject to any variations permitted in s44(4)-(7) DPA 2018. Victims' groups reported that a lack of meaningful engagement with police and limited privacy information for individuals may undermine public confidence in reporting a serious crime and its subsequent investigation.

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.

4.9 Training

As part of the investigation, the ICO reviewed material distributed by the National Police Chiefs' Council (NPCC). The ICO was concerned with the focus on processing relying on data subjects' consent. Whilst the information did address some concerns about the reasonable lines of enquiry, it stopped short of covering the full range of issues associated with this sensitive processing.

Feedback from forces revealed a lack of consistency in application of the principles contained in the NPCC distribution, increasing the risk that individuals in some force areas may be afforded a lower or inadequate degree of protection against privacy intrusion and excessive processing.

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.

4.10 Technology refresh

The investigation saw examples of projects being undertaken to evaluate new technology for analysis of extracted data and was invited to review the specification of requirements of new systems. The ICO was concerned that considerations about data protection obligations or privacy by design and default principles were not sufficiently prominent in these projects.

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.

4.11 Data Protection Officers

GDPR requires that public authorities (including police forces) have in place a Data Protection Officer (DPO) to advise on data protection matters and assist with compliance with data processing legislation. The investigation found that DPOs were not always consulted when designing processing operations. Enquiries from police forces received by the ICO demonstrate that there are sometimes inconsistencies between what DPOs consider compliant and the actual practice of investigators. More effective collaboration by MPE practitioners and DPOs should assist in ensuring that the principle of privacy by design and default is respected and that all requires policies and documentation are in place.

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.

4.12 Data protection impact assessments

The investigation did not find evidence of DPIAs being in place for all MPE operations. The Commissioner considers that, whilst there is only a legal requirement to carry out a DPIA prior to commencing **new** processing, it would be beneficial to do this for any existing processing. This would assist police forces with clearly setting out the lawful basis and demonstrating that they have considered and mitigated all relevant risks to the greatest extent possible. This

is particularly important when considering a potential change to the lawful basis for processing.

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.

4.13 Ongoing reform

The Commissioner has received representations from groups on behalf of victims raising their concerns about a wide range of issues associated with the processing of data from individuals' mobile phones and the impacts these have on the individuals concerned and more generally confidence in the criminal justice system.

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.

5. Conclusions

Law and order are fundamental to the maintenance of civil society and with this comes the right to a fair trial. Police forces across England and Wales, as in the rest of the UK, have the duty to investigate crimes and pursue all reasonable lines of enquiry to produce evidence that points towards or away from suspects, and they must do this whilst upholding the original Peel principles[82] that were intended to define an ethical police force. One of these principles is "to recognise always that to secure and maintain the respect and approval of the public means also the securing of the willing co-operation of the public in the task of securing observance of laws." The Commissioner is concerned that questions raised about the way in which police forces routinely access and extract the contents of mobile phones suggest that there may have been some erosion of this public confidence. This investigation has considered whether all appropriate safeguards are in place to ensure that individuals' privacy is not unduly impacted by police mobile phone extraction, and this report makes recommendations that, if implemented effectively, should contribute to restoring this confidence.

This report has set out in one place, for the first time, all the legislation that is relevant to the extraction of mobile phone data by police in the context of criminal investigations.

The investigation was complex, involving a wide range of stakeholders. It highlighted the challenge of applying a range of general legislation to a specific innovative practice, where privacy safeguards have not necessarily been designed in from the outset.

It is recognised that, in many cases, the use of mobile phone extraction can be an essential tool in ensuring offenders can be brought to justice. However, this practice, involving some of our most sensitive personal information, can be highly intrusive into individuals' private lives and has the potential to impact significant numbers of people not involved in the investigation. It is therefore a tool that must be used only to the extent it is strictly necessary and always applied in a way that is fair and in accordance with the law.

Failure to do so will result in diminishing confidence in the criminal justice system and a reluctance on the part of complainants in particular to come forward and report crimes for fear that their personal digital data and privacy will be compromised through non-compliant practices.

The Commissioner understands the police and prosecutors' rationale for relying on Consent rather than coercive powers for taking possession of phones from complainants and witnesses and processing data from these devices. The desire

[82] https://www.gov.uk/government/publications/policing-by-consent

expressed by civil society groups and victims' representatives for complainants to have control over what digital data is made available to the police and their view that the individual's consent forms the best means of achieving this control also resonate with the ICO. However, Consent in the context of data protection raises particular challenges for data controllers and data subjects and in our view is very unlikely to be the appropriate condition for processing. Whilst there is an alternative and, in our view, more appropriate condition for processing, it is the Commissioner's strong view that this condition should in any event take place on the basis of a consensual and informed approach and should not be viewed as a coercive option. This alternative condition also requires the police to ensure that the processing passes the higher bar of strict necessity required when sensitive personal data is being processed.

This is a complex picture, with very different views on aspects of the law. Data protection is only one part of a complex picture. Work needs to continue at pace with government departments, civil society groups, police, prosecutors and regulators, to ensure that those involved in MPE have the right knowledge, training and understanding to ensure compliance with the law and that those affected by it understand how and why their data is processed and receive the protections afforded by the legislation. We have also asked relevant departments charged with reviewing the Victims' Code and the CPIA to take the opportunity provided by the reviews to fully incorporate data protection and privacy considerations.

This report provides clear guidance and recommendations about improvements required to achieve a consistent application of the law across England and Wales. These should be implemented as soon as possible and are not dependant on other programmes of work aimed at improving disclosure for example. Key is the call to government to introduce a statutory code of practice that provides increased clarity and foreseeability about how the personal data taken from complainants and witnesses is handled and in what circumstances MPE is appropriate. Such a code would also provide a platform for setting out the role that consent has in this process.

The individual recommendations are focused on raising standards of practice, including by advising the police to assume the material held on a phone amounts to **sensitive** data from the outset. This higher bar affords a greater degree of protection for data subjects and will provide increased confidence in the handling of personal data and the approach to privacy in this context. The report provides advice to investigating officers and decision makers about how best to comply with the existing law.

The findings of this work will feed directly into the broader investigation by the ICO into the processing of victims' data in the criminal justice system which the ICO will report on later this year.

The ICO notes the range of work underway into many of the issues in scope in this investigation: the national disclosure improvement plan (NDIP), the recommendations in the Attorney General's review of the effectiveness and efficiency of disclosure and the HMCPSI report. It is important that the ICO investigation is considered alongside these reports.

The scale and breadth of the challenge clearly requires a more integrated whole-system approach so that recommendations in one area do not result in adverse consequences for another. The ICO will continue to support cross-organisation efforts to improve the situation and calls for a national consortium to work together to tackle these complex issues.

Enquiries into MPE practice in Scotland and Northern Ireland continue, and the Commissioner's findings about these devolved jurisdictions will be published in due course.

On publication of this initial report, the Commissioner will engage further with the NPCC and the College of Policing to request that they collaborate to design and publish a plan to assist police forces in addressing the issues identified by this investigation. The Commissioner will also offer NPCC support in redrafting digital processing notices. In addition, she will write to all Chief Constables, Commissioners and Police and Crime Commissioners to share the report with them and remind them of their data protection obligations. The Commissioner recognises that these improvements will take time to implement and will continue to monitor progress including via her audit powers (and where appropriate in collaboration with HMICFRS) to ensure that necessary steps are taken to address the data protection issues identified.

List of abbreviations

AGO ..... Attorney General's Office

CJPA ..... Criminal Justice and Police Act 2001

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

FSR.....Forensic Science Regulator

GDPR .....General Data Protection Regulation 2018

HMCPSI .....HM Crown Prosecution Service Inspectorate

ICO..... Information Commissioner's Office

IPA ..... Investigatory Powers Act 2016

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

NPCC .....National Police Chiefs' Council

PACE..... Police and Criminal Evidence Act 1984

PI .....Privacy International

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