Seizing the Future

Seeking clarity of law in the seizure and search of mobile devices in Scotland

Matthew Rice,
Scotland Director
Open Rights Group

Table of Contents

About Open Rights Group

As society goes digital we wish to preserve its openness. We want a society built on laws, free from disproportionate, unaccountable surveillance and censorship. We want a society in which information flows more freely. We want a state that is transparent and accountable, where the public's rights are acknowledged and upheld.

We want a world where we each control the data our digital lives create, deciding who can use it and how. We want the public to fully understand their digital rights, and be equipped to be creative and free individuals. We stand for fit-for-purpose digital copyright regimes that promote free expression and diverse participation in culture.

We uphold human rights like free expression and privacy. We condemn and work against repressive laws or systems that deny people these rights.

We campaign, lobby, talk to the media, go to court — whatever it takes to build and support a movement for freedom in the digital age. We believe in coalition, and work with partners across the political spectrum.

We scrutinise and critique the policies and actions of governments, companies, and other groups as they relate to the Internet. We warn the public when policies — even well-intentioned ones — stand to undermine the freedom to use the Internet to make a better society

.

Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537.

Introduction

The seizure and subsequent search of electronic devices, in particular smartphones, by police forces is a challenge for the existing legal frameworks of common law countries. It raises questions of legal certainty and compatibility with the rule of under seizure rules that are widely drawn and at risk of allowing arbitrary enforcement.

The justification for interfering with Article 8 rights require the action to be "in accordance with the law". This is a key test. If the action is not found to be 'in accordance with the law' the necessity and proportionality of the interference, another very loaded topic when it comes to electronic devices, are not necessary[1]. There is a four part test for whether a seizure and search is in accordance with the law as set out in the jurisprudence of the European Court of Human Rights, these are:

- Does it have a basis in domestic law?
- Is the law adequately accessible?
- Is the law reasonably foreseeable?
- Is the law compatible with the rule of law?

Putting these standards together the seizure and search of electronic devices must have a set of rules based in law that are available to the public, giving a reasonable explanation of for what reasons devices can be taken from an individual, providing sufficient safeguards for that seizure to prevent against arbitrary interference.

Electronic devices are becoming central to our lives. Our relationships are contained within them, our correspondence, our thoughts, our fears, our identities. A search of an electronic device will provide more insight into an individual than any other piece of property, including their home. This is why police forces seize these devices, whether you are a witness, a victim,

[1] M.M. v. The Netherlands, No. 39339/98 , 2003, §46.

or a suspect your electronic device holds the key to exonerate and incriminate an individual in criminal investigations.

So how should our devices be treated in criminal investigations? Are they to be looked at as a very extensive diary? Is that sufficient to reflect the sophistication of this technology? When we don't fully understand the level of information retained on a device and what could be searched for, the law bears a responsibility to protect the right to privacy by drawing sufficient safeguards for the public against arbitrary interference. These safeguards include some form of judicial oversight, a clear scope for the search, and accessible information for the public about what the seizure and search of electronic devices entail.

This paper seeks to explore the standards illustrated in the jurisprudence of European Court of Human Rights. First taking from cases that articulate broad principles of "in accordance with the law" the paper also visits some of the recent judgements that have come out of Bulgaria that have dealt directly with the search and seizure of electronic devices. The paper then applies these standards to the situation currently in Scotland where there is a discussion whether to roll out forensic devices to police stations across Scotland to aid in the screening of seized devices for information of evidential worth.

The issue of seizure and search of electronic devices engages many different bodies of law, from criminal law and evidential procedure, to data protection in the context of law enforcement processing. Underpinning these different systems are questions of the rule of law and safeguarding fundamental rights. These overarching questions are best dealt with by assessing the relevant jurisprudence from the European Court of Human Rights (ECHR), interpreting the European Convention on Human Rights (ECtHR). While the other bodies of law are of course of great importance, this paper will focus on human rights jurisprudence to explore this topic and only make cursory reference to other bodies of law, such as Part 3 of the Data Protection Act 2018 which contains the relevant regime for processing personal data for law enforcement purposes.

The paper concludes that the laws in Scotland are not in a suitable form to be considered "in accordance with the law". While they may operate with a basis in domestic law given the

common law system that Scotland operates, the laws are not adequately accessible and fail to provide foreseeability for individuals to moderate their conduct, finally it fails to be compatible with the rule of law in providing sufficient safeguards against arbitrary interference.

Mobile Forensics

Mobile phone forensics is the practice of extracting data from a mobile device. In the past this may have involved palm pilots or personal planners[2], even mobile phones that could only send and receive messages and calls. Nowadays, 'Mobile Phone forensics' is a practice for accessing and extracting information held on a mobile device. It can provide access to a wide array of information held on an individual's device, engaging with different aspects of Article 8 rights (private life and correspondence). Forensics can extract:

- Contacts
- Messages
- Pictures
- Location of device
- Social media accounts
- Web browsing history
- Application usage
- Device identifiers

This information can include deleted information depending on the type of acquisition used. Techniques are also widely available for circumventing security and password locks that are often on the devices.[3] In short, forensics can reveal all the data that you have stored on a

[2] See the case of Rollo v. HM Advocate 1997 JC 23.
[3] Cellebrite, Products, UFED Ultimate, https://www.cellebrite.com/en/products/ufed-ultimate/ [accessed 13 April 2019].

device, and even data that you have provided to the device that you may not have realised such as location, or data that you believe is no longer available such as deleted data.

These different types of information that could be accessed are covered by Article 8 rights to respect for privacy of correspondence[4] and of private life[5]. Storage and retention of this information entails issues of data protection too.[6]

Scotland's cyber capabilities

Police Scotland, among other police forces across the United Kingdom[7], have purchased and use mobile forensics equipment. Currently the practice is that a mobile device is seized when it is believed to contain information relating to a criminal investigation.[8] The device is then transported to one of five "Cyber Hubs' in Scotland where forensic tests are performed.

At the Cyber Hubs, the electronic device will be imaged, a process where the contents will be copied and stored to analyse whether it contains evidential value. After analysis, if there were no evidence found, the device would be returned to the individual. This process engages questions of proportionality for a full imaging of a device, the retention of the image of the phone, and the length of time a phone an individual's phone is detained.

This system is now seemingly at breaking point. Each year there is a backlog of over ten thousand mobile phones, SIM cards, tablets, and mobile storage devices examined.[9] There is

[4] Electronic messages (Copland v. United Kingdom §41, Bărbulescu v. Romania §72), stored data (Wieser and Bicos Beteiligungen GmbH v. Austria §45)
[5] Case of Niemitz v. Germany, 13710/88, 1992, §30 - business premises can have private relationships formed there that attract protection of Article 8.
[6] This paper will not be going further into the data protection issues suffice to say there are many.
[7] For further information on this see Privacy International's report "Digital stop and search: how the UK police can secretly download everything from your mobile phone" , https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile. [accessed 13 April 2019].
[8] Evidence to the Justice Sub-Committee on Policing, 10 May 2018, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526 [accessed 13 April 2019].
[9] Digital Triage Device (Cyber Kiosks) Stakeholder Group Minute of Meeting, 27 July 2018, http://www.scotland.police.uk/assets/pdf/138327/307421/501417/Cyber-Kiosk-Stakeholder-Meeting-Minutes-27-July-2018?view=Standard [accessed 13 April 2019].

reportedly a backlog of 10s of thousands of devices.[10] It also appears to be a low success rate in these searches with only 4% of the seized devices being used evidentially after examination is complete.[11] The turn-around time for a device to be seized, tested, and a decision made can be weeks[12]. Additionally, according to Police Scotland, the rate that devices do contain information of evidential value is low, leading to a waste of resources and an unnecessary deprivation of an individual's liberty in the form of removing from them a communication device that is central to their lives.

In an effort to combat the backlog and resource waste, Police Scotland announced plans to purchase 'cyber kiosks'. Trials were held in Edinburgh, Stirling over 5 months in 2016 from May to September. 195 mobile phones were seized and 262 SIM cards were examined in Edinburgh and 180 mobile devices were examined in Stirling. However, no records of the success-rate or legal bases used for the seizure of these devices were retained.[13] Neither were any warrants issued for testing or screening these phones, which suggests that the default option taken by Police Scotland is to exercise their common law or statutory powers that do not require warrants.[14] Despite this failure to record any sort of meaningful metrics of success around the 'cyber kiosk' pilots, Police Scotland went ahead with plans to rollout the 'cyber kiosk' system.

The 'cyber kiosk' systems are stand alone examination systems, which will be located at selected police stations across Scotland. There will be 41 kiosks[15]. Trained officers will operate the devices.

---

[10] Digital Triage Device (Cyber Kiosks) Stakeholder Group Minute of Meeting, 30 October 2018 pg. 5, http://www.scotland.police.uk/assets/pdf/138327/307421/501417/Cyber-Kiosk-External-Reference-Group-Minutes-30th-October-2018?view=Standard [accessed 14 April 2019].

[11] Justice Sub-Committee on Policing Committee session 13 September 2018, evidence DCS Gerry McLean, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&i=105715&c=2111475#ScotParlOR [accessed 14 April 2019].

[12] Digital Triage Device (Cyber Kiosks) Stakeholder Group Minute of Meeting, 27 July 2018, http://www.scotland.police.uk/assets/pdf/138327/307421/501417/Cyber-Kiosk-Stakeholder-Meeting-Minutes-27-July-2018?view=Standard [accessed 13 April 2019].

[13] Justice Sub-Committee on Policing evidence session, 10 May 2018 http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526&i=104575&c=2092175#ScotParlOR. [accessed 14 April 2019]

[14] *ibid*.

[15] Police Scotland submission to Justice Sub-Committee on Policing, 30 April 2018, https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-PS.pdf

Police Scotland have proposed procedures whereby devices seized or provided in relation to certain high priority cases or specialised alleged crimes, such as child abuse, will not involve the kiosks but will continue (as now) do go direct to cyber hubs for full examination. Otherwise, the officer in charge of the case will be required to prepare a submission form of search criteria specifying what names, numbers identifiers or other data types are to be searched for by the kiosk.

PS envisage that devices which go to kiosks will be examined semi-automatically, based on submitted search criteria. It is not required or anticipated that the human operator will examine the device, as opposed to entering the search criteria. If relevant hits are found, the consequences are that a record of the search is prepared, and the device forward to a cyber for fuller manual examination. If not, the requesting officer and if need by COPFS will be notified that no relevant data was found. PS are explicit and unequivocal in requiring that no data is copied after the process is complete, or retained in the kiosk. [16]

The distinction between the cyber kiosk system and the cyber hub system is meaningful for Police Scotland from a resource perspective, but from a legal framework perspective there is no difference. The interference with Article 8 rights still occurs and there is still a requirement to provide a clear legal basis for the interference.

The paper now turns to explore what the different legal bases Police Scotland are relying on.

Scotland's legal basis

In the debate about the roll-out of the "cyber kiosks" in Scotland, and the wider discussion of mobile phone forensics in the United Kingdom, the debates have turned to the lawful basis for their use and practice. While Police Scotland have sought to make a practical distinction between the proposed 'cyber kiosks' and the current 'Cyber Hubs', it is confirmed that it is the same lawful basis for both.[17]

[16] Footnote 13, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526
[17] Detective Chief Superintendent McLean, 15 November 2018, Sub-Committee on Justice and Policing, pg. 6 http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11785&mode=pdf.

In correspondence with Police Scotland, the Crown Office Procurator Fiscal Service broadly categorised the legal basis to allow Police Officers to seize an item as:

- Where an individual has been arrested
- Where there is a statutory power of search of an individual or their property without the need for a search warrant
- Where a search warrant has been granted either under legislative powers or the common law
- Where the owner has given consent
- Where there is a common law power; or
- Where there is urgency.[18]

Common law

Relevant cases that have been cited in relation to the seizure of items and search include Rollo v. HMA from 1997 and J.L. & E.I. v. HMA from 2014.

In the case of Rollo, the issue was whether an electronic notepad or diary, a Memomaster[19], fell within the meaning of a 'document' for the purposes of a search carried out in terms of a judicial warrant issued under s.23(3)(b) of the Misuse of Drugs Act 1971. The High Court of Justiciary observed that the essential element of a document is that it is something containing recorded information of some sort and a store of recorded information is not to be deprived of qualifying as a document because it is protected in some way by a passcode.

---

[18] Letter from Crown Office and Procurator Fiscal Service to Police Scotland, 30 January 2019, https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190130COPFStoPS-CyberKiosks.pdf.

[19] A Memomaster is a personal information manager that contains address books, telephone numbers, and a scheduler, an example of the device is available here https://www.scotcourts.gov.uk/search-judgments/judgment?id=8fb18aa6-8980-69d2-b500-ff0000d74aa7

In J.L. and E.I. v. HM Advocate, it dealt particularly with police powers of search in relation to persons detained under the now repealed provision of s. 14 of the Criminal Procedure (Scotland) Act 1995 where the police had reason to suspect that a person had committed an offence punishable by imprisonment.[20] In this case it was argued that the iPhone 5 constituted a 'living filing cabinet' providing access to email, personal banking, health records, still images, moving images, audio files and personal calendars and that there was no power under the 1995 Act that allows a Police Officer to examine the contents of a mobile telephone.[21]

The Court rejected this assessment on the basis of the facts available to it. It was not clear that the search performed by the Police involved access to email, personal banking, health records or any of the social media sites.[22] The facts available to the court were that the data subject to challenge was in the form of text messages contained within the iPhone 5.[23]

The court stated that an effective examination under section 14(7) of the Criminal Procedure (Scotland) Act 1995, 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 the court was told, 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 the court's opinion, doing so was clearly within the powers conferred by section 14(7). The court dismissed the appeal.

The High Court stated that a power of search of the person comprehends looking for an item, seizing it and examining it. The Court further stated that if a police officer has lawfully arrested a person that officer may in exercise of the common law power of search following an arrest take possession of the person's jacket or handbag, examine the entries made in that diary with a view these entries forming a basis for a further inquiry or being admitted as evidence in future criminal proceedings.

---

[20] J L and E I v. HM Advocate [2014] HCJAC 35 at 5, https://www.scotcourts.gov.uk/search-judgments/judgment?id=8fb18aa6-8980-69d2-b500-ff0000d74aa7 .
[21] *Ibid* at 6.
[22] *Ibid* at 12.
[23] *Ibid* at 13.

The High Court found that there was no speciality attributed to the article recovered simply because what is found was an electronic device and was not satisfied that there was any illegality or irregularity in recovering the stored data which was contained within the phone.

Consent

In the case of witnesses or victims, Police Scotland assert that informed consent for seizure and examination of that device is recommended. It does not make reference to other categories such as suspects or accused where consent can be a lawful basis.

Statutory law

The Police have given indication of statutory powers where a warrant is provided such as the Misuse of Drugs Act 1971, and the Terrorism Act 2000.[24] There is no comprehensive list available of statutory law where provision a warrant allows for the search and seizure of items.

According to Police Scotland, all seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision. The policing purpose is outlined under the general duties of a constable under section 20, Police Fire and Reform (Scotland) Act 2012, which are:

(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.

[24] Evidence of Gerry McLean to Justice Sub-Committee on Policing, 13 September 2018, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&i=105715&c=2111409#ScotParlOR.

Section 20 of the Police Fire and Reform Act also applies to situations where the owner of an electronic device cannot be identified as a victim, witness, suspect, accused or where consent cannot be obtained where failure to do so could result in a compromise to an individual's right to life, the loss of evidence and / or the ends of justice to be defeated.

Article 8 assessment "In accordance with the law"

Under the European Convention of Human Rights, Article 8 guarantees the right to privacy of private and family, home, and correspondence. This right is not absolute and can be interfered with. However, the interference must satisfy strict tests for it to be considered lawful. In many discussions of surveillance of correspondence, the discussion turns around the necessity and proportionality of a measure[25].

Before an assessment of the necessity and proportionality of an interference with Article 8 rights comes an assessment whether the interference is "in accordance with the law". This paper will not seek to explore the necessity and proportionality of seizing and searching mobile devices, but this does not mean it is not important consideration to make which has been decisive in the past.

However, in search and seizure, surveillance is not an appropriate analogy. Instead we are dealing with the notion of overtly seizing property for assessment by law enforcement. This means different standards are at play despite the fact that as in surveillance the right to private correspondence is engaged and sophisticated technology is at play both the device for examination, and the technology used to examine. However, the overt seizure of the property turns this discussion away from the proportionality and necessity of a measure of secret surveillance, to one focused on the clarity of the law, its accessibility, and the foreseeability of its reaches.

[25] For instance, see the litigation by various civil society organisations against secret surveillance measures in the United Kingdom challenging the necessity and proportionality of a measure, 10 Human Rights Organisations v. United Kingdom, Application No. 24960/15, https://privacyinternational.org/legal-action/10-human-rights-organisations-v-united-kingdom. [accessed 14 April 2019].

In accordance with the law tests

The test as to whether a measure is in accordance with the law consists of three stages[26]:

Firstly that the impugned measure should have some *basis in domestic law*[27]*;*

Secondly, the law must be *adequately accessible*[28]*;*

Thirdly, the law must be *reasonably foreseeable*[29]*;*

Fourthly, the law must be *compatible with the rule of law*[30].

Basis in domestic law

The first is whether the measure has a basis in domestic law. This comprises exploring the source of law that the interference is made under. The Court has always understood the term "law" in its "substantive" sense, not its "formal" one; which gives meaning to include forms of law of lower rank than statute.[31] In this regard settled case-law cannot be disregarded.[32] As a common law country this is an important point to keep in mind for Scots law.

Adequately accessible

It is not enough for a source of law to be available for the interference with Article 8 to be justified. The citizen must be able to have an indication that is adequate in the circumstances

[26] Silver and Others v. United Kingdom at
[27] Sunday Times v. United Kingdom, 1979, § 47
[28] *Ibid* §49
[29] *Ibid.*
[30] Silver and Others v. United Kingdom, Application no. 5947/72, 1983, §90.
[31] Wilde, Ooms and Versyp judgement of 18 June 1971, Series A no. 12, p. 45, §93.
[32] See Huvig v. France, Application no. 11105/84, §27.

of the legal rules applicable to a given case. The type of individual concerned, their level of knowledge and profession can have a bearing on this fact.

The Court has shown that it is not wholly necessary for the law to be primary legislation to be deemed adequately accessible, administrative arrangements can be included too[33]. Codes of Practice and internal guidance can be included but the level of public access to that guidance will be considered carefully[34].

Reasonably foreseeable

A norm cannot be regarded as "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[35]

In the case of measures of secret surveillance the test of foreseeability has consistently been qualified that it is not necessary for the individual to be able to understand all aspects of the surveillance that could occur against them.[36] However, the seizure and search of an electronic device is not an example of secret surveillance. The device is taken from an individual by police, there is no need to cloak or draw widely the scope of this power.

Instead, in ECtHR case law it is a responsibility for the State to provide clear rules for what a person can be stopped and searched for; the powers of the police to compel surrender of a device and the scope of search that can be undertaken.[37] In cases where search and seizure of electronic devices have been challenged the question often turns on whether there is adequate

[33] Malone v. United Kingdom, Application no. 8691/79, §76.
[34] Khan v. United Kingdom §26
[35] Sunday Times judgement Application no. 6538/74, 1979, §49.
[36] Weber and Saravia v. Germany, 54934/00, §93.
[37] Gillan and Quinton, 4158/05, §77.

safeguards available to protect against arbitrary interference.[38] The sophistication of the technology being used to perform the interference has also made its way into the Court's consideration.[39]

Compatible with the Rule of Law

Compatibility with the rule of law ties the three prior tests together, bringing it under a discussion as to whether there are sufficient safeguards in place to protect against arbitrary interference. This test suggests that while there may be a measure for seizing a device based in domestic law, accessible and articulated reasonably for an individual to understand the effect of their actions, but if there are not sufficient safeguards that underpin this measure, it will fail to be "in accordance with the law".

In stop and search cases this has often turned on the standards for triggering a search, whether prior judicial authorisation is required, or what standard of suspicion must be established.[40] For electronic devices, the need for prior judicial authorisation in the form of a warrant would appear to be a prerequisite for compatibility, and only in exigent circumstances would a search of electronic devices without a warrant be deemed acceptable.[41] Further, due to the technology used to perform a search of an electronic device and its sophistication, the search parameters should be drawn narrowly to prevent collateral intrusion.[42]

The paper will now turn to assess whether each basis in law from Police Scotland provides sufficient clarity to be considered 'in accordance with the law'.

The circumstances of the legality of any stop and search are often fact dependent, and the manner of the search and behaviour of the officers executing the search are decisive also, making an analysis without facts difficult. However, there are some reflections of the proposed

[38] Iliya Stefanov. Bulgaria, 65755 / 01, §38
[39] Weber and Saravia v. Germany, App No. 54934/00 §93
[40] Gillan and Quinton v. United Kingdom §70
[41] See Iiiya Stefanov v. Bulgaria 2001 65755 / 01 and Prezhdarovi v. Bulgaria 2005 8429/05
[42] *Ibid*, in particular Prezhdarovi at §49.

legal basis in Scotland that can be looked at against the standards of "in accordance with the law".

Scots law

Basis in domestic law

Police Scotland maintains that a mixture of statutory law, common law, and custom provide a basis in domestic law. The cases of Sunday Times, Chappell, Dudgeon and Malone[43] all reflected that a "law" can include both written law and unwritten law. However, it is unclear whether consent outwith clear boundaries would be accepted by the Courts as being "in accordance with the law".

Consensual stop and search has not been explored by the European Court of Human Rights, in particular witnesses or victims freely giving consent for their items to be searched. This is a contentious area but one which Police Scotland have previously presented as one of the scenarios for using this power.[44] Further, there is a call to remove consensual non-statutory stop and search in Scotland for all stop and search due to its inability to suitably guarantee safeguards[45] Consent as a basis for processing sensitive personal data certainly raises concerns around suitability under part 3 of the Data Protection Act 2018[46] which incorporates Law Enforcement Directive[47], but that is for another paper.

[43] See the Sunday Times judgment of 26 April 1979, Series A no. 30, p. 30, § 47, the Dudgeon judgment of 22 October 1981, Series A no. 45, p. 19, § 44, and the Chappell judgment of 30 March 1989, Series A no. 152, p. 22, § 52

[44] These grounds are presented in a presentation from Police Scotland entitled "Draft Legal Basis – Overview" Digital Triage Devices (Cyber Kiosks), presented on 9 January 2019.

[45] Advisory Group on Stop and Search, August 2015, page 49.

[46] Data Protection Act 2018, Part 3, http://www.legislation.gov.uk/ukpga/2018/12/part/3/enacted.

[47] Directive (EU) 2016/680, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN.

In summary, two of the three sources for the action (statutory and common law) would likely clear the basis in domestic law with consensual stop and search presenting a risk of a violation due to its inability to point to a clear source of law.

Adequately accessible

For a law to be adequately accessible, according to the Sunday Times judgement it needs to provide the "citizen to be given an indication that is adequate in the circumstances of the legal rules applicable to a given case"[48]. In the case of Silver and Others the Court held that "a law which confers a discretion must indicate the scope of that discretion"[49], whether that be incorporated in substantive law. Police Scotland, in the trial and the subsequent discussion of the legal basis under which the seizure of devices could occur have not shown accessibility.

In the trials in 2016 it was revealed that those who had their devices removed did not receive any communication about the search of their devices.[50] They were not informed that their device would be placed into a processing system that would reveal correspondence and aspects of their personal life, nor their rights in line with this. Given the complexity of this area of law, and the multiple statutes Police Scotland could exercise this discretion under, this would appear to not provide accessibility.

Throughout the discussions of the search and seizure of digital devices in Scotland, the Police have maintained that the laws are sufficient clear and accessible. Accessibility in this regard could be interpreted as a relatively practical question: are the different laws and scope of those laws available in one place for an individual to understand what laws Police Scotland are empowered to act under?

---

[48] Sunday Times judgement, 1979, §47.
[49] Silver and Others v. United Kingdom, §88.
[50] Justice Sub-Committee on Policing evidence session, 10 May 2018, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526&i=104575&c=2092182#ScotParlOR. [Accessed 14 April 2019].

The answer appears to be no. Questions from the Justice Sub-Committee of Policing on the precise legal basis have been responded to with broad examples, citing standards of law (such as statute, and common law) without providing definitive statements about the limits of those laws[51]. Applying the standards of accessibility, the failure to give a coherent answer is of deep concern.

Reasonably foreseeable

Reasonable foreseeability, the second part of the legal certainty test, require the law to be drafted with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[52] For items seized in the past, such as diaries and effects, this would be somewhat self-evident about what a police officer would be able to glean from seizing their effects. Electronic devices, with their storage capacity and myriad applications, create uncertainty as to what would be available in a search.

This uncertainty is not to be exploited by allowing for wider discretionary power. In the case of Weber and Saravia, which involved the scope of powers of secret surveillance, the Court emphasised the importance of clear, detailed rules in law "especially as the technology available for use is continually becoming more sophisticated"[53]. While search and seizure is not a secret surveillance power the sophistication of the technology involved, both the device seized and the technology used to view it, means the responsibility for clear, detailed rules, remains.

As shown above Police Scotland have failed to provide a comprehensive statement of the laws where search and seizure could be used, instead providing examples of certain statutes that

[51] Evidence to Justice Sub-Committee on Policing, DCS Gerry McLean, 13 September 2018, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11670&i=105715&c=2111409#ScotParlOR [accessed 14 April 2019].
[52] Sunday Times judgement 1979, §49.
[53] Weber and Saravia §93.

carry warrant requirements such as the Misuse of Drugs Act 1971. Further, they have cited broad policing purposes under Section 20 of Police Fire and Reform (Scotland) Act 2012 which lists those purposes as:

- To prevent and detect crime
- To maintain order
- To protect life and property
- 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
- Where required to serve an execute a warrant, citation or deliverance issued, or process duly endorsed, by a Lord Commissioner of Justiciary, justice of the peace or stipendiary in relation to criminal proceedings, and
- To attend court to give evidence.

In the case of Copland v. United Kingdom, where a College was monitoring the telephone, email and internet use of an employee, the Court stated a requirement that:

> "the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures."[54]

The wording that the Court were presented in Copland were statutory powers to do "anything necessary or expedient" for the purposes of providing higher and further education, and found that did not provide reasonable foreseeability. Police Scotland, if they were to justify the seizure and search of items under section 20 of the Police Fire and Reform Act, are dealing in the same vague proclamations.

Citing these broad powers that a police constable can reach to in the absence of more specific laws, as Police Scotland have suggested, almost certainly places the lawfulness of search and seizure under this law at risk. There is little clarity as to the scope of the discretion being provided to Police Scotland. No clear threshold for crime is available, all crimes appear to be

[54] Copland v. United Kingdom, Application no. 62617/00, §46.

considered applicable for search and seizure of electronic devices[55], maintaining order is an opaque term that has not been provided sufficient clarity. This is a concerning set of broad powers, and does not bode well for the test of legal certainty.

In further Sub-Committee minutes Police Scotland admitted that there was no specific communication given to individuals during the trials[56]. The lack of any clear communication given to individuals during the trials would have raised distinct questions about the foreseeability given to an individual about the scope of the powers available to Police Scotland when they seize a device.

Case law

The available case law cited by Police Scotland does not improve foreseeability. The case of HM Advocate v. Rollo from 1997 dealt particularly and discretely with the issue as to whether an electronic notepad or diary (the Memomaster) fell within the meaning a 'document' under the Misuse of Drugs Act 1971. It is not readily apparent that the decision in Rollo can be read so as to provide the blanket approval of the collection, seizure and search of electronic devices. In Rollo, the search clearly proceeded under the authority of a judicial warrant. It is unclear whether Police Scotland consider this case to advance the foreseeability of the law in searches that are not carried out without a warrant. If they did, they would be mistaken in that assessment.

In JL and EI, that decision dealt particularly with police powers of search in relation to persons detained under section 14 of the Criminal Procedure (Scotland) Act 1995. That statute is now repealed. Those powers of detention and subsequent search only applied where the police had reason to suspect that a person had committed an offence punishable by imprisonment,

[55] Evidence to the Justice Sub-Committee on Policing, Detective Superintendent Nicola Burnett, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526&i=104575&c=2092174#ScotParlOR.
[56] *ibid*.

giving a threshold of crimes from which it is reasonable to seize and search an electronic device. By contrast, the replacement search and seizure provisions introduced in the Criminal Justice (Scotland) Act 2016 can also apply to offences not punishable by imprisonment. It cannot by assumed that the decision in JL and EI will apply in relation to these different legislative provisions where there are now different standards of crime under consideration. This position was clearly articulated in a briefing provided by the Scottish Criminal Bar Association the Justice Sub-Committee on Policing.[57]

The reliance on case law to give an interpretive force to Police Scotland's powers have confused matters. This is the result of case law based on old statutes and perhaps more importantly old technology. When in the past common law was able to be relied upon to keep broad principles up to date with revisions, the pace of technological development has meant that common law is becoming as cumbersome as primary legislation.

Achieving legal certainty is a tall order in these heady modern times. Foreseeability in the face of sophisticated and intrusive technology capable of revealing so much of a person's private life requires carefully drawn measures to demonstrate to the citizen what a given action might entail, it also carries with it a responsibility for safeguards which will be dealt with briefly below, currently the laws in Scotland do not provide a suitable framework for that foreseeability.

Accessibility has also proven difficult to achieve because of the long tail of legislative measures which would allow Police Scotland to seize and search electronic devices. However, it is frustrating that technology is not being used to achieve accessibility. The Internet has given us access to the world's information at our fingertips, it has never been easier to provide information to society in one place, updated when new information, and new interpretations are available. Yet no effort has been made to improve the accessibility of the relevant powers for search and seizure for policing, whether that be primary law, codes of practice, or common law. A repository of relevant laws is merely a matter of collation on one web page and then

[57] Scottish Criminal Bar Association Response to The Scottish Parliament Justice Sub-Committee on Policing, 28 March 2019 https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190328JFtoCC_CyberKiosks.pdf [accessed 22 May 2019].

made available to the public, a lot easier than the days of statute being laid in the Parliament library to be accessed only if a person is able to travel there.

That failure to embrace technology to provide certainty, where there is clearly an embrace to use technology to deliver other policing purposes is disappointing.

Compatible with the rule of law

A test that has developed recently in European Court of Human Rights jurisprudence has resolved to discuss whether a measure is compatible with the rule of law. This rule explores the set of safeguards around a given measure. The rule exists as an additional consideration against the certainty of a law, so if there is any wavering around the accessibility and foreseeability of a given measure compatibility with the rule of law can be considered to bring about a decision. This test began in cases relating to secret surveillance where accessibility and foreseeability of a law would be limited in other circumstances[58], raising the importance of safeguards, but has since made its way into considerations of overt search and seizure.[59]

The available cases have established clear safeguards that must be in place to secure against the arbitrary interference of an individuals rights by an unfettered power. In both cases the Court placed great emphasis on the need for a prior judicial warrant, or in exigent circumstances a warrant after the fact, in both cases within 24 hours. The Court expressed a great deal of concern for any law in a Member State that contained national laws that empowered to order and effect searches without a judicial warrant.[60] Further, the Court took into consideration the scope of the search and seizure operation to be taken into account when deciding whether the measure met the requirements.[61]

[58] See Rotaru v. Romania, Liberty and Others v. United Kingdom, and Sallinen and Others v. Finland
[59] See Stefanov v. Bulgaria and Prezhdarovi v. Bulgaria.
[60] Heino v. Finland, 56720/09, §42.
[61] Iliya Stefanov v. Bulgaria §38.

For search and seizure in Scotland, it has been established that the Police rely on powers of search that include executing a search and seizure operation without a warrant. That basis is clearly challengeable from the existing case law standards. The scope of search warrants are difficult to articulate without a definitive list of statutes but it has previously confirmed that there is no minimum threshold for when a search can be executed[62], throwing in doubt the acceptability of the scope of a given warrant. It is unclear how many electronic devices entered in the Cyberhubs have been done so under a judicial warrant. The Convenor of the Justice Sub-Committee asked the same question in terms of the cyber kiosks during the trials in Edinburgh and Stirling, Police Scotland were unable to say how many warrants were issued.[63]

If it is accepted that warrants may have been administered in some cases, there are questions to be asked of the level of understanding given to an individual when their device is seized. In further Sub-Committee minutes Police Scotland admitted that there was no specific communication given to individuals during the trials.[64] The lack of any clear communication given to individuals, combined with times in which warrants were not issued during the trials raises distinct questions about the compatibility with the rule of law. If an individual is not able to understand the scope of the powers the Police are entitled to use, nor the technology used in searching their device, the rule of law is woefully underserved.

Across these tests, the Scottish system for seizure and search of an electronic device fails to be "in accordance with the law". Each of the available basis have a risk attached to them. Statutory laws fail to adequately limit their scope in the face of the technology used, and case law has not updated itself to face the challenge presented by the technology, thus failing to bring legal certainty. Consensual searches fail to have any basis in law at all. Finally, the compatibility with the rule of law in the form of safeguards is on shaky ground, with inadequate information provided to individuals when their phones are seized and an inability to demonstrate judicial authorisation as the *de facto* method of oversight.

---

[62] Footnote 52.
[63] The Convenor to Nicola Burnett, Justice Sub-Committee on Policing, 10 May 2018, http://www.parliament.scot/parliamentarybusiness/report.aspx?r=11526.
[64] *ibid*.

The Future

The seizure of mobile devices are evidently necessary for crime fighting, it is not just cyber-crimes that include mobile phones and electronic devices, but increasingly there is a digital footprint in many crimes involving correspondence, location, intention, or documentation of crimes such as captured images and video. It is inevitable that Police Scotland and forces across the United Kingdom will continue their reliance on the seizure and search of mobile devices to investigate crime. However, the current legal framework for seizing electronic devices is clearly out of step with current standards. The increased involvement of electronic devices means creating modern standards all the more important, this is not an esoteric pursuit on a niche topic but a signpost of the direction of travel for criminal investigation, it begs the question why not make sure that standards are also travelling in that same direction.

On 8 May 2019, the Scottish Police Authority released a legal opinion authored by Murdo Macleod QC from 29 April 2019 that they argue confirms the legal basis for the seizure and search of legal bases.[65] The opinion touches on all the bases covered in this paper. In particular it focuses on the power to seize and search devices without a warrant and cites JL and EI v. HM Advocate as a "binding authority" for the seizure and search of electronic devices without a warrant.[66] The opinion fails to acknowledge that the legislation the case is based on has now been repealed and that the repealing legislation Criminal Justice (Scotland) Act 2016 contains sufficiently different standards.

Most importantly the legal advice discusses the future of this area of law. In providing a tentative approval of the current legal basis it quite clearly articulates, in particular under the common law and the basis of JL as a "binding" authority:

"...it might be thought better to involve the Government in bringing forward legislation to underpin the use of **cyber kiosks and cybercrime hub** [emphasis added]. The consultation

[65] Opinion of Senior Counsel for The Chief Constabulary of the Police Service of Scotland in relation to Cyber Kiosks, Murdo Macleod QC, 29 April 2019, www.spa.police.uk/assets/126884/532470/532474/552201/552457. [accessed 22 May 2019].
[66] *Ibid* at para 11 – 12.

process would inform Parliament and, hopefully, lead to **a proper legislative framework fit for the digital age** [emphasis added]**."**[67]

This is not an effort to scupper Police Scotland's investigative capabilities. This is trying to articulate that for dealing with a technology that holds personal information with a scope and depth that we have never reckoned with before, the standards for seizing and searching that device, even "offline", requires careful consideration. Maintaining public confidence and understanding of the investigative techniques, and the powers to use those techniques, is critical. The root of this confidence stems from a clear legal framework.

The available framework fails to admit the scope of privacy contained in these devices, which eclipse that of any piece of property that has come before. The solutions available to the framework lie in updating and reflecting the need for safeguards, in the form of new rules underpinned by prior judicial authorisation and clearly establishing this on a legislative footing.

Clear rules and communication material when devices are seized are also required. These rules should provide an understanding regarding:

- the scope of a given search, such as parameters or selectors that could be used;
- the sources of information that will be searched (e.g. images, correspondence, location, application usage);
- the crimes that devices can be seized to investigate;
- the retention period for the information;
- the rights of an individual to challenge the seizure of the device;

These rules are not exhaustive, merely reflective of some of the concerns raised by the European Court of Human Rights in previous cases. There are standards and principles developed by civil society organisations such as Privacy International's "Necessary Hacking Safeguards"[68] that could also be reflected.

---

[67] *Ibid* at para 32.
[68] "Government Hacking and Surveillance: 10 Necessary Safeguards", Privacy International, https://privacyinternational.org/type-resource/necessary-hacking-safeguards. [accessed 22 May 2019].

The challenge faced now and for the future is to maintain public understanding and awareness of the scope of the powers available to the police in searching and seizing devices with storage and functionality that most of society are unable to comprehend. This lack of understanding of sophisticated technology is not a blindspot that can be used to expand the powers of policing. It is a test to draw adequate safeguards in accordance with the law that help the public to maintain trust in the criminal justice system. It is aiming to achieve that principle that will help maintain harmony with the rule of law in years to come.