Information Commissioner's Office

Mobile phone data extraction by police in Scotland

Investigation report

June 2021

ico.
Information Commissioner's Office

Foreword

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

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

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

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

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

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

This new report outlines our findings around Police Scotland's practices. The investigation found positive steps had been taken to improve compliance with data protection legislation. In particular, in response to the Scottish Parliament Justice Sub-Committee on Policing, policies had been improved around the use of 'cyber kiosks' to view the contents of devices to ascertain whether they contain material of potential evidential value.

Further work is needed. The same level of consideration given to the data protection implications of cyber kiosks must now be given to all mobile phone extraction operations, including the Digital Forensics Hubs used to extract data from phones.

Due to the nature of the investigation and prosecution system in Scotland, the respective data protection roles of Police Scotland, the Crown Office and Procurator Fiscal Service, and the Scottish Police Authority also need clarifying.

The ICO will continue to support Police Scotland's work, and I will be expecting the force to provide evidence of its compliance with the law in the coming months.

This report is published alongside a similar report covering Northern Ireland, and an updated report covering England and Wales. We are encouraged by the consensus across the UK regions that action is needed, but there is further work to be done.

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

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

Elizabeth Denham CBE
UK Information Commissioner

Contents

Executive summary

Background

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

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

The ICO subsequently engaged with Police Scotland in order to assess the extent to which the organisation complies with data protection legislation in undertaking its MPE operations.

The operating model in Police Scotland comprises two separate operations:

- cyber kiosks, that it uses to view the contents of devices to ascertain whether they contain material of potential evidential value.
- Digital Forensics Hubs, that extract data from devices.

In 2018-19, the Scottish Parliament Justice Sub-Committee on Policing scrutinised Police Scotland's cyber kiosk implementation project. This prompted the force to consider, in detail, the lawful basis for its kiosk operations and put measures in place to provide the public with information about their processing activities. Whilst Police Scotland should have undertaken a data protection impact assessment (DPIA) prior to beginning the roll-out of this new technology, we commend the force on engaging positively with the Sub-Committee, the ICO and other stakeholders in order to take onboard their critique and revise its governance accordingly.

The force demonstrated a considerable amount of learning from its engagement with the Scottish Parliament, the ICO and other stakeholders. It can now show, through its policies, a largely compliant approach to the processing within the scope of its cyber kiosk operations. However, some of the details of the governance documentation require further work.

More importantly, Police Scotland must apply the same level of detailed consideration to all of its MPE operations and demonstrate compliance with data protection legislation for its end-to-end processing. This should include

- viewing the contents of a device using a cyber kiosk;
- where appropriate, the data's extraction at a Digital Forensics Hub; and
- the subsequent analysis, disclosure and management of the extracted data.

Scotland is unique in the UK in having a unified prosecution system where the Crown Office and Procurator Fiscal Service has overall responsibility for the investigation and prosecution of crimes. Criminal justice legislation requires Police Scotland to comply with lawful instructions it receives from Procurators Fiscal. In addition, the Scottish Police Authority has a legal obligation to provide forensic services to Police Scotland and others. It is important to consider how this impacts on each organisation's accountability in relation to data protection legislation.

Recommendations

Recommendation 1: Police Scotland, the Crown Office and Procurator Fiscal Service and the Scottish Police Authority should jointly assess and clarify their mutual relationships and respective roles under the Data Protection Act 2018 in relation to law enforcement processing associated with criminal investigation.

They should use the findings of this assessment as the basis for the review and revision of the governance and relevant policy documentation around MPE.

Recommendation 2: Police Scotland should ensure it has DPIAs in place that cover all of its MPE operations, in order to demonstrate it understands and appropriately addresses the information risks associated with this practice.

To ensure compliance with data protection requirements, Police Scotland should review and update such assessments prior to the procurement or roll-out of new hardware or software for MPE and processing, including any analytical capabilities. Where it identifies residual high risks associated with new processing, the force should undertake prior consultation with the ICO, as required under s65 of the DPA 2018.

Recommendation 3: In order to provide assurance around the integrity of the data extraction processes, Police Scotland should accelerate its work to implement and maintain the standards set out in the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

Recommendation 4: Police Scotland should review and revise the information it provides to the public, including the range of documentation it publishes on its website and anything it provides directly to people during engagement. It should ensure that the documentation:

- adequately covers all processing arising from MPE;
- is consistent; and
- provides unambiguous information on privacy and information rights.

When considering this recommendation, the force should engage with, and may wish to adapt to its circumstances, the work the National Police Chiefs' Council

(NPCC) is undertaking in relation to digital processing notices as a response to recommendation 2 of the England and Wales report.

Recommendation 5: Police Scotland should review its data retention policy documentation and supplement it with materials to include:

- alignment of regular review and deletion processes across all operational, analytical and forensic environments; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that the force does not process it further and so officers cannot inappropriately access, review or disseminate the data.

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

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

Other work

In parallel with this investigation, the ICO engaged with the Police Service of Northern Ireland to examine its MPE operations. We published a separate report with these findings alongside this one.

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

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

Next steps

Police Scotland should build upon the data protection work it undertook in relation to cyber kiosks and ensure it is compliant across the full extent of its MPE operations. The ICO acknowledges the spirit in which the force's senior leadership engaged with external scrutiny. We are confident that Police Scotland understands the importance of accountability and continues to improve its approach to MPE. The force should address the recommendations we make in

this report at the earliest opportunity, in collaboration with other colleagues represented by the NPCC.

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

1. Introduction

1.1 Background

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

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

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

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

The ICO is therefore publishing three new reports:

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

1.2 Investigative approach

The ICO aimed to understand the MPE practices that the Scottish policing and justice sector currently employ. This was in order to assess compliance with data

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

protection legislation and make recommendations for any required improvements. To do this effectively, it was necessary to first examine the applicable criminal justice and law enforcement legislation in Scotland.

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

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

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

We note that the Scottish Police Authority (SPA) has a duty in law[2] to provide forensic services to Police Scotland and other Scottish criminal justice organisations. However, since the force does not engage any forensic services the SPA provides in relation to MPE, we view the SPA's operational activities to be beyond the scope of this investigation.

We are grateful to Police Scotland and the COPFS for their willingness to engage with the investigation and for the openness and candour with which they conducted the engagement. This significantly assisted the investigation, in light of the COVID-19 pandemic restrictions.

1.3 Regulatory approach

Whilst time has elapsed between the England and Wales report's publication and this one, the investigation always intended to cover the UK as a whole. The ICO was therefore keen to apply the same approach to the engagement with all police forces so as to not disproportionately impact any of the forces involved. We explained in the England and Wales report that the investigation was a review of practice across the 43 police forces in England and Wales, rather than a more traditional investigation into a particular controller (an individual

[2] s31 Police and Fire Reform (Scotland) Act 2012

organisation), which might lead to enforcement action. Whilst the PSNI and Police Scotland are single organisations, the ICO adopted a similar fact-finding stance to Northern Ireland and Scotland respectively. This approach recognises the complexity of MPE and focuses on understanding and articulating the systemic change that we require, rather than targeting individual organisations.

1.4 Structure of this report

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

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

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

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

2. Current practice

2.1 Overview

Police Scotland has a two-tier system for its MPE operations:

- cyber kiosks; and
- Digital Forensics Hubs.

These each have a different role in the investigative process.

2.1.1 Cyber kiosks

Cyber kiosks are purpose-built, standalone devices that allow suitably trained officers and staff to view data stored on a range of digital devices, including mobile phones. Police Scotland uses these devices with mobile phones, tablets and SIM cards, to ascertain whether they contain material of evidential value. Through this 'triage' process, the operator of the cyber kiosk can view, but not save, extract or process in any other way, the data that the kiosk reveals.

Civil society groups claimed that Police Scotland failed to take sufficient account of privacy and information rights in its introduction of cyber kiosks. This led to scrutiny by the Scottish Parliament Justice Sub-Committee on Policing, who published a report[3] in April 2019. An independent External Reference Group (ERG), comprising a range of victim-focused, human rights and privacy professionals including the ICO, was also established to provide critique and expert advice.

The Scottish Parliament requested a pause in the roll-out of the cyber kiosks until Police Scotland completed work to establish a proper lawful basis for its operation. Through engagement with the ERG, the force clarified the lawful basis for their use of the technology and produced a range of public-facing material[4] to explain the governance around their operation.

Police Scotland completed the roll-out in August 2020, and 41 cyber kiosks are currently in use across Police Scotland to triage device enquiries.

2.1.2 Digital Forensics Hubs

Digital Forensics Hubs provide Police Scotland's core MPE capability for forensic extraction of data from devices by specialist staff. This includes the execution of Level 1 (configured logical extraction), Level 2 (logical and physical extraction)

[3] 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-
[4] https://www.scotland.police.uk/about-us/police-scotland/specialist-crime-division/cybercrime-investigations-and-digital-forensics/cyber-kiosks/

and Level 3 (specialist extraction and examination) methods. These facilities are similar to those found in other forces across the UK.

2.2 Relevant organisations

Whilst the focus of this investigation was the MPE practice of Police Scotland, it is important to understand the interaction the force has with other organisations that have statutory roles in this area.

2.2.1 Crown Office and Procurator Fiscal Service

The Crown Office and Procurator Fiscal Service (COPFS)[5] is Scotland's prosecution service. Procurators Fiscal have overall responsibility for the investigation and prosecution of crimes and are organised on a regional basis. Acting on behalf of the Lord Advocate, they have the power to direct police[6] as to the reporting and investigation of offences.

Under normal circumstances, the police investigate an offence, charge a suspect and send a report to the Procurator Fiscal who then makes a decision as to whether a prosecution is appropriate.

However, it is not uncommon for the Procurator Fiscal to intervene in an investigation to require the police to pursue a particular line of enquiry or, in the case of MPE, to acquire specific data.

2.2.2 Scottish Police Authority

The Scottish Police Authority (SPA)[7] was established under the Police and Fire Reform (Scotland) Act 2012 as an independent authority governing policing in Scotland.

One of the SPA's statutory functions is to provide forensic services[8] to a number of bodies, including Police Scotland and the COPFS.

The investigation found that Police Scotland utilised its own forensic MPE capabilities (cyber kiosks and Digital Forensics Hubs) rather than engaging any MPE services the SPA may provide. For this reason, we assessed the operational activities of the SPA to be beyond the scope of the investigation.

[5] https://www.copfs.gov.uk
[6] s12 Criminal Procedure (Scotland) Act 1995 and s17(3) Police and Fire Reform (Scotland) Act 2012
[7] https://www.spa.police.uk
[8] s31 Police and Fire Reform (Scotland) Act 2012

2.3 Process

An officer in charge (OIC) of a case commissions a request for device examination by the completion of an Examination Request Form (ERF)[9]. The ERF contains the officer's rationale for the request along with any specific requirements.

The officer submits the completed ERF to a supervisor for initial review to ensure that it meets the required policy standards for authorisation. If it meets the required criteria, the supervisor approves the ERF and forwards it to the Cybercrime Gateway, where specialist staff apply consistent standards to assess and grade submissions.

HM Inspectorate of Constabulary in Scotland commented in its "Strategic review of Police Scotland's response to online child sexual abuse"[10] on the value of the Cybercrime Gateway in ensuring that the force only progresses properly justified examinations:

> "… We found that there remains a tendency for front line officers, due to a lack of experience or knowledge, to seize devices unnecessarily for subsequent examination. The deployment of digital forensic examiners to provide on-site advice and expertise reduces this demand."[11]

The Cybercrime Gateway provides a response to the OIC, either approving the device for examination or rejecting the request, with reasons.

Depending on the circumstances of the case, requests are submitted for examination either via a cyber kiosk or a Digital Forensics Hub, and separate ERFs exist for each.

In many cases, an officer undertakes a cyber kiosk review to triage the device and establish whether there is anything of likely evidential value. If there is no such material, the force passes the device back to its owner.

If there is relevant material, then the officer submits a revised ERF, via the supervisor, with specifics of the Digital Forensics Hub examination required.

In some specific circumstances, officers must not use cyber kiosks. These include, but are not limited to:

- examinations the COPFS requests;
- enquiries relating to a complaint about the police;

---

[9] https://www.scotland.police.uk/spa-media/oudl4uvi/digital-device-examination-request-form-erf-flow-process.pdf
[10] https://www.hmics.scot/sites/default/files/publications/HMICS20200226PUB.pdf
[11] para 161 HMICS Strategic review of Police Scotland's response to online child sexual abuse

- requests by the Professional Standards Department or Anti-Corruption Unit; or
- where the device is not working or is operating in a foreign language.

These are circumstances in which officers already know the specific extraction requirements, where a triage by a human being would not be effective, or where such action might compromise the investigation's integrity.

Where someone reports a case to the COPFS, the Procurator Fiscal can commission work by issuing a formal standard forensic instruction (SFI) to the relevant OIC. The OIC then follows the ERF process described above to commission the work of the Digital Forensics Hub.

If, at any stage, an officer assesses that an SFI does not meet the criteria required to comply with policy or legislation, the OIC would engage with the COPFS to discuss revising the request.

2.4 Compliance with data protection principles

Part 3 of the DPA 2018 sets out the requirements[12] which apply to the processing of personal data for law enforcement purposes. We assess the level of compliance of Police Scotland in relation to each of the data processing principles below.

2.4.1 First principle: lawful and fair

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

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

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

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

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

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

> "(a) the processing is **strictly necessary** for the law enforcement purpose,
>
> (b) the processing meets at least one of the conditions in Schedule 8[13], and
>
> (c) at the time when the processing is carried out, the controller has an appropriate policy document in place."[14]

In section 7.3 of its "Legal basis for the seizure and examination of digital devices" document[15], Police Scotland states its basis in law for MPE to be:

> "… provided by Section 20 of the Police and Fire Reform Act 2012 (duties of a constable) and the Code of Practice made under Section 164 of the Criminal Justice and Licensing Scotland Act 2010 (obligation on police to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown)."

It does appear that the obligations arising from the Criminal Justice and Licensing (Scotland) Act 2010 (Section 164) Code of Practice – Disclosure Of Evidence In Criminal Proceedings[16] (regarding pursuing reasonable lines of enquiry and recording relevant material) may meet the requirement that processing for the law enforcement purpose is 'based on law'.

The force's legal basis document goes on, at section 7.4, to refer to the s35(5) DPA 2018 'strict necessity' condition which, again, reflects an appropriate basis for the processing.

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

---

[13] Schedule 8 DPA 2018 details the conditions for sensitive processing under Part 3 DPA 2018
[14] s35(5) DPA 2018
[15] https://www.scotland.police.uk/spa-media/5sdhf3lt/digital-device-seizure-examination-legal-basis.pdf
[16] http://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Guidelines_and_Policy/Code%20of%20Practice%20-%20Disclosure%20of%20Evidence%20in%20Criminal%20Proceedings.pdf

2.4.2 Second principle: limited purpose

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

Police Scotland evidenced a robust process by which it commissions the acquisition of data from mobile phones, including a two-stage authorisation protocol to ensure such requests are lawful and relate to a legitimate investigative requirement. It limits access to reports about data extracted to those working on the investigation.

The ICO is not aware of any processing for secondary purposes. However, Police Scotland could be more explicit as to its policy in relation to the use of analytic tools to interrogate retained digital material, especially in relation to any processing outside the Digital Forensics Hub environment.

2.4.3 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.

Police Scotland provided evidence of its commissioning process, which involves a two-stage review and authorisation protocol to ensure that it only processes legitimate requests.

It is reassuring that the force applies the same standards to viewing data using cyber kiosks as it does to the extraction of data in a Digital Forensics Hub. Subject to this condition, whilst the ICO would consider the viewing of data using a cyber kiosk to be a form of processing, we recognise that effective use of cyber kiosks can be a positive factor in reducing excessive processing.

Due to the limitations of this investigation, we could not fully examine the extent to which, in practice, Police Scotland limits extractions by specific parameters based on specific lines of enquiry. We remind the force of its obligations in this regard, especially with the further opportunities to do this following cyber kiosk triage.

2.4.4 Fourth principle: accuracy

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

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

- complainants.

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

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

In the context of MPE in the criminal justice sector, it is important that the methods Police Scotland uses to interrogate devices and extract data from them are accurate and reliable. The relevant accreditation for policing organisations is certification to the ISO/IEC17025 international laboratory standard.

The ICO notes that HM Inspectorate of Constabulary in Scotland recommends, in its June 2017 report[17] of its Thematic Inspection of the Scottish Police Authority Forensic Services, that:

> "Police Scotland should consider quality accreditation for digital forensics in line with Forensic Science Regulator recommendations, UK Forensic Strategy and wider good practice in order to support effective public performance reporting and assurance."

Police Scotland is yet to address this recommendation, though the force stated that it is seeking approval and funding for the work necessary to achieve accreditation.

In the interim, Police Scotland cannot demonstrate to externally validated standards that it is using extraction methods which produce reliable results.

2.4.5 Fifth principle: storage limitation

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

Police Scotland published its Record Retention Standard Operating Procedure (SOP)[18] and Productions SOP[19]. The ICO also accessed the digitally stored evidence SOP[20].

[17] https://www.hmics.scot/sites/default/files/publications/HMICS20170627PUB.pdf
[18] https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf
[19] https://www.scotland.police.uk/spa-media/emeh31wh/productions-sop-v6.pdf
[20] Not available on the Police Scotland website

These documents are helpful in explaining, at a high level, the principles to apply in relation to requirements around the force's retention, review and deletion of records and other materials.

Due to the investigation's limitations, the ICO could not assess the extent to which Police Scotland observed these SOPs in practice.

Whilst the SOPs are helpful documents, they lack some of the expected detail in relation to digital forensic materials of the type extracted from mobile phones.

Although the Productions SOP refers to mobile phones, there is no reference to the potential for multiple instances of records or the relationship between a production (eg a mobile phone or the image of the data extracted from it) and other records (eg working copies of the data or reports produced from it). Also, there is no consideration of the possible separation of relevant material from that which is not relevant to the case.

Given the complexity of the management of data acquired from the examination of mobile devices, Police Scotland would benefit from developing more specific policy documentation. This documentation would provide assurance as to how the force is complying with data protection legislation and not retaining material for longer than necessary.

2.4.6 Sixth principle: security

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

The provision of specialist services through Digital Forensics Hubs across Police Scotland allows the management of digital forensic materials. The ICO received a reasonable level of assurance in relation to the security of the assets that Police Scotland stores within these facilities.

2.5 Privacy information

Controllers engaging in law enforcement processing must provide privacy information that helps people understand how organisations are processing their data[21].

Police Scotland published[22] a number of 'privacy notices' that cover a range of different areas of processing across the force. Whilst these documents are

[21] s44(1)&(2) DPA 2018
[22] https://www.scotland.police.uk/access-to-information/data-protection/privacy-notices/

helpful in providing some basic information, none of the documents provide privacy information in relation to MPE or digital forensics in general.

The force's 'Digital Device Examination and Consent FAQ' document[23] also appears on the Police Scotland website. It aims to offer clarity to the public around the circumstances under which the force may take their device and what their rights are in relation to consenting (or objecting) to their device's examination.

An extract from that document states:

> "**Q3. Why does Police Scotland take and examine digital devices?**
>
> We take and examine devices where there is reasonable belief that they may contain evidence or information relating to a police investigation or incident.
>
> Doing so must be necessary, proportionate, and reasonable in the circumstances; we cannot do it "just in case" there is anything of relevance on a device. There must be a reasonable belief that it may contain evidence or information relating to a police investigation or incident."

Whilst the use of plain English is helpful, this statement does appear to give licence for justification in a wide range of circumstances. A reasonable belief that a device "may" contain information relating to "a police investigation or incident" may not be sufficiently specific to meet the criteria for the force's processing to be based on law.

The document would benefit from more close alignment with the force's statements around reasonable lines of enquiry and strict necessity, as related in section 2.3.1 of this report. It would be helpful to explain how the force considers alternatives to MPE prior to resorting to this means of pursuing the enquiry.

The following is a further extract from the FAQ document:

> "**Q5. If the police ask for my consent, do I have to give it?**
>
> No. Although your device can greatly assist an investigation, you can refuse or withdraw your consent at any time. Sometimes we might need to use one of the other powers (warrant or common law) if you refuse consent or withdraw it. This will depend on the investigation and what might be on the device.

[23] https://www.scotland.police.uk/spa-media/nqthariw/digital-examination-and-consent-faqs.pdf

> **Q6. What happens if I refuse consent, or provide consent, then later withdraw it?**
>
> If we don't use another power you will be able to keep your device, or it will be returned as soon as possible after we confirm consent is withdrawn.
>
> We will continue the investigation without your device, and still follow all other reasonable lines of enquiry.
>
> Your decision at any stage will not affect how we treat you."

These statements around consent could lead to confusion, especially in relation to its withdrawal.

The ICO previously reported, in the England and Wales report, the importance of distinguishing between:

- seeking agreement with a device holder to take possession of their device for the purpose of examining it; and
- the processing of data the device contains.

This is an important distinction that the force's public-facing documentation now clearly reflects.

A reasonable interpretation of the statements in the FAQ document is that withdrawal of consent relates only to the retention of the device. This would be consistent with the force's statements elsewhere in relation to the 'strict necessity' condition for processing. If this is the case, then Police Scotland should make clear that it would be difficult to erase the data once the organisation has it.

Police Scotland may find it helpful to consider Bater-James & Anor v R [2020] EWCA Crim 790[24] and that judgment's considerations around the impact on cases where a witness declines a request to access their device. Whilst it should not affect how the police treat a citizen (as stated in the FAQ document), it may have an impact on the case itself.

The force structures engagement with complainants and witnesses around an information leaflet providing details of the MPE process. The force asks those having their devices taken to sign a separate statement confirming the engagement took place, their understanding of the information provided, and whether or not they provide consent. This can assist people in understanding the process and having clarity about their rights, especially at a time when they may be vulnerable.

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

Police Scotland clearly makes attempts to provide information explaining the force's use of MPE to both those persons investigators engage with directly and also the wider public. However, this documentation would benefit from detailed review and revision to ensure it is sufficiently clear and consistent.

2.6 Data protection by design and default

Law enforcement controllers have an obligation to implement data protection by design and default[25]. This requires them to introduce appropriate technical and organisational measures which are designed to apply the data protection principles in an effective manner, and to integrate the safeguards necessary for that purpose into the processing itself.

The investigation team was unable to fully investigate the specifics of the particular technologies in use by Police Scotland. However, it is clear that the development work the force undertook following the scrutiny of its cyber kiosk project led to improvements in business process design and policy documentation.

However, the documentation Police Scotland provided does not suggest that the same standards apply to wider MPE operations involving the extraction and management of data from phones.

2.7 Logging

Organisations have an obligation to maintain logs of processing operations[26], including the:

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

of data.

Police Scotland's use of a dedicated Cybercrime Gateway, using standard forms and processes to authorise and carry out triage of devices using cyber kiosks, provides a level of reassurance around the maintenance of records of MPE operations.

We saw evidence that Police Scotland has the capability in the Digital Forensics Hubs to log user actions relating to data officers extract from digital devices.

[25] s57 DPA 2018
[26] s62 DPA 2018

However, it was beyond the investigation's scope to examine whether Police Scotland logs activities in circumstances where the extracted data is being processed further in other technical environments, for example in analytic environments or case management systems.

We remind Police Scotland of the requirement[27] for controllers to maintain logs that the force can make available to the Information Commissioner on request.

2.8 Data protection impact assessments

Organisations are required to undertake a data protection impact assessment (DPIA) when designing processing that might result in a high risk to the rights and freedoms of individuals[28]. This is particularly important in the case of MPE, due to the likelihood of sensitive processing and the intrusion of a nature likely to impact on the rights that Article 8 ECHR provides. The organisation must carry out and document the assessment prior to any processing taking place.

Police Scotland did not complete a DPIA prior to beginning trials of cyber kiosks. During the engagement as a result of the challenges brought by the Scottish Parliament Justice Sub-Committee on Policing and the ERG, Police Scotland developed a DPIA that covered its proposed operations for the cyber kiosks.

However, this only covered the force's use of cyber kiosks, rather than the full extent of its MPE operations. As we note in this report, not all device examinations pass through this triage process.

We acknowledge that the processing Police Scotland undertakes using Digital Forensics Hubs was in operation prior to the DPA 2018 and the associated requirement for organisations to complete DPIAs. However, in the continued absence of any privacy impact assessment or other similar risk assessment for this wider processing, Police Scotland does not provide any insight into the risks associated with the extraction, storage, further processing and management of data from mobile phones.

[27] s62(5) DPA 2018
[28] s64 DPA 2018

3. Key findings and recommendations

Police Scotland now has a relatively mature digital forensics function that carries out MPE. The force had the benefit of the scrutiny of the Scottish Parliament Justice Sub-Committee on Policing and the ERG. It is clear that the engagement with these bodies and with the ICO directly greatly assisted the force in understanding its obligations and demonstrating its compliance with data protection legislation. We commend the force in taking onboard, and responding positively to, this constructive challenge.

Police Scotland should also take the opportunity to learn from the substantial amount of work taking place across the UK following the publication of the ICO's England and Wales report. The majority of this is directly relevant to Scotland. We therefore encourage the force to collaborate with these developments, so that it can both feed in the experience gleaned from the scrutiny of its own operations and (to the greatest extent possible) implement the outputs from this wider work.

Also, whilst Police Scotland does not usually come under the auspices of the College of Policing guidance[29], it would significantly benefit from reviewing the Authorised Professional Practice (APP) and preparing similar guidance for use in Scotland. This would assist in providing consistent standards of compliance with data protection legislation and respect for the information rights of citizens regardless of where they are in the UK.

3.1 Roles and relationships

Given the importance of understanding the accountabilities and responsibilities of organisations under data protection law, it is helpful to reflect on the respective roles of Police Scotland, the Procurators Fiscal and the SPA in relation to criminal investigations.

The Chief Constable of Police Scotland and the Procurators Fiscal are each a "competent authority"[30] by virtue of their being named in Schedule 7 DPA 2018[31], enabling them to be controllers for processing under Part 3 DPA 2018.

The SPA may meet the alternative qualifying condition[32] to be a competent authority due to its statutory function in relation to law enforcement purposes.

[29] The College of Policing is the professional body for those who work in police forces in England and Wales, and it produces Authorised Professional Practice for those forces.
[30] s30 DPA 2018
[31] s30(1)(a) DPA 2018
[32] s30(1)(b) DPA 2018

A controller:

> "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"[33]

A processor:

> "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[34]

In cases where a Procurator Fiscal is directing an investigation or prescribing how Police Scotland undertakes particular lines of enquiry, there is the question of whether Police Scotland is effectively processing on behalf of the Procurator Fiscal, who is acting as a controller. Equally, both parties could be joint controllers.

Similarly, it is conceivable that the SPA may act as either a controller or a processor in relation to law enforcement processing for criminal investigation.

This is not purely an academic consideration; it is important that organisations are clear about their mutual legal obligations and that the public understand their information rights and what they might expect from the different parties.

The ICO appreciates that this matter has implications wider than MPE, and therefore organisations should take care to analyse the situation and assess the impacts of any conclusions they draw.

Recommendation 1

Police Scotland, the Crown Office and Procurator Fiscal Service and the Scottish Police Authority should jointly assess and clarify their mutual relationships and respective roles under the Data Protection Act 2018 in relation to law enforcement processing associated with criminal investigation.

They should use the findings of this assessment as the basis for the review and revision of the governance and relevant policy documentation around MPE.

[33] article 4(7) UK GDPR
[34] article 4(8) UK GDPR

3.2 Data protection impact assessment

The force has lessons to learn in relation to the systematic assessment of the impact of new data processing operations, especially in cases where the processing is likely to involve sensitive personal data.

The most significant learning point from the scrutiny of the Scottish Parliament Justice Sub-Committee on Policing, the ERG and this investigation is the requirement for the force to engage the DPIA process **prior to** commencing any new, high risk processing.

In addition, it is important that any DPIA reflects the full extent of the relevant processing by the controller, rather than focusing on one particular technology that is part of a wider end-to-end process. Currently, the force has a DPIA for its cyber kiosk processing but not for the processing carried out by the Digital Forensics Hub. Police Scotland has been using this latter processing for some time and it predates the introduction of the legislation requiring DPIAs. However, conducting an end-to-end review that leads to a DPIA would provide the force with opportunities to address the areas where it is not fully compliant.

Recommendation 2

Police Scotland should ensure it has DPIAs in place that cover all of its MPE operations, in order to demonstrate it understands and appropriately addresses the information risks associated with this practice.

To ensure compliance with data protection requirements, Police Scotland should review and update such assessments prior to the procurement or roll-out of new hardware or software for MPE and processing, including any analytical capabilities. Where it identifies residual high risks associated with new processing, the force should undertake prior consultation with the ICO, as required under s65 of the DPA 2018.

3.3 Standards and accreditation

Police Scotland is yet to demonstrate that it meets the requirements for certification to the ISO/IEC17025 international laboratory standard, as set out by the Forensic Science Regulator and as HM Inspectorate of Constabulary in Scotland recommends. This means that there is an absence of assurance in the integrity (and hence accuracy) of the data the force extracts from devices.

Recommendation 3

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

3.4 Privacy information

Police Scotland provides a large amount of information in relation to its processing activities. However, it could make the information relating to MPE clearer and more consistent, particularly in relation to:

- the specifics of this processing; and
- the role of consent or agreement to provide devices for examination.

Police Scotland may wish to refer to the work the NPCC is carrying out to improve and provide consistency in the information officers provide to people they engage with when seeking agreement to take their device. This draws upon, in particular, the findings in Bater-James & Anor v R [2020] EWCA Crim 790. This work should also be equally of benefit to Police Scotland as it is to other forces across the UK.

Recommendation 4

Police Scotland should review and revise the information it provides to the public, including the range of documentation it publishes on its website and anything it provides directly to people during engagement. It should ensure that the documentation:

- adequately covers all processing arising from MPE;
- is consistent; and
- provides unambiguous information on privacy and information rights.

When considering this recommendation, the force should engage with, and may wish to adapt to their its circumstances, the work the NPCC is undertaking in relation to digital processing notices as a response to recommendation 2 of the England and Wales report.

3.5 Data management

Whilst there is evidence that Police Scotland considered the lawfulness of viewing and extracting data from mobile phones, the investigation identified

some gaps in documented policy relating to the management of that data once the force acquires it. In particular, the documentation should cover the end-to-end processing of the digital forensic data, both within and outside the forensic environment.

Recommendation 5

Police Scotland should review its data retention policy documentation and supplement it with materials to include:

- alignment of regular review and deletion processes across all operational, analytical and forensic environments; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that the force does not process it further and so officers cannot inappropriately access, review or disseminate the data.

3.6 Consistency of approach

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

Recommendation 6

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

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

4. Conclusions

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

This investigation found that Police Scotland provided a reasonable level of assurance that the force is complying with data protection legislation and having due consideration for privacy issues. This is perhaps to be expected, given the level of scrutiny from which the force benefitted in relation to its cyber kiosk project.

Police Scotland should further improve confidence in its MPE operations by implementing the recommendations we make in this report.

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

- the ICO's England and Wales report[35];
- a discontinued judicial review[36]; and
- the recently published Attorney General's Guidelines on Disclosure[37] and CPIA Code[38].

Whilst the Scottish criminal justice system is distinct from elsewhere in the UK, the principles underpinning these wider developmental activities addressing privacy and information rights issues are relevant to considerations in Scotland. We therefore encourage Police Scotland to engage with NPCC colleagues and the College of Policing to ensure an efficient and consistent response.

The ICO is committed to assisting stakeholders in understanding these recommendations and would be very happy to continue engagement with Police

---

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

[36] A claim for judicial review was established on behalf of two women who had reported rape to the police and were claiming that the downloading of the whole of their personal digital data was not relevant to the allegations they had made.

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

[38] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf

Scotland and others in ensuring they embed the necessary changes into practice.

List of abbreviations

APP ..... Authorised Professional Practice

COPFS ..... Crown Office and Procurator Fiscal Service

DPA 2018 ..... Data Protection Act 2018

DPIA ..... Data protection impact assessment

ECHR ..... European Convention on Human Rights

ERF ..... Examination Request Form

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

HRA ..... Human Rights Act 1998

ICO ..... Information Commissioner's Office

IPA ..... Investigatory Powers Act 2016

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

NPCC ..... National Police Chiefs' Council

OIC ..... Officer in charge

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

SFI ..... Standard Forensic Instruction

SPA ..... Scottish Police Authority

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