Thank you for the opportunity to comment to the scrutiny of the Sub-Committee on this issue. We have considered both the response to the letter of the Justice Minister on digital device triage systems (cyber kiosks) and the Legal Opinion provided by Police Scotland. The Commission is still not satisfied that the use of this technology by Police Scotland complies with the requirements of Article 8 of the European Convention on Human Rights (ECHR). This is because the law surrounding the use of cyber-kiosks lacks sufficient quality to be accessible and foreseeable. In addition, there are no adequate safeguards in place as the legislature (when enacted) did not consider situations of seizure and search in this particular context. Therefore the current framework or the lack of it does not provide sufficient and robust safeguards for people’s privacy rights in this context.

The Commission would like to acknowledge that the use of mobile device examination and other similar techniques consisting of checking the telephone records and social media activity of suspects and of some victims (for example missing persons/trafficked persons) could play an important part in the prevention and detection of crime. It is clear that protecting the public must involve recovering deleted and encrypted electronic information of those involved in criminal activity, however this measure should be taken in compliance with human rights law and standards. This is both in the interest of Police Scotland and the public in general. While the legality is fact dependent, it is reasonably foreseeable that there could be instances where the measure in question is not “in accordance with the law”. This is likely to be the case where it is deployed outside the context of judicial warrants.

We are also concerned that both Police Scotland and the Scottish Police Authority recent statements¹ do not fairly represent the advice of counsel. The

Legal Opinion is cautious and qualified in relation to the legal basis rather than ‘clear and unambiguous’. This is based on several recommendations within the advice given to strengthen the legal basis and the acknowledgment of a very limited legal analysis of this area of law in Scotland [Para 10]. The legal authority relied upon seems to offer a wide discretion by the police conducting the examination and not directly analogous for comparison. On the contrary, the existing legal analysis in other national and international courts stress the requirement of lawfulness and need of clear procedural safeguards to avoid arbitrary use of power and overuse of discretion.

The Legal Opinion also recognises the merits of developing a legislative framework fit for the digital age, and echoes our call for a statutory code of practice to cover the use of this kind of technology as the more appropriate option [Para 32 and 33]. The Legal Opinion points out the need for accessibility and foreseeability of the law and a further detailed consideration of the law to take place for example by the Scottish Law Commission [Para 31].

Where witnesses and complainants are concerned, the analysis is also insufficient [Para 29]. There are already questions of whether consent can be valid in the case of complainants given the pressures that they face and the imbalance of power. Recent cases over the ‘mandatory examination’ of complainants mobile devices in sexual offence cases make clear evidence of how challenging and unwelcome this can be. It is important to note that any information arising from a cyber-kiosk examination may be subject to disclosure in a prosecution. Furthermore, the use of warrants for complainants and witnesses also have implications for access to justice. These issues are not considered properly at the moment.

Given the cautious nature of the advice and the issues raised above together with Police Scotland’s ambition to be ‘world class in how they consider and tackle cybercrime’ [Para 1.2 of SPA report), it would not be appropriate for Police Scotland to proceed with the roll out of cyber kiosks on the current basis.

2 

JL v HM Advocate, 2014 JC 199 which is cited as binding authority, itself acknowledges that the requirements for examination would depend on the nature of the item and the nature of the information involved [Para 11].

3 For example: ECtHR, Huvig v. France, 1990; Gillan and Quinton vs the UK, 2010; Zakharov vs Russia, 2015 and Heino v. Finland, 56720/09. Also US Supreme: Court Riley v California, 2014. All these issues and a detail description of how MPB/E engages Article 8 of the ECHR and why the use of this technology is not currently compliant with Article 8 (in all cases) where presented in our letter to the Sub-Committee in March 2019.
We look forward to hearing more from the Cabinet Secretary on these points during his evidence to the Justice Sub-Committee on 13 June. Our view remains that way forward is the enactment of legislation in relation to all digital forensics\(^4\) and statutory guidance (e.g. a code of practice) covering the browsing and extraction of data from digital devices that integrate Article 8 requirements. We also favour the requirement of a judicial warrant for any search of mobile phones (and digital media), unless it is explicitly and clearly defined by law.

We are sending this correspondence to Police Scotland and to the Cabinet Secretary for Justice Humza Yousaf for their information.

The Commission would welcome the opportunity to discuss this issue further with you if you wish.

Judith Robertson
Chair, SHRC

---

\(^4\) The issue of right to privacy does not only involve cyber-kiosks and this would be in line with the Scottish Government’s approach to Biometrics and other Forensic Data for which a Code of Practice and Biometrics Commissioner is proposed.