Justice Sub-Committee on Policing

Police Scotland's proposed use of digital device triage systems (cyber-kiosks)

Written submission from Open Rights Group

Open Rights Group welcomes the openness and engagement in the consultation process that Police Scotland have undertaken. Their willingness to take criticism and advice to improve their current practices is a refreshing one and something police forces across the United Kingdom would do well to take on. However, Open Rights Group cannot fully endorse an immediate rollout programme until a clear legal basis is provided and reflected in improved policy documents including the Data Protection Impact Assessment and Equality and Human Rights Impact Assessments and a demonstration that the use is subject to appropriate safeguards and oversight.

Further and more importantly while the reference group was formed to specifically consider the roll-out of cyber kiosks in a triage context, Open Rights Group considers that the best solution for a clear legal basis is to establish a holistic framework that covers (a) lawful bases for seizure, or surrender with informed consent, of devices (b) preliminary examination and selection (triage) that the kiosks will perform and (c) the operation and oversight of the pre-existing Cybercrime Hubs when triage results in the device being subjected to further, Hub, examination.

The kiosks may bring benefits in terms of reducing backlogs. The means by which devices are sent for kiosk review must be underpinned by a full and proper legal framework, well beyond the present state of the assessments. If the full framework does not also apply to the operation of the Cybercrime Hubs then the validity of material applying only to kiosks is undermined.

Assessing the Impact Assessments, statements from other stakeholder meetings involving members of the Crown Office Procurator Fiscal Service, and applying international human rights standards, it is clear that the legal basis has not been clearly articulated.

Other issues exist, and some flow from the lack of a legal basis. This submission from Open Rights Group seeks to illustrate some of the most pressing questions that need to be dealt with.

The use and operation of digital forensics, which could involve both the kiosks and the Cybercrime Hubs, represent an interference with fundamental human rights and engage data protection as a processing activity, including sensitive personal data. In recognition of this, Police Scotland have prepared a Data Protection Impact Assessment and Equality and Human Rights Impact Assessment.

These impact assessments, while undergoing improvements throughout the consultative process, leave fundamental questions unanswered.

Key Questions:

- How does the current explanation of legal framework satisfy the "quality of law" test?
- What common law powers would the Police likely use to seize and examine phones?
- How are the parameters of an examination sufficiently narrowly defined to prevent arbitrary interference?
- How is the public expected to understand the different powers of seizure with the myriad legislative provisions?
- How does the inclusion of the category "unknown" in the list of types of individual's devices satisfy the data protection principle that personal data relevant, accurate and up to date?
- How does the current system satisfy Data Protection Act 2018 requirements for law enforcement processing of sensitive personal data?

The categories of personal data and sensitive personal data that will inevitably be present on every type of modern device, and which will be thus examined during kiosk reviews include:

- Personal health and medical data
- Racial or ethnic origin;
- Sexual interest and sexuality;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership.

Digital devices carry so much of our personal lives it is our diary, our calendar, our correspondence, our photos, our location. Never before has so much of a person been available in a single piece of property. It is of the utmost importance that Police Scotland's framework reflect the nature of the interference, giving due regard to the insights devices provide, and giving the public and others clarity as to their rights, the limits of police powers and the safeguards that come with it.

'Quality of Law'

In the Human Rights Impact Assessment at pg. 6, Police Scotland provide the legal framework for Kiosk Use.

> "The police are entitled at common law to seize anything it is reasonably believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure."
>
> "All seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision."

According to the European Court of Human Rights, National law must be clear, foreseeable and adequately accessible.[1] Domestic law must indicate with reasonable

[1] Silver and Others v. United Kingdom, para 87.

clarity the scope and manner of exercise of the relevant discretion given to public authorities, in this case Police Scotland, so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society.[2]

For foreseeability, the test for 'in accordance with the law' is key for human rights assessments, not only to establish the necessity and proportionality of a measure, but also to give the public clarity and foreseeability about their rights. Domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which, and the conditions on which, the authorities are entitled to resort to measures affecting their fundamental human rights.[3] Vague references to common law powers and statutory powers that don't contain provision for seizure fail to give satisfactory foreseeability.

These principles are so important that a finding that the measure was not 'in accordance with the law' suffices for the European Court of Human Rights to hold that there has been a violation of Article 8 of the European Convention on Human Rights.[4]

The legal framework underpinning the use of the Cybercrime Hubs, for which kiosks are intended to be a new preliminary stage, are a mix of common law powers, statutory power that makes provision for seizure, and statutory offences that make no provision for seizure. This imprecision is concerning. It leaves the public in the dark about the foreseeability and clarity of Police Scotland's powers in a scenario where intimate and sensitive personal information could be examined.

Open Rights Group is concerned that the current legal framework regarding the seizure, examination and subsequent extraction of data is not sufficiently clearly articulated or comprehensive so as to be foreseeable and thus satisfy human rights standards.

Police Scotland anticipated this problem in the formation of two groups. One, the reference group, was made up of organisations such as the Information Commissioner's Office, the Scottish Human Rights Commission, Privacy International, and representatives from Open Rights Group, among others. This new panel augmented the pre-existing stakeholder group, which included Crown Office Procurator Fiscal Service, Her Majesty's Inspectorate of the Constabulary, and the Scottish Police Authority, amongst others. The remit of the latter stakeholder group was "to look at implementation within a legal framework"[5].

In minutes released on the deliberations of the stakeholder group, representatives from Crown Office emphasised the need to inform the public what common law

[2] Piechowicz v. Poland, para 212
[3] Fernández Martinez v. Spain, para 117.
[4] M.M. v. The Netherlands, s.46.
[5] Digital Triage Device (Cyber Kiosk) Stakeholder Reference Group, Minute of the Meeting, 26 July 2018, page 2 http://www.scotland.police.uk/assets/pdf/138327/307421/501417/Cyber-Kiosk-Stakeholder-Meeting-Minutes-July-2018?view=Standard .

powers allowed them to do.[6] Importantly that information needed to inform members of the public that in some cases they do not need to comply. From what information is provided in the document sets and what public facing documents would be available, it is far from clear how the public could be considered to be informed at this stage.

Further, in supplementary correspondence to the Justice Sub-Committee on Policing, the Information Commissioner's Office on 2 November 2018 noted that the Crown Counsel were expected to deliver information regarding legal basis to Police Scotland which would then be sent on to the Reference Group.[7] No document has been received as of yet by the Reference Group members. This indicates that more work needs to be done to on legal basis, and that Police Scotland admit as much.

The Sub-Committee should satisfy themselves that the legal basis of the whole digital forensics framework is satisfied before deciding whether the roll-out of the forensic kiosks should progress

Proportionality of searches

As a result of the lack of clear legal basis it is difficult to assess the proportionality of the kiosks. For instance, what would be a parameter of a search that would be deemed proportionate, a specific date, communications to a specific number, or list of numbers, a specific location? All of these? It is not clear from the current framework provided how the searches are going to be suitably limited.

This is particularly important given the amount of information contained on modern mobile devices. Until a clear legal framework is articulated, understanding the proportionality of the kiosk in its search capabilities is guesswork.

Failing data protection principles - Processing 'unknown' data

The General Data Protection Regulation is underpinned by seven key principles, these range from requirements for processing to be lawful and fair, all the way to adequate security being in place. The fourth Data Protection Principle is that data is adequate, relevant and limited to what is necessary, this is known as data minimisation.[8]

This principle is important because it requires a data controller, in this case Police Scotland, only collects and processes data that they actually need. The Information

[6] Digital Triage Device (Cyber Kiosk) Stakeholder Group, Minute of Meeting, 27 July 2018, Page 5 http://www.scotland.police.uk/assets/pdf/138327/307421/501417/Cyber-Kiosk-Stakeholder-Meeting-Minutes-27-July-2018?view=Standard.

[7] Police Scotland's proposed use of digital device triage systems (cyber-kiosks), Supplementary written submission from the Information Commissioner's Office, 2 November 2018, http://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICOsupplementary.pdf.

[8] Article 5.1(c), General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Commissioner's Office has said that data minimisation is particularly important in law enforcement processing or processing of sensitive personal data.[9]

At page 22 of the Data Protection Impact Assessment, when asked how a clear distinction would be made between personal data relating to different categories of data subjects, Police Scotland lay out the four categories of data subjects they plan to use for this purpose:

- Suspects
- Witness
- Victim
- Unknown

The inclusion of the latter category "Unknown" raises concerns about the relevance and adequacy of the data processed. It is difficult to see how you can maintain the data is relevant if the category it exists in is unknown by definition.

Open Rights Group recommends removing the 'unknown' category from the categories of data subjects included in the operation of digital forensics and subsequently reflecting that in the Data Protection Impact Assessment.

Law enforcement processing 'sensitive personal data'

Searches by the kiosk are going to process sensitive personal data. Sensitive personal data is a category of personal data in the Data Protection Act 2018 that have sensitive characteristics attached, these categories are found in the General Data Protection Regulation and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health, or data concerning a natural person's sex life or sexual orientation, among others.[10] The Data Protection Impact Assessment provided by Police Scotland at page 11 (Q16) recognises that there will be sensitive processing undertaken.

The processing of sensitive personal data brings additional responsibilities, particularly articulating an additional basis for processing. Law enforcement processing of sensitive personal data is permitted only in two limited cases set out in the Data Protection Act 2018 at section 35 (4) and (5).

Section 35(4) is for cases in which the data subject has given consent, this is not considered here as Police Scotland state at page 15 that the basis for processing data in the kiosks is not a consensual basis.

35(5) requires that (a) the processing is strictly necessary for the law enforcement purpose and (b) meets at least one additional condition found in Schedule 8 and (c) at the time when the processing is carried out, the controller (Police Scotland) has an appropriate policy document in place.

---

[9] Information Commissioner's Office, Guide to the General Data Protection Regulation, principle (c) : Data Minimisation, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

[10] Article 9(1), General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

An appropriate policy document needs to, among other things, "Explain the controller's procedures for securing compliance with the data protection principles" and "Explain the controller's policies regarding the retention and erasure of personal data processed".[11] Given the need for a clearer legal basis to be articulated, put forward earlier in this document, Open Rights Group considers that the current document sets are not yet satisfactory as an appropriate policy document and would urge clarity to be sought and reflected in the documents before operation of the cyber kiosks takes place.

Open Rights Group recommends that due to the need for a clear legal basis to be provided, Police Scotland should consider whether its intended processing of sensitive personal data meets the required standards set out in Data Protection Act 2018.

Consider the entire cyber framework

The report from Privacy International 'Digital Stop and Search' explains that the majority of police forces in the United Kingdom use a model similar to the one proposed by Police Scotland, where kiosks carry out analysis and Hubs are used to serve a number of forces.[12] The work currently being undertaken to only scrutinise the laws and policies to underpin the kiosks are arguably missing the bigger picture, and the bigger opportunity.

The current status of police force's operating digital forensic kiosks across the UK is under scrutiny by the Information Commissioner's Office.[13] Questions have been raised about the suitability of the Police and Criminal Evidence Act 1984 for the task of grappling with seized digital devices.[14]

Police Scotland are facing the same questions regarding the suitability of its own system. There is an opportunity to develop a holistic model that encompasses the whole seizure, examination, and extraction of data from a digital device. Without taking a view of the whole system Police Scotland face continued questions being raised regarding the suitability of their digital forensics regime. The kiosks may bring benefits in terms of reducing backlogs, particularly if underpinned by a proper legal framework but if that framework fails to apply to the operation of the Cybercrime Hubs then it would undo all of that worthwhile work.

Open Rights Group call for a full assessment of Scotland's digital forensic legal framework and support a holistic approach incorporating all stages of device seizure, examination, and extraction of data.

---

[11] Section 42(1), Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/contents.
[12] Digital stop and search: How the UK police can secretly download everything from your mobile phone, pg. 6 and graph on pg. 11, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.
[13] Correspondence from David Freedland to Justice Sub-Committee on Policing, 29 October 2018, http://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/ICT-ICO.pdf and also reporting from Peter Swinden, Police probed over data trawl of mobile phones, https://www.heraldscotland.com/news/16207864.police-probed-over-data-trawl-of-mobile-phones/.
[14] Police should need warrants to search mobile phones, say campaigners, The Guardian, January 2017 https://www.theguardian.com/uk-news/2017/jan/13/police-warrant-search-mobile-phones-campaigners-privacy-international.

Matthew Rice
Scotland Director
Open Rights Group
13 November 2018