62 Britton Street
London, EC1M 5UY
United Kingdom
T +44 (0)203 422 4321
@privacyint
www.privacyinternational.org

12 March 2019

By email only

John Finnie MSP
Convener, Justice Sub-Committee on Policing
c/o Justice Sub-Committee Clerks
Room T2.60
The Scottish Parliament
Edinburgh, EH9 1SP

Dear Mr Finnie,

Re: **Digital device triage systems**

Thank you for your letter of 27 February 2019, seeking Privacy International's view on whether we are satisfied that Police Scotland can legally use cyber kiosks. Privacy International's view is that further consideration / action is needed as we are not satisfied that there is a clear legal basis. Privacy International is further dissatisfied regarding the legal basis for the use of mobile phone extraction technology at the cybercrime hubs and would urge the Committee to expand its consideration of this technology to their use both at cyber kiosks and cybercrime hubs.

We note that Police Scotland is confident of the legal basis to support the use of the cyber kiosks, and in an effort to move this discussion forward, we join the calls for the Police to make this legal advice public and set out the lawful basis in clear straightforward terms, as requested during the Committee meeting in December 2018.

As you note in your letter, Privacy International is one of the members of the Digital Triage Device (Cyber Kiosk) Reference Group. Unfortunately, we have not been in a position to attend the last two meetings. However, we have sought to follow the work of the Committee as it relates to this matter and are in touch with Open Rights Group who are also represented on the Reference Group. We are also continuing to engage with the UK Information Commissioner's Office in relation to their ongoing investigation into the use of mobile phone extraction technology across the UK.[1]

[1] In April 2017, Privacy International submitted a complaint to the ICO concerning the use of mobile phone extraction technology by Police Forces https://privacyinternational.org/sites/default/files/2018-

Our concerns around the legal basis for the use of mobile phone extraction technology have been raised in the evidence the Committee has received from Diego Quiroz from the Scottish Human Rights Commission, David Freeland from the UK Information Commissioner's Office as well as submissions from the Open Rights Group.

As noted above, to date, we remain unconvinced that the Police have a clear legal basis for the use of mobile phone extraction technology. Notably, the legal framework relied on by Police Scotland lacks clarity and the related human rights and data protection concerns have not been sufficiently addressed. These concerns are not solely focused on the kiosks but extend also to the use of the technology at the cybercrime hubs – a point raised by Members of the Committee in December and echoed in the evidence provided by Mr Quiroz, Mr Freeland and the Open Rights Group.

The powers that the Police rely on will to an extent be fact dependent, however, the need for a clear legal basis is also a requirement of both the Human Rights Act 1998 and the Data Protection Act 2018. Any interference with rights under the Human Rights Act 1998 must be "in accordance with the law" and any processing of personal data by the Police must have a lawful basis under the Data Protection Act 2018. The law must be accessible, clear and foreseeable. Amongst the most critical concerns we have is that the use of mobile phone extraction technology is not accompanied by the safeguards of an independent warrant.

To this end, we understand the Police seek to rely on a range of common law and statutory powers (e.g. under the Firearms Act 1968, the Misuse of Drugs Act 1971 and the Criminal Justice (Scotland) Act 2016) and have also looked to existing case law. The Police state in their letter to the Committee of 15 October 2018, that when the "*power of search requires officers to retain evidence from a digital device then* [the Police] *have looked to case law; HM Advocate v Rollo 1997 JC 23 to describe the legal basis under which we retrieve information which is stored digitally.*" This case concerned contraventions under the Misuse of Drugs Act 1971 and access to a Memomaster Electronic Notepad. Police Scotland also shared the case of *J.L+E.I v. HM Advocate* 2014 HCJAC 35, concerning access to an iPhone 5 under the Criminal Procedure (Scotland) Act 1995. The Opinion delivered by Lord Brodie in *J.L+E.I v. HM Advocate*, states: *"For all that we were told, in the present case, examining the iPhone 5 involved little more than connecting the device to a power supply, switching it on and touching the appropriate portions of the screen. In our opinion, so doing was clearly within the powers conferred by section 14(7)."*

In our view, these cases are not sufficiently analogous / do not give full consideration to the matter in question both in terms of the technology and that our

---

04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf

devices are becoming ever more personal and pervasive in our lives with more and more data. This means that the difference between seizing and browsing versus examining a mobile phone as can be done via the kiosks and hubs is profound and not necessarily contemplated in the seizure powers the Police currently rely on.

We also note that the Committee's attention has already been drawn to decisions from other jurisdictions (e.g. the United States Supreme Court decision of *Riley v. California* [2014] 134 S. Ct. 2473 and the Canadian Supreme Court decisions of *R v. Morelli* [2010] 1 S.C.R. 253 and *R v. Fearon* [2014] 3 S.C.R. 621 and more recently *R v. Marakah* [2017] 2 S.C.R. 608 which have grappled with the issue of police access to data held on mobile phones. These decisions articulate the novel role of mobile phones in people's lives and highlight that in the majority of cases there is a need for a warrant / pre-judicial authorisation.

Thus, in our view, reliance by Police Scotland on these two named cases together with a patchwork of statutory provisions and powers, as we understand to be the case from evidence provide to date, does not meet the requirements of accessibility, clarity and foreseeability. It is not sufficiently clear what the basis for the use of this technology is in domestic law. It therefore does not have sufficient quality to be foreseeable to affected persons and whilst it is something Police Scotland are working towards, there are still questions as to whether there are adequate and effective guarantees against abuse.

Examination and extraction of data from mobile phones is highly intrusive of the right to privacy and data protection rights of not just the user of the phone but many others with whom they communicate and about whom they store data. Furthermore, it encompasses activities that are recognised as the interception of communications, equipment interference and the acquisition of communication data. Although not directly relevant to Police Scotland, the National Crime Agency and National Police Chiefs' Council provided evidence to the UK Parliament during discussion of the Investigatory Powers Act where they described "equipment interference" as encompassing physical access to and examination of a device.[2] Such power should be accompanied by a number of safeguards, including pre-judicial authorisation. Therefore, further consideration is required of the safeguard of such authorisation (see the European Court of Human Rights decision in *Zakharov v. Russia* [2015] 39 BHRC 435 and the position of the European Court of Justice in *Tele2 Sverige* [2017] QB 771).

In this regard, we have drawn the Reference Group's attention to two documents Privacy International has produced related to what a legal basis, necessity and proportionality analysis entail. The first is our "Guide to International Human Rights Law and Surveillance", which cites the relevant jurisprudence on the principles

[2] https://publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB63.pdf

underlying an assessment of any Article 8 interference.[3] The second is our "Government Hacking and Surveillance: 10 Necessary Safeguards".[4] This document outlines safeguards that we believe must accompany any use of government hacking (this includes equipment interference) and identifies the legal basis for these safeguards. On a related note, the Committee may be interested in an explainer[5] and video[6] on Mobile Phone Extraction that Privacy International has recently produced with Liberty.

Finally, Police Scotland is not alone in grappling with these issues. Privacy International's report[7] highlighted numerous deficiencies and the lack of a legal basis in forces across England and Wales using similar technology as Police Scotland. Whilst it is our position that these issues should have been resolved long before the procurement of this technology, it is to Police Scotland and the Committee's credit that this issue is being taken forward.

Should you require any further information or have any questions please do let us know.

Sincerely yours,

Ailidh Callander, Legal Officer
Privacy International

[3] https://privacyinternational.org/sites/default/files/2017-12/Guide%20to%20International%20Law%20and%20Surveillance%20August%202017.pdf
[4] https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf
[5] https://privacyinternational.org/feature/2718/your-local-police-force-could-download-everything-your-phone-without-your-consent
[6] https://privacyinternational.org/feature/2718/your-local-police-force-could-download-everything-your-phone-without-your-consent
[7] https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile