Opinion of Senior Counsel

for

THE CHIEF CONSTABLE OF

THE POLICE SERVICE OF SCOTLAND

in relation to

Cyber kiosks

Introduction

[1] I am asked to provide an opinion on the legality of Digital Device Triage Systems, colloquially known as "cyber kiosks". This opinion is based on: various documents provided by the Legal Services Department of the Police Service of Scotland ("Police Scotland"); a perusal of the relevant legal authorities and commentaries; and a demonstration provided by Police Scotland at its Crime Campus on 26 April 2019. For the purposes of this opinion I have concentrated on the area of warrantless search of arrested persons,[1] and Information Communication Technology ("ICT") devices; in the present context - mobile telephones and tablet devices.

[2] My principal conclusion is that there is a lawful basis for the use of cyber kiosks.

The need for Cyber kiosks

[3] It is perhaps rather trite to observe that ICT devices can be used in the commission of certain crimes and may be repositories for highly relevant evidence.[2] I understand that rapid growth in their use has placed significant demands on the Cybercrime Unit of Police Scotland which would ordinarily examine all recovered devices.[3] Cyber kiosks are desktop computers which can be connected to ICT devices to enable a quick examination of stored data – commonly referred to as "triaging". In the event that relevant data is found, the device will be fast-tracked to the Cybercrime Unit. If no relevant data is found, the device may be returned to its owner. As a result, it is hoped that backlogs and delays will be reduced and the

[1] The scope for search prior to arrest is now very limited. See para [28] and footnote 38 *infra*. I also touch on the position with regard to witnesses and complainers at paragraphs [29] and [30].

[2] They may also yield exculpatory evidence which might avoid the need for a lengthy investigation. Alternatively, if there is a prosecution, the Police are obliged to disclose any exculpatory evidence.

[3] See, for example, Cybercrime kiosk toolkit at 2.1. This document was provided to me in draft form, although I understand it is at an advanced stage of preparation.

process of examining ICT devices rendered altogether more efficient. The beneficial consequences arising from a new, and better, capability to investigate, prevent and detect criminal activity should be obvious, and include the time saved in returning devices to their owners, many of whom – such as vulnerable complainers or other witnesses - may be more reliant on their devices than others in the community.

The operation of cyber kiosks

[4] The operators of cyber kiosks are to be trained and accredited,[4] and are the subject of supervisory oversight.[5] The examination of an ICT device on a kiosk must be authorised by a supervisor (the rank of Sergeant or above[6]) who, importantly, may only do so if satisfied that *"fundamental principles of necessity, proportionality and Human Rights considerations are met for every authoristation"*.[7] The Supervisor must also be satisfied that the examination is for a *"policing purpose"* and that the device has been lawfully seized *("by warrant, common law, or other legislative power").*[8] If nothing significant is found, the device will be returned to its owner.[9] Crucially, it is made clear to supervisors that *"Speculative enquiries (e.g. find any evidence of criminality) should be rejected."*[10]

[5] As I understand it, the machines are to be configured, so that it is only the stored contents that can be examined and, to this end, the examination is conducted "off-line" with the sim-card removed from the device. The examination is, where possible, restricted to certain parameters, such as timescales, or by entering search terms such as the names of individuals or other keywords. This should minimise the scope for *"collateral intrusion"*.[11] Once viewed the data is not retained or downloaded as *"…the kiosks are unable to copy and store device data".*[12] An audit trail is automatically generated showing the details of the examiner and the time of examination.[13]

---

[4] Cybercrime kiosk toolkit at 2.4.
[5] Ibid at 4.3
[6] Interestingly, for non-cybercrime related inquiries, the relevant Standard Operating Procedure ("SOP") requires that a supervisor of at least the rank of Inspector should be contacted and *"asked for permission to examine the phone"* (SOP for digitally stored evidence at 5.3.5). This to some extent mirrors the level of authority required for the taking of certain samples, per, for example s.18(6) of the Criminal Procedure (Scotland) 1995 Act ("the 1995 Act"). The distinction may lie in the fact that the SOP relates to manual examination (without the use of a kiosk) by non-expert officers. One imagines that such *ad hoc* examinations would occur very infrequently.
[7] Ibid at 4.4.
[8] Ibid at 8.1
[9] See Cyber kiosk Flow chart provided by Police Scotland
[10] See toolkit at Appendix G bullet 3. See also Appendix 'I'
[11] Cybercrime kiosk toolkit at 8.1. See also 10.2
[12] Ibid 5.4
[13] This is stressed in the SOP for Digitally Stored Evidence (2.1(c))

[6] If anything significant is found in the course of the examination, the device is submitted to the Cybercrime Unit for full examination and, if appropriate, the preparation of an evidential report.[14] The device may only be returned to its owner at this stage if the Crown and Office and Procurator Fiscal Service ("COPFS") is satisfied that it is appropriate to do so.[15] According to Police Scotland, all personal data that is downloaded or retained at the Cybercrime Unit is securely stored in accordance with data protection legislation.[16]

The common law power of search without warrant

[7] The common law power to search, seize and examine following arrest was succinctly summarised in the case of *JL v HM Advocate*.[17]

> "A power of "search" of the person comprehends looking for an item (going through pockets, for example: *Bell v Leadbetter* at 1934 J.C., p.77) seizing it and examining it. Accordingly, 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, 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 a further inquiry or being admitted as evidence in future criminal proceedings."[18]

Statutory powers of search without warrant

[8] In terms of the 2016 Criminal Justice (Scotland) Act 2016 ("the 2016 Act") a police constable may search any arrested person or seize any item in their possession whether or not they have been charged with an offence.[19] Essentially this is a

---

[14] See Cyber kiosk Flow chart

[15] Ibid

[16] Ibid. I am not in a position to consider GDPR issues on the information provided to me thus far.

[17] *JL v HM Advocate,* 2014 JC 199 (sometimes referred to as L v HM Advocate). The Court also drew no distinction between arrest and detention. *"By virtue of s.14(7) of the 1995 Act, police officers have the, same power following a detention."* (at para 11). The 2016 Act simplifies procedure by removing the distinction between detention and arrest. Prior to arrest there require to be reasonable grounds for suspicion that the person has committed, or is committing, an imprisonable offence or, for non-imprisonable offences, as well as the foregoing reasonable suspicion, if it would not be in the interests of justice to delay arrest in order to seek a warrant (interests of justice are defined in ss(3)). In reality, all common law offences are imprisonable, as are the vast majority of statutory offences.

[18] ibid, at paragraph 11

[19] *Per* Sections 47 and 48 of the 2016 Act, which preserve the existing Common Law powers. Subject to certain statutory exceptions it is unlawful to search a person who is not in police custody (s.65(2)). However, a person is deemed to be in police custody from the time of arrest until such time as they are

statutory formulation of the common law position.

[9] There are also specific statutory powers of search of an individual, without warrant, in respect of particular crimes, such as terrorism or misuse of drugs offences.[20]

Seizure and examination of ICT devices

[10] It would be fair to say that there has been relatively sparse judicial consideration of the lawfulness of seizure and examination of such devices to date in Scotland.[21] [22] However, it seems to me that there is clear authority for the proposition that "stored" contents on a device can legitimately be recovered without a warrant.

[11] In *JL v HM Advocate*,[23] two appellants were detained under section 14 of the Criminal Procedure (Scotland) Act 1995. The iPhone belonging to one of the detained appellants had been searched and access thereby obtained to incriminating text messages. The first appellant argued that that as the iPhone was continuously connected to the internet, the search amounted to an examination of her private "cyberspace". The second appellant sought to distinguish information "held" on a device such as text messages with that which could be accessed by the device on the internet. Since the police had intended to interrogate the phone to access the appellant's Facebook page and to ascertain its whereabouts at various times with reference to geo-positioning data, the fact that what was eventually retrieved was stored messages was irrelevant. In short, the police had intended to obtain "virtual material". The Court decided that as the grounds of appeal only focussed on the "contents" of the iPhone, and since there were no findings in fact as to the relevant technology and the intentions of the police, the appeal should be decided purely on the basis of what was "contained" in the device. Whilst the Court acknowledged that what was required for the examination of a particular item would depend on the

---

released from custody or brought before a court (s.64).

[20] By virtue of Schedule 7 (8)(1) of the Terrorism Act 2000 and s.23 of the Misuse of Drugs Act 1971 respectively.

[21] I can find only two academic treatments on the topic:*"Power of Search in a digital world"* – Crim. L.B. 2018, 156, 1-3, and a consideration of *JL v HMA* S.C.L. 2014, Jul, 475-487

[22] In *Rollo v HM Advocate* 1997 SLT 558 , police acting on a warrant found important information on a Sharp "Memomaster" electronic notepad. The Appeal Court ruled that the device was a "document" in terms of the section in terms of which the warrant was issued; that its contents were admissible in evidence. The essence of the term "document" was the information recorded on it. Further, it was immaterial that the information required to be processed by means of translation, decoding or electronic retrieval. The fact that there were electronic barriers that the police officers were required to circumvent to access the information, made it no different to a diary with a lock on it. Twenty years later, it might seem rather obvious that details in such an electronic notepad were comparable to written documents, but the case is important for spelling out this principle.

[23] See footnote 15, supra

nature of the item and the nature of the information that was to be recovered, the examination in this case involved, "little more than connecting the device to a power supply, switching it on and touching the appropriate portions of the screen." The Court was therefore satisfied that there was no irregularity or illegality in so doing.

[12] Accordingly, in my view this case is binding authority in support of the contention that the seizure and examination, without a warrant, of the contents of an ICT device, independent of any connection to the internet, is permissible.

The European Convention on Human Rights ("ECHR")

[13] Assuming that the right to respect for private and family life (Article 8) is engaged, the question then arises as to whether the interference is justified in terms of Article 8 (2). If it is, then there will be no violation. By virtue of Article 8(2):

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic wellbeing 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."* [emphasis added]

[14] In terms of satisfying the ECHR test, it seems to me that the scheme for examination of digital devices by cyber kiosk not only accords with domestic legal requirements but is also "necessary" and "proportionate". It is designed simply to ensure that Police Scotland can more efficiently exercise its existing powers in preventing, investigating and detecting crime. Importantly, the scheme has various safeguards in place such as the need for authorisation, together with the limitations of the kiosk itself. It seems to me that the scheme would meet Strasbourg's expectations in terms of its accordance with domestic law, its necessity and its proportionality.

[15] Additionally, as I understand it, cyber kiosks are no more intrusive than the systems that have been in existence for many years at the central Cybercrime Units. Although by no means determinative of the issue, from a perusal of the authorities I cannot find any Scottish case where it has been suggested, far less established, that the examination without warrant, of ICT devices at the existing Cybercrime unit, has in any way breached Convention rights.[24] [25]

[24] With the possible exception of *JL*, although it appears that constables simply read through text messages without recourse to any official cybercrime facilities.

[16] It appears that a tenable argument could be advanced for the proposition that the use of the kiosks might serve to enhance the human rights of individuals. For example, in terms of the right to life (Article 2) it is not difficult to imagine circumstances in which the seizure and speedy examination of ICT devices might materially assist in the prevention of a homicide or the expeditious location of a missing person.[26] Similarly, the quick return of a mobile phone to a vulnerable victim might give that person the opportunity to call for help if their life was in danger.

[17] In terms of the right to a fair trial (Article 6) it is entirely possible that exculpatory evidence might be identified, in some circumstances perhaps resulting in the halting of a protracted investigation or a criminal trial. In terms of freedom of expression (Article 10), the rapid return of an ICT device might enable an individual to resume communicating on the internet, perhaps through facebook posts, tweets and the like.

[18] The need for a degree of certainty about legal rights and responsibilities is also a requirement of ECHR law, and the Court has ruled that the law must also be adequately accessible and foreseeable; that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his or her conduct.[27]

The legal position in Canada

[19] Reference has been made in several quarters to the recent, and rapid, evolution of case law in this field in Canada, where a spate of Supreme Court cases has grappled with the examination of digital devices against the back-drop of Section 8 of the Canadian Charter of Rights and Freedoms, which states: *"Everyone has the right to be secure against unreasonable search or seizure."* The fact the Scottish courts hold Canadian jurisprudence in high regard,[28] makes it all the more relevant.

[20] In the case of *R v Vu*,[29] Justice Cromwell set out the legal position with his

---

[25] There appears to be nothing directly in point in wider European jurisprudence. For a more detailed assessment of the application of ECHR law in this general area, see Reed and Murdoch, *Human Rights in Scotland,* 4th ed, at 6.102 to 6.106

[26] "A recent murder investigation in Germany utilised metrics from the apps on an individual's phone. In that case, Apple's iPhone health app activity record stated that the suspect was "'climbing stairs,' which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up." Privacy international 8/39 – March 2018

[27] See *Colon v Netherlands* [2012] ECHR 946 @ paragraph 72

[28] See for example, *Starrs v HMA, Jenkins v HMA, Gage v HMA, Holland v HMA* etc. Also lectures given by Canadian justices in Scotland, such as the seminal Mcfadyen lecture on *Scientific Evidence* by Justice Cromwell in 2011

[29] *R v Vu* 2013 SCC 32

customary clarity.

> "[40] It is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer…
>
> [44] … While documents accessible in a filing cabinet are always at the same location as the filing cabinet, the same is not true of information that can be accessed through a computer. The intervener the Canadian Civil Liberties Association notes that, when connected to the Internet, computers serve as portals to an almost infinite amount of information that is shared between different users and is stored almost anywhere in the world. Similarly, a computer that is connected to a network will allow police to access information on other devices. Thus, a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized…
>
> [45] These numerous and striking differences between computers and traditional "receptacles" call for distinctive treatment under s. 8 of the Charter. The animating assumption of the traditional rule — that if the search of a place is justified, so is the search of receptacles found within it — simply cannot apply with respect to computer searches…
>
> [51] As I explained above, if computers give rise to particular privacy interests that distinguish them from other receptacles typically found in a place, then s. 8 requires those interests to be taken into account *before* the search takes place, not just after-the-fact, in order to ensure that the state's interest in conducting the search justifies the intrusion into individual privacy. In effect, the privacy interests at stake when computers are searched require that those devices be treated, to a certain extent, as a separate place."

[21] It should be noted that this case dealt with a scenario where a warrant had been obtained prior to the search and, also, that the appeal was unsuccessful on the basis, *inter alia,* that there was a clear societal interest in adjudicating the charge.[30]

[22] Circumstances more similar to the matter in hand are to be found in the subsequent Supreme Court case of *R v Fearon,*[31] where the appellant was searched, without a warrant, immediately following his arrest. Police officers browsed through

---

[30] Similarly to the position in Scotland where procedural irregularities can be excused if other factors are present, such as the error not being made in bad faith, the gravity of the offence etc (per *Lawrie v Muir* 1950 JC 19)

[31] *R v Fearon*, 2014 SCC 77

a smart phone and found a text which stated *"we did it"* and a photograph of a handgun. In delivering the leading judgment in a majority decision, Justice Cromwell extended what he had said about computers in *R v Vu* to include mobile telephones.[32] He went on to conclude that examination of the phone, without a warrant, was justified. Setting out the over-arching principles to be applied for searches of phones without a warrant, he proposed a four-part test to be applied in individual cases.[33]

[23] Albeit the suggested test does not refer to a system for searching, but rather to the criteria to be applied to *ad hoc* searches, it seems to me that it is broadly similar to the proposed framework for examination by cyber kiosks.

[24] Justice Cromwell concluded his judgment by suggesting that his framework is not the only way of ensuring that warrantless searches were constitutionally compliant, that there were many ways of maintaining a balance between law enforcement and privacy concerns and, *"this may be is an area where legislation may be desirable"*.[34]

The legal position in England and Wales

[25] As I understand it, cyber kiosks have been "rolled out" in the great majority of police forces in England and Wales and their use has not been suspended, thus far. However, that is not to say that their use has a lawful basis in that jurisdiction. The difficulty is that, unlike the position in Canada, there has been little, if any, legal consideration of the matter.[35]

Other views

[26] It is apparent, that various concerns have been raised about the use of cyber kiosks by many well regarded and influential stakeholders, organisations involved in the promotion of human rights and academic commentators.

[27] Among those concerns, is a fear that Police could access some sort of portal to a person's cyberspace (as was argued in the *JL* case), for example, enabling police to enter an individual's facebook page or "cloud" facility. As I understand it, and as described above, the cyber kiosks will be disabled from undertaking such an

[32] See paragraph 51 of *R v Fearon*
[33] Ibid at paragraph 83
[34] Ibid at paragraph 84
[35] The statute covering procedure in England and Wales – the Police and Criminal Evidence Act, 1984 (known as PACE) does not appear to cater for such a manner of search, and the leading textbook _ Archbold *Criminal pleading, Evidence and Practice* also appears to be silent on the matter.

exercise.[36]

[28] A further concern is that an ICT device may be interrogated arbitrarily following "stop and search" procedures.[37] However, it seems to me doubtful that the seizure of an ICT device in these circumstances would be considered anything other than a "fishing expedition". The common law in Scotland does not entitle the Police to search without warrant prior to apprehension, except in urgent cases.[38] In any event, Police Scotland has indicated to those operating the cyber kiosks and those supervising the process that this is prohibited. Further comfort may also be drawn from Police Scotland's stark assurance that, *"It must be made absolutely clear that this not and never will be acceptable practice, or allowed."*[39]

Seizure and examination of ICT devices from complainers and witnesses

[29] It seems to me there is no apparent basis for the seizure and examination of an ICT device from a complainer or witness, other than by consent or by warrant.

[30] As it is desirable for relevant evidence to be examined expeditiously,[40] and therefore consensually, it is essential that the fears and concerns of victims and wider society about potential invasion of privacy are allayed as publicly and comprehensively as possible. Quite how public confidence in this scheme can be built and maintained in terms of communication and education, is beyond the scope of this note, but it is clear that the topic is deeply sensitive and troubling to many.[41]

Going forward

[31] The law in relation to the seizure and examination of ICT devices has not been considered since the case of *JL*. It may be that this is because the case is considered definitive. Another, and perhaps more likely, explanation is that an

---

[36] Supra at paragraph 5

[37] Pursuant to Section 73 of the Criminal Justice Act 2016 ("the 2016 Act") a Code of Practice relating to Police powers to stop and search individuals (prior to arrest) came into force on 11 May 2017.[37] Put shortly, a constable must have reasonable grounds for suspicion beforehand. The Code sets out the test for "reasonable suspicion" in great detail. The suspicion must be based on facts, information or intelligence from which a reasonable person would be entitled to reach the same conclusion. Personal factors such as ethnicity, are specifically excluded. For a stop and search to be justified, it must be "appropriate", "necessary" and "proportionate". Understandably perhaps, there is no mention of what items may be retrieved. Traditionally, such searches would check for weapons, drugs or alcohol.

[38] See Renton and Brown, Criminal Procedure at 7-22

[39] This is taken from a (draft) Police Scotland paper on *"Digital Device Triage - Cyber kiosks Considerations and determination"*. I understand that it reflects current Police Scotland thinking on the matter.

[40] Experience shows that obtaining a warrant can be a time-consuming exercise.

[41] At the time of writing (29 April 2019) the main headline on the BBC news website is: *"Rape victims among those to be asked to hand phones to police"*

appropriate case has not arisen which would necessitate further reconsideration of the issues. It seems to me that the issues focused in *JL* and the wider debate arising from this fast-developing area might benefit from further detailed consideration. As discussed above, there are widespread and sincerely held concerns about the investigation of cyber-crime. Reference has been made to involvement by the Scottish Law Commission. I have the greatest respect for that organisation and, in an ideal world, it would be a suitable vehicle for consideration of the legal aspects of this debate. Putting aside whether the Commission has the resources or time to examine this issue, it might also be thought that the debate is more than academic in nature, touching as it does on a consideration of the realities of policing and the concerns of wider society to ensure that crime is thoroughly investigated and prosecuted, whilst balanced against the requirement for civil liberties to be maintained and need for protection of victims.

[32] Against that background, it might be thought better to involve the Government in bringing forward legislation to underpin the use of cyber kiosks and cybercrime hub. The consultation process would inform Parliament and, hopefully, lead to a proper legislative framework fit for the digital age. It is possible that a working group, drawn from across the criminal justice network, could be set up to examine the issue in detail.

Codes of Practice

[33] In recent years the Lord Advocate has been required by statute to issue a code of practice on the questioning of suspects and the conduct of identification parades.[42] In doing so he is obliged to consult with various relevant bodies such as the Judiciary, professional legal bodies, the Police and the Scottish Human Rights Commission.[43] Similarly, as discussed above, the Scottish Ministers have been required to issue a code of practice on the searching of persons not in police custody.[44] It seems to me that there might be merit in at least considering a code of practice, underpinned by statute, covering the seizure and examination of ICT devices and any other relevant digital equipment. In an environment where the law perhaps struggles to keep up with the rapid advancement of digital technology, it is essential that the right balance continues to be struck between the need for the police to investigate crime effectively and the maintenance of procedural safeguards and rights. To this end, the latter model, where a code of practice may be reviewed and revised, might be deemed the more appropriate option.

---

[42] Section 57(1) of the 2016 Act
[43] Ibid, Section 57(5)
[44] Ibid, Section 73

[34] In the meantime, in my opinion the use of cyber kiosks in the manner envisaged by Police Scotland is lawful.

Opinion of

Murdo Macleod

M A MacLeod QC — Advocates Library

29 April 2019 — Edinburgh