SCOTTISH POLICE AUTHORITY

Agenda Item 3

Meeting	**SPA Strategy, Policy & Performance Committee**
Date	**8th May 2019**
Location	**SPA Headquarters, Pacific Quay**
Title of Paper	**Digital Triage Devices (Cyber Kiosks)**
Presented By	**ACC Steve Johnson**
Recommendation to Members	**For Discussion**
Appendix Attached	**Appendix A** – Police Scotland Response to JSC Report **Appendix B** – Opinion of Senior Counsel – Lawfulness of Cyber Kiosks

PURPOSE

This Paper is presented to advise SPA Members on Police Scotland's proposals for the roll out of Digital Triage Devices (Cyber Kiosks).

1. BACKGROUND

1.1 Police Scotland must provide an effective policing service to tackle cybercrime and the threats it poses to the communities of Scotland. It must continuously assess its organisational and technological responses to those threats. In a world where the greater proportion of the population possess some sort of digital device and lead an increasing proportion of their life online, Police Scotland cannot become overwhelmed by the sheer number and variety of such devices which might need to be closely examined in a range of situations, as this would undermine our ability to protect the public.

1.2 Police Scotland has an ambition, on behalf of the citizens of Scotland, to be world class in how we consider and tackle cybercrime and how we mitigate the threats it poses to the communities of Scotland. Despite significant modernisation and remodelling by Police Scotland, increases in the involvement of digital devices in investigations and the capability and complexity of them consequently leads to examination backlogs within Digital Forensic Units.

1.3 Within the UK alone there are over 51 million Smartphone users, this number is growing every year.[1] In 2017, Police Scotland reported that over 40,000 mobile devices were seized. 90% of those submitted for examination were Smartphones and formed a substantial part of the workload undertaken by Police Scotland's Digital Forensic Units. Child Protection/Sexual Exploitation cases are among the crime types that are typically encountered.

1.4 Police Scotland prioritises digital device examination but it is often very challenging to meet the various associated demands, for example: evidence for court cases, serious crime investigations, missing persons and all other incidents where such a device potentially holds evidence. These exponential demands mean that a Digital Triage capability is now a basic front line capability requirement to ensure effective service delivery.

1.5 Cyber Kiosks give front line officers the opportunity to be digitally equipped to progress enquiries more efficiently. By virtue of how we now live, digital devices are part of everyday life and as such are a regular consideration in the progression and management of police incidents and investigations. The ability to identify what is

[1] Statista, https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/

and is not evidence is invaluable in terms of service provision and keeping people safe.

1.6 Cyber Kiosks are an existing and industry recognised means of providing such a capability and indeed they are already in use within several UK forces.

1.7 Police Scotland's proposed use of Cyber Kiosks is only to provide a triage capability. That is to say, to check the contents only, with no data storage or retention of data from the device. This means a specially trained individual will look at the data in a digital device via a Cyber Kiosk and assess if it contains information relevant to the Police investigation or incident. If it does, it will be submitted to one of Police Scotland's Digital Forensic Units for a detailed evidential examination. Police Scotland will only use the Kiosk for mobile phones and tablets.

1.8 The principal benefits deriving from Cyber Kiosks will include:-

- Establishing the relevance of digital devices to investigations at a far earlier stage.
- Enabling often complex investigations to be prioritised/expedited more efficiently.
- Returning digital devices which are deemed not to be relevant to their owners without undue delay.
- Requiring fewer digital devices to be submitted to Cybercrime Units for detailed forensic analysis.
- Providing capacity gains which will enhance service delivery across communities.

2. ENGAGEMENT & CONSULTATION

2.1 Appropriate safeguards are key to public confidence in relation to kiosk use. As a consequence, and following concerns being raised, Police Scotland established an External Reference Group and a Stakeholder Reference Group. The purpose of these groups is to help inform the development, the direction and the implementation of the Cyber Kiosks. The ability to have this point of reference, challenge and external expertise has been critical in our development of assessments, policy, practice, procedure and training, all of which underpin Cyber Kiosk use in Police Scotland. Minutes of these meetings can be found on the Police Scotland Website.

2.2 We are grateful to members of both groups for their ongoing support and input.

Stakeholder Reference Group Membership

- Scottish Police Authority (SPA)
- Her Majesty's Inspectorate of Constabulary Scotland (HMICS)
- SPA Forensic Services
- Scottish Police Federation (SPF)
- Staff Associations
- Crown Office and Procurator Fiscals Service (COPFS)
- Police Scotland Information Management

External Reference Group

- Open Rights Group
- Scottish Human Rights Commission (SHRC)
- Privacy International
- Information Commissioner Office (ICO)
- Scottish Institute for Policing Research
- Academia
- Mr Aamer Anwar

2.3 In addition, we have been grateful for the support and input from the Police Scotland National Independent Strategic Advisory Group (NISAG) in their role as 'critical friend' to provide advice to Police Scotland on policies and processes.

2.4 As a consequence of this active and ongoing engagement, Police Scotland has developed a comprehensive suite of documents in support of Cyber Kiosk use:-

  - Data Privacy Impact Assessment (DPIA)
  - Equality & Human Rights Impact Assessment (EqHRIA)
  - Cyber Kiosk Toolkit - for operatives
  - Examination Request Guidance Document
  - Digital Forensic Examination Principles – public commitment to how Police Scotland will conduct examinations
  - Consent Digital Forensic Examination – Victims & Witnesses
  - Process Map – From Cyber Kiosk to Hub (Digital Forensic Unit)
  - Public Information Leaflet
  - Public FAQs – Digital Evidence Examination

2.5 We anticipate submitting these to the respective Reference Groups for further consultation prior to our next meetings on 11 June 2019.

2.6 **DPIA Development -** Police Scotland recognises that specific concerns have been raised by both group members and the wider public in relation to data privacy. Mr. David Freeland, (ICO) is a valued member of the External Reference Group and has provided comment as we have developed our document suite, in particular, in relation to the DPIA.

2.7 Police Scotland recognises the risk associated when accessing citizens' data during the triage process. It is accepted that it will not be possible to remove all risk of collateral intrusion in digital device examination however, this can be minimised and mitigated. The draft DPIA now addresses same, outlining mitigations and associated risk scores. The Cyber Kiosks are used to 'triage' relevant data held on digital devices, not 'extract everything wholesale'.

2.8 A principle of data protection law is that the information that is obtained must be adequate, relevant and limited to the specific purpose. Police Scotland's proposed use of Cyber Kiosks takes cognisance of this principle. They provide the capability for more focused triage, facilitating a more relevant, limited and specific review of data and potentially negate the need for download of digital devices. This significantly reduces the risk of collateral intrusion and may negate the requirement for submission to the Digital Forensic Hub for a more detailed examination.

2.9 **Equalities Implications -** Matters raised by the Scottish Parliament Justice Sub-Committee on Policing pertaining to data privacy, human rights and legal basis have been considered and mitigated in the aforementioned DPIA, EqHRIA and wider document suite. The Legal Opinion received from Senior Counsel indicates that all key ECHR Articles will be complied with.

2.10 **Victims, Witnesses and Consent –** We are aware of recent media reporting regarding English Police Forces' engagement with victims of sexual crime and in particular, obtaining access to digital devices.

2.11 Unfortunate language has been used in many media reports referencing 'digital stop search' and 'digital strip search'. To be clear, there is no change in policy for Police Scotland. Triage of digital devices or indeed more detailed forensic examinations have and will only ever be undertaken in Police Scotland when there is a legal basis for the seizure and examination of that device, or where consent has been recorded.

3. SCOTTISH PARLIAMENT JUSTICE SUB-COMMITTEE ON POLICING

3.1 The Sub-Committee began its consideration of Police Scotland's proposed use of Digital Triage Devices in May 2018. Various contributors, including Police Scotland, have provided oral and written submissions.

3.2 On 8 April 2019, the Sub-Committee published *"Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks)."*

3.3 Police Scotland welcomes the Report, which confirms the need to progress policing into the digital age in an appropriate manner to maximise public safety. The key themes of the Report directed toward Police Scotland are in respect of Cyber Kiosk trials conducted in Edinburgh and Stirling, oversight, governance, finance, procurement, engagement, consultation and the legal basis for use of Cyber Kiosks.

3.4 We are now satisfied that we have addressed all matters arising. Specific details in relation to this are attached at **Appendix A – Police Scotland Interim Feedback Response to Justice Sub-Committee on Policing Report.**

3.5 **Kiosks Trials in Edinburgh and Stirling** – Police Scotland has previously acknowledged to the Sub-Committee that there were certain shortcomings in the trials conducted with regard to Cyber Kiosks. This has been taken on board throughout the organisation.

3.6 **Oversight & Governance –** As previously indicated, Police Scotland has developed a suite of documents to support and articulate our policy, practice, procedure, and training in our proposed use of Cyber Kiosks.

3.7 **Finance/Procurement –** Cellebrite has been used across Police Scotland's command areas for a number of years as a forensic tool used by examiners. In April 2018, 41 Cyber Kiosks and associated licence/support were purchased at a cost of £370,684 (excluding VAT). We have made a significant investment in support of transforming the service and it is imperative that we introduce this capability.

3.8 **Engagement & Consultation –** See Section 2 of this report.

3.9 **Legal Basis for Use of Cyber Kiosks -** Both Police Scotland and COPFS have, from the outset, been confident about the existence of a proper basis in law for the proposed use of Cyber Kiosks. Nonetheless, it has also remained conscious that other views have been offered on the same issue.

3.10 To offer reassurance, Police Scotland has sought and secured the Legal Opinion of leading Senior Counsel, Murdo MacLeod QC. The Opinion is clear and unambiguous – there is a lawful basis for the use of Cyber Kiosks. In the interests of public transparency and confidence, a copy of this Legal Opinion has been provided as an accompaniment to this report for publication on the Scottish Police Authority website. The legal opinion will also be shared with members of the External and Stakeholder Reference Groups

3.11 In addition, on 20 March 2019, Lindsay Miller, Deputy Crown Agent Serious Casework, COPFS, replied to the Convenor of the Sub-Committee in response to a request regarding legal basis to;

"Please give your view on whether or not, at present, Police Scotland can legally use this new technology, or whether you consider that further consideration of this issue or further action is needed before these devices can be rolled out''.

3.12 The response supported the existence of a legal basis for use of the technology and considered existing practices and the role of Scottish Courts.

''The introduction of the Digital Device Triage Systems would not change the process Police Scotland Digital Forensic Hubs currently use to provide relevant evidence from a digital device to COPFS…it is perhaps of note that Police Scotland Digital Forensic Hubs currently examine thousands of digital devices every year, providing evidence to COPFS which is in turn presented at court, subject to legal scrutiny and is often crucial in securing convictions in all types of cases including the most serious and complex''.

3.13 The following was provided with specific reference to powers of examination;

''As was highlighted in my letter to Police Scotland dated 30 January 2019 the Police do have powers of seizure and examination which apply irrespective of whether it is a digital device or any other item. Those powers are governed by legal provisions and principles.

Where a digital device is seized by Police Scotland and examined then the seizure and examination should comply with the provisions and principles outlined, failing which, any evidence secured will risk being ruled inadmissible by a Court based on it having been secured unfairly. That applies whichever process is used to examine the device, including the use of the Digital Device Triage System."

3.14 In conclusion, Police Scotland is entirely satisfied that the use of cyber kiosks is lawful and that we have developed robust policy, practice and procedure which underpins the values of the Service and how we seek to interact with and protect the citizens of Scotland.

4. Next Steps

4.1 There has been considerable attention in respect of Cyber Kiosks, including consideration by the Scottish Police Authority parliamentary scrutiny, and input from other interested parties. This has added significant value to the development of Police Scotland's delivery considerations and response to the changing patterns of crime. We will continue to consider the Justice Sub-Committee's Report and the recently received Legal Opinion while engaging in ongoing discussions with the Authority.

In addition, the following actions/activities are ongoing:-

- Training of 410 police officers (*training completion anticipated 10 May*).
- Suite of documents (as referenced in paragraph 2.4) to be finalised and provided for further consultation (*document finalisation anticipated 21 May*).

- Training De-Brief to be completed *(anticipated 28 June)*.

- The Stakeholder and External Reference Groups will meet again on 11 June 2019 *(anticipated final comment regarding the document suite to be gathered at this meeting and documents finalised for 28 June 2019).*

4.2 We are cognisant that the ICO is still considering UK Law Enforcement's use of Digital Triage Devices and we understand that a related report will be published in the summer of 2019. Active engagement with the ICO will continue, however as outlined previously, the existing law is clear and unambiguous, providing a lawful basis for use.

4.3 Police Scotland must ensure it remains at the forefront of victim support, service delivery and crucially, continues to support the administration of criminal justice. The provision of technological capability to meet demand and alleviate some of the pressures being placed on both front line officers and specialist teams is imperative. Failure to provide such capability seriously undermines our commitment to Keeping People Safe.

4.4 Now that we have unambiguous clarity from both COPFS and independent Senior Counsel on the legal basis for their use, and subject to ongoing discussions with the Scottish Police Authority, in the interests of the safety of citizens in Scotland, our intention is to start the operational roll-out of Cyber Kiosks as soon as is practicably possible.

5. FINANCIAL IMPLICATIONS

5.1 As outlined above Section 3.7.

6. PERSONNEL IMPLICATIONS

6.1 Frontline officers trained in the use of the technology will be able to offer an improved level of service to our communities.

7. LEGAL IMPLICATIONS

7.1 Whilst we are confident that existing law supports our use of Cyber Kiosks, it is clear that this matter will rightfully remain a matter of public scrutiny. The challenge remains for Police Scotland to ensure we are capable of investigating crime whilst balancing civil liberties and managing the need to Keep People Safe.

7.2 Further detail - As outlined above Section 3.9-3.14.

8. REPUTATIONAL IMPLICATIONS

8.1 As a Service we require to be relevant in a digital age. This fundamental frontline triage capability is but one element of a significant technological transformation required to ensure we are efficient, effective and digitally capable. Any continued compromise to service delivery is not acceptable to Police Scotland or the communities we serve.

9. SOCIAL IMPLICATIONS

9.1 As outlined at 4.3.

10. COMMUNITY IMPACT

10.1 Police Scotland requires the appropriate and necessary capabilities to protect the citizens of Scotland – especially the most vulnerable.

11. EQUALITIES IMPLICATIONS

11.1 All aspects have been considered and mitigated in the aforementioned DPIA and EqHRIA.

12. ENVIRONMENT IMPLICATIONS

12.1 The ability of frontline officers to have ready access to triage capability has a positive impact environmentally as there is the opportunity to reduce the number of digital devices being submitted and transported to Digital Forensic Units located across the country.

RECOMMENDATIONS

Members are requested to note the information contained within this report.

Appendix A

Scottish Parliament Justice Sub-Committee on Policing

Interim Feedback Response

COMMITTEE PARAGRAPH REFRENCE	JSC EVALUATION CONTENT	PSoS RESPONSE
43.	The Sub-Committee is concerned to learn that Police Scotland undertook trials of using cyber kiosks to search the mobile phones of suspects, witnesses and victims of crimes in Edinburgh (E Division) and Stirling (J Division) without undertaking the required governance, scrutiny and impact assessments. Those members of the public whose phones were seized and searched were not made aware that their phones were to be searched using cyber kiosks as part of a trial, or the implications, and were not provided with the option of giving their consent.	In relation to Sub-committee evaluations at page 9, paragraph 43 and 44, it is important to provide formal recognition that the trials conducted with regard to Kiosks fell below the standard that would be expected of the Service. Police Scotland acknowledges that as an organisation such trials and pilots should have been better conducted in terms of management, governance, data collection and the required assessments and this is a matter which has been taken on board throughout the organisation.
44.	Cyber kiosks are able to access personal and private data including data protected by passwords, and to copy large quantities of data. The Sub- Committee is concerned that this technology was used on a trial basis without any human rights, equality or community impact assessments, data protection or security assessments, and in the absence of any public information campaign. The decision to purchase 41 cyber kiosks seems to have been taken without any analysis of the outcomes of the two trials by the Scottish Police Authority.	As per Above
45.	The Sub-Committee fully supports Police Scotland's ambition to transform to effectively tackle digital crime. However, prior to the introduction of any new technology to be used for policing purposes, an assessment of both the benefits and the risks should have been carried out. It appears that, in relation to the introduction of cyber kiosks, only the benefits were presented by Police Scotland to the SPA, with the known risks identified in the Police and Crime Commissioner for North Yorkshire's report, and any issues raised in feedback from those within J Division, not provided. The Scottish Police Authority, for its part, seems to have accepted the information provided with very little critical assessment.	As per Above
46.	This lack of effective scrutiny puts the reputation of the police service, and the rights of the public, at risk. It has also led to the investment of over half a million pounds in technology that, at present, Police Scotland is unable to use.	As per Above

Appendix A

75.	The Sub-Committee questions the rationale for commencing training of police officers in the use cyber kiosks prior to the question of the legal basis of their use being determined and the necessary equalities and human rights and data protection impact assessments being finalised. The timing of any training for officers seems to have prejudged the outcome of any such assessments, which had not been completed by that point in time.	Police Scotland has maintained a confidence in an existing legal basis now confirmed by Senior Counsel Opinion. It is important to signify the stage at which the Impact Assessments are at and again refer to the support provided by External Reference and Stakeholder Groups regarding the suitability of those assessments to support training, a decision made in recognition that the legal basis supporting use was at the time under continued consideration. The training and engagement of the Kiosk operators will not terminate at the point of qualification. Mechanisms are in place to ensure ongoing communication and review of Kiosk use post implementation which includes the ability to provide any updates to guidance or processes should the need arise. Any such need identified as a result of changes to guidance or the assessments at the conclusion of the considerations surrounding the legal basis can be shared with these officers prior to Kiosk implementation. The logistical challenge of training is considerable and has taken seven months. It was felt prudent in light of the aforementioned approval to continue with the training to ensure resources were in place should equipment use be authorised.
76.	The Sub-Committee asks Police Scotland to provide details of the results of its evaluation of the training provided to officers to operate cyber kiosks.	The full evaluation to be carried out at the conclusion of training is yet to be undertaken (training scheduled to finish on May 9 2019) however activity is underway to ensure this is in place. In December 2018, Post Phase 1 Evaluation was undertaken, the findings of which were presented to the External Reference and Stakeholder Groups in January 2019.

Appendix A

77.	The Sub-Committee asks Police Scotland to confirm whether training provided to police officers for the use of cyber kiosks is to be on-going, and updated to include human rights, data protection and security requirements.	Human rights, data protection and security requirements have formed part of Kiosk operator training from the outset. In addition to the training package provided by Cellebrite, Police Scotland designed and delivered an additional Module of the course (Module 1), delivered to all trained officers which provided guidance on the Human Rights and Data protection implications of device examination. This module was designed using the feedback provided by contributors during compilation of the respective Human Rights and Data Protection Impact Assessments which were ratified by the Stakeholder and External Reference Groups on 30 October 2018 as sufficiently advanced to support training which commenced in November 2018.
87.	As the contract award notice included known capital and revenue costs, which combined were above the £500,000 threshold of Police Scotland's authority, the Sub-Committee would have expected the SPA to consider this expenditure prior to publishing the contract.	The SPA's Scheme of Delegation provides that tenders and contract awards for goods and services of up to £500,000 can be authorised by Police Scotland, Head of Procurement, without a requirement for additional authorisation by the Chief Executive Officer of the SPA. In the case of the Kiosks this procurement was funded by allocated capital funds, under £500,000, therefore the contract award of £370,684 (exc VAT) or £444,821 (inc VAT) could be authorised by Police Scotland, Head of Procurement, in accordance with SPA Scheme of Delegation. Police Scotland acknowledge the direction from SPA around this matter.
95.	The Sub-Committee welcomes Police Scotland's establishment of the stakeholders' group and the external reference group to consult on its proposal to use cyber kiosks.	Police Scotland welcomes the evaluation by the Sub-Committee in relation to its support for the implementation and continued engagement of Police Scotland with the Stakeholder and External Reference groups outlined in Paragraphs 95 and 96. We take this opportunity to thank members for their valued contributions to this issue and assure both groups and the Justice Sub-Committee that their investment has provided the Service with direction and

Appendix A

		a framework for the implementation of new technology and associated policies within Police Scotland in future, allowing our decisions to be better informed.
96.	The Sub-Committee views consultation with relevant stakeholders prior to the implementation of new policing policies or technology as best practice. It is essential for public confidence that Police Scotland demonstrates that it has given due consideration to the views of the stakeholders' group and the external reference group on its proposed introduction of the use of cyber kiosks.	As above
143.	The Sub-Committee is still not reassured that the legal framework being relied upon by Police Scotland for the use of cyber kiosks is suitably robust or provides the necessary safeguards for members of the public. Any process must be mindful to protect the integrity and robustness of the investigation and prosecution service.	Police Scotland remains confident a legal basis for Kiosk use. On 29 April 2019 Opinion of Senior Counsel was received on the legality of Digital Device Triage Systems (Cyber Kiosks). The principal conclusion states; ''there is lawful basis for the use of cyber kiosks''
144.	The Sub-Committee recognises the importance of public confidence in policing and policing by consent. There is, therefore, an urgent need for clarity and public reassurance before this new technology can be introduced.	The Service has recognised the requirement for the enhancement of the means in which we capture device examination consent from victims and witnesses as is acknowledged by DCS Gerry McLean on page 18, paragraph 99. Police Scotland has commenced activity to design and implement a new Force Form to accurately and adequately capture the freely given, specific, informed, unambiguous and ongoing consent of victims and witness. Police Scotland is of a view that implementation of this would be essential to any proposed roll out of Kiosks.
145.	The Sub-Committee believes that a legal framework is required which 'keeps pace' with technology. The Sub-Committee recommends that the Cabinet Secretary for Justice considers whether the current legal framework enables Police Scotland to seize and search digital devices, and considers the suggestions provided to the Sub-Committee to resolve the legality issue.	Although this evaluation is not directed at Police Scotland it should be noted that the Independent Senior Legal Counsel received by Police Scotland on 29 April 2019 whilst clear and unambiguous that there is in Scots Law a legal basis for the use of Cyber Kiosks it is acknowledged that this matter might

Appendix A

		benefit from further detailed consideration.
148.	The Sub-Committee asks the Scottish Police Authority to confirm its planned scrutiny of Police Scotland's review of its use of digital device triage systems, including the proposal to consider extending their use to export and store data, and Police Scotland's data security and retention policies and practices to support its proposed use of cyber kiosks.	Although a question directed to the Scottish Police Authority it is perhaps of assistance to note that there is no current proposal to review the use of Kiosks with a view to extending their capability to anything other than triage. Any extension in use would be considered only when appropriate and after sufficient time and scrutiny regarding the current proposed usage had achieved the confidence required. This would involve the review and appropriate amendment of the associated training and documents including Human Rights and Data Protection Impact Assessments.
149.	The Sub-Committee do not believe that the cyber kiosks should be deployed by Police Scotland until equalities and human rights and data protection impact assessments are agreed by key stakeholders.	Police Scotland now have unambiguous clarity from both COPFS and Independent Senior Counsel that the legal framework exists and there is a legal basis for use of the Kiosks by Police Scotland.
150.	The Sub-Committee do not believe that the cyber kiosks should be deployed by Police Scotland until clarity on the legal framework is established.	As Above
160.	Similar legal concerns regarding Police Scotland's digital forensic hubs were raised in evidence. This issue was not part of the remit of the Sub- Committee's inquiry, but would merit consideration by the Cabinet Secretary for Justice.	It is clear to Police Scotland that any determination taken with regard the use of Kiosks must be considered with regard to the implications on Digital Forensic Hubs.

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