

LEGAL BASIS FOR THE SEIZURE AND EXAMINATION OF DIGITAL DEVICES

1. Introduction

- 1.1 This document outlines the existing legal basis for the examination of digital devices.
- 1.2 Police Scotland proceeds on the premise that there must be a proper basis in law for the actions of its officers and staff. In proceeding upon that basic premise and with regard to the examination of digital devices Police Scotland's actions accord with the law as it is understood to be.
- 1.3 The powers outlined herein apply only to the contents of a device, commonly referred to as 'stored data' and not 'online data' accessed via that device.

2. Common Law Powers

- 2.1 The common law of Scotland operates no differently in relation to the seizure of a digital device by a police officer in the course of an investigation to any other item which is reasonably suspected to be evidence in a police investigation or incident.
- 2.2 The same applies when it comes to examination of the 'contents' of any such device. A digital device can be regarded as being the electronic equivalent of a briefcase or filing cabinet, where the device is often protected by some sort of barrier or lock which requires a PIN or password to access its 'contents'.
- 2.3 Therefore, if a police officer in the execution of a lawful power seizes a digital device, the law allows for the examination of that device for information held within.
- 2.4 The extent of the current common law power of seizure in Scotland (including subsequent powers of examination) will be guided by what is said by the Scottish Courts in instances where challenges have been mounted to the use of such powers Police Scotland will be guided by judicial precedent but recognises that each judgement will be 'fact specific' and that caution requires to be exercised in the broader application of general principles from such judgements. Any decision regarding admissibility is determined by the Courts, with the common law having a degree of adaptability which guides law enforcement as to what is permitted and deemed lawful.
- 2.5 Where evidence has been recovered as a result of actions for which there is legal authority, then that evidence will be admissible subject to any other legal rules which may apply.

3. Statutory Powers - Accused / Suspects / Temporarily Detained Persons (Powers of Search)

- 3.1 A search will be lawful where there is a statutory power, a warrant conferring such a power or a power at common law. Section 47 and 48 the Criminal Justice (Scotland) Act 2016 permits a police constable to search any arrested person or seize and examine any item in their possession whether or not they have been charged with an offence.
- 3.2 A list of statutory powers of search of the person includes, but is not limited to:
 - Section 47 Criminal Justice Scotland Act 2016 – Search on arrest and charge
 - Section 48 Criminal Justice Scotland Act 2016 – Search on arrest

- Section 47 Firearms Act 1968 (Firearms)
- Section 23 Misuse of Drugs Act 1971 (Drugs)
- Section 60 Civic Government (Scotland) Act 1982 (Stolen property)
- Section 4 Crossbows Act 1987 (Crossbows)
- Section 11 Protection of Badgers Act 1992 (Evidence of commission of an offence under that Act)
- Section 101 Conservation (Natural Habitat etc.) Regulations 1994 (Evidence of commission of an offence under that Act)
- Section 4 Wild Mammals Protection Act 1996 (Evidence of commission of an offence under that Act)
- Schedule 7, Terrorism Act 2000

Relevant Case Law

- 3.3 In *Rollo –v- HMA* (1997) JC 23, the defendant appealed his conviction on the basis that a digital device (a Sharp Memomaster 500) which had been seized under a search warrant issued under Section 23 Misuse of Drugs Act 1971 did not constitute a ‘document’ and therefore the examination was inadmissible. The Court found that access to certain information contained in the device (comprising a list of names and telephone numbers) was protected and required the use of a password (which police officers guessed). The High Court of Justiciary on appeal observed the essential element of a ‘document’ (for the purpose of the search under section 23 of the Misuse of Drugs Act 1971) to be something that contains recorded information of some sort and that a store of recorded information is not to be deprived of qualifying as a ‘document’ because it is protected in some way against unwanted access, deeming electronic security methods (passkey) as no different from a lock on a locked diary.
- 3.4 As a matter of general proposition, where a lawful power of search exists, the power of search enables a police officer to search for an item, seize it and examine it, *J.L. & E.I. -v- HMA (2014) HCJAC 35*. This case concerned an appeal against the Sheriff’s decision to admit evidence obtained as a result of the interrogation of a mobile phone seized from a person detained under section 14 of the Criminal Procedure (Scotland) Act 1995. The data subject to challenge was a text conversation contained within an iPhone 5 in digital format. The stated grounds for appeal were that the police officers had no authority to examine the mobile telephone without either seeking permission or alternatively seeking a warrant. In the course of the appeal it was argued that the iPhone 5 device in question was a “Smartphone”, a “portable computer” and was able to provide access to email, personal banking, health records, still images, moving images, audio files, personal calendars and was a “living filing cabinet” and the appellants “private cyberspace” for which there was no authority to examine.
- 3.5 The High Court of Justiciary stated that

‘A power of search of the person comprehends looking for an item, seizing it and examining it. Accordingly if a police officer has lawfully arrested a person they may in exercise of the common law power of search following an arrest, take possession of the person’s jacket or handbag, look inside the jacket pocket or handbag and on finding for example a diary, examine the entries made in that diary with a view to these entries forming a basis for further inquiry or being admitted as evidence in future criminal proceedings’.

'The section 14(7) power of search used in this case includes power to examine. What will be required for the effective examination of a particular item will depend on the nature of that item and what is the nature of the information which it is hoped to elicit from the examination. For all that we were told, in the present case, examining the iPhone 5 involved little more than connecting the device to a power supply, switching it on and touching the appropriate portions of the screen. In our opinion, so doing was clearly within the powers conferred by section 14(7).'

There was found to be no speciality attributed to the article recovered simply because it was an electronic device, namely an iPhone 5, with the court not being satisfied that there was any illegality or irregularity in recovering the stored data which was contained within the device.

4. Victims and Witnesses

- 4.1 The authorities to take a digital device for the purpose of examination from a victim or witness are; where consent is provided; where there is a warrant; or, where there is urgency (common law power).
- 4.2 The duty of a constable is outlined in legislation. The requirement this legislation imposes is also a consideration in actions taken by police officers (discharge of the general duty of an officer under Section 20 of the Police and Fire Reform Act 2012).
'It is the duty of a constable—
 - (a) to prevent and detect crime,*
 - (b) to maintain order,*
 - (c) to protect life and property,*
 - (d) to take such lawful measures, and make such reports to the appropriate prosecutor, as may be needed to bring offenders with all due speed to justice'.*
- 4.3 Urgency is unique to the individual circumstances encountered. The general considerations that urgency would normally involve include a reasonable belief that a device contains evidence in circumstances where other legal authority (consent / warrant) are not reasonably achievable. The case should be sufficiently serious and apply only where necessary, proportionate, in the interests of justice and where there is urgency - failure to do so would likely result in the loss of life or loss of evidence. The disposable nature of digital evidence is such that urgency is likely to be a particular consideration. In such cases officers may consider common law powers of seizure. Such actions would still have to accord with other relevant applicable principles such as Article 8 of ECHR.
- 4.4 It may therefore be the case that seizure of a device at common law from a victim / witness may be justified in certain cases, if there is adequate 'urgency' to justify the action. This would require due regard to the specific facts and circumstances encountered at that time.
- 4.5 The admissibility of evidence is a matter for the court to decide having considered the evidence, and the specific facts and circumstances of the case and fairness to the accused of the approach taken. The courts decisions can inform and guide law enforcement activity.

5. Other Device Owner / User – Deceased / Missing Person / Other.

- 5.1 This includes any set of circumstances where the owner (or person entitled to possession of the digital device) cannot be identified or classified as a victim, witness, suspect or accused and thereby consent cannot be obtained.
- 5.2 In such circumstances, and in the absence of any other powers, the power of seizure and examination requires justification under common law and in discharge of the general duty of an officer under Section 20 of the Police and Fire Reform Act 2012. Such actions would still have to accord with other relevant applicable principles such as Article 8 of ECHR. Officers may consider using such powers where necessary, proportionate, in the interests of the public/individual's interests, in the interests of justice or where there is an urgency as failure to do so could result in a compromise to an individual's right to life or likely result in the loss of evidence and/or allow the ends of justice to be defeated.

6. ECHR

- 6.1 The European Convention on Human Rights is a consideration which underpins any decision made by Police Scotland.
- 6.2 Article 5, the right of liberty and security of person, is a qualified right meaning its operation can be limited in certain circumstances provided for by the law. Article 6, the right to a fair trial or hearing, on the other hand, is an absolute right. The seizure and examination of digital devices, if carried out properly should not unlawfully infringe on an individual's Article 5 or 6 rights.
- 6.3 The examination of digital devices is likely to infringe upon an individual's Article 8 right to respect for private and family life however, this is not an absolute right. Infringement of Article 8 rights concerning a victim, witness, suspect or accused is permitted if that infringement is in *'accordance with the law, 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'*.
- 6.4 'Necessary' for the purposes of Article 8, means the interference must correspond to a pressing social need (such as the administration of justice) and be proportionate to the legitimate aim pursued.
- 6.5 The examination of digital devices in accordance with the law pursues a legitimate aim and is necessary to ensure that the Police have adequate and reasonable powers for the prevention, investigation and detection of crime.
- 6.6 The seizure and examination of digital devices ought to be seen in the context of being part of the role of the Police, and its protection of human rights, in particular Article 2. This process may protect the public from risk, whether from themselves or others via seizure and examination of a digital device which might materially assist in the speedy location of a missing person or dangerous individual. Similarly Articles 5 and 6, where the product of such examination supports the investigation of crime including yielding exculpatory evidence which in some circumstances perhaps results in the halting of a protracted investigation or criminal trial. This can be seen as being in recognition of a person's rights under Articles 5 and/or 6.

- 6.7 Digital forensic examination can also impact upon the exercise of an individual's rights under Article 10, Right to freedom of expression. This would not be by virtue of the data reviewed but would arise in consequence of the effective denial of access to a device which is a means by which individuals exercise their right to expression via the various platforms, applications and communication opportunities the device provides. As such, the denial of an individual's access to their device should be with due regard to the necessity and proportionality within the circumstances of the investigation. In terms of freedom of expression (Article 10), the rapid return of a digital device might enable an individual to resume their communication and expression.
- 6.8 To protect these rights, in every circumstance examinations require proportionality, necessity, legitimacy and relevance which must be recognised and guide police activity. It is a fundamental part of a police officer's decision-making processes to have regard to the foregoing principles and to act in accordance with them.
- 6.9 These Articles along with other legislative requirements impose obligations upon law enforcement to protect life, to prevent and detect crime and to maintain order whilst acting within the existing legal framework.

7 Data Protection

- 7.1 Authority to take a device can be by consent, statute, common law, or warrant. Any subsequent processing of recovered personal data is permitted and governed separately by the Data Protection Act 2018 (the Act).
- 7.2 Law Enforcement Processing is covered by Part 3 of the Act, which sets out principles for data processing.
The first principle - that the processing must be lawful and fair - is detailed in Section 35, with 35(2) making provision for processing where there is a basis in law for either (a) the data to be processed by consent (not to be confused with any consent relied upon for seizure), or (b) the data to be processed because it is necessary to perform a task for law enforcement purposes.
- 7.3 In the case of data from a digital device police rely on Section 35(2)(b) , with basis in law being 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).
- 7.4 There is a likelihood that there will be sensitive data – that is to say personal data revealing racial or ethnic origin, political opinion etc. – amongst the data recovered from a device. This is referred to as sensitive processing and Section 35(4) and (5) of the Act outline the requirements for such processing. Police Scotland meet the requirements by virtue of
- (i) The processing being strictly necessary for a law enforcement purpose;
 - (ii) The processing meeting at least one condition in Schedule 8 of the Act, principally;
 - 1 – the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest
 - 3 - the processing is necessary for protecting individual's vital interests;
 - 4 - the processing is necessary for the safeguarding of children and individuals at risk.

- (iii) At the time of the processing there being in place an Appropriate Policy Document (APD), namely the 'Law Enforcement Appropriate Policy Document' publicly available on the Police Scotland web site.

7.5 All data processing is compliant with the Act.