Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

Audrey Nicoll MSP
Convenor
Criminal Justice Committee
Scottish Parliament
Justice.committee@parliament.scot

03 May 2022

Dear Convenor,

Criminal Justice Committee Roundtable Evidence Session on 18 May 2022: Tackling online Child Abuse, grooming and Exploitation

I refer to the call for evidence to support the above discussions and would offer the following brief comments relative to where such issues intersect with my functions as Scottish Biometrics Commissioner.

Firstly, and as the Committee will be aware, the true nature, extent, and impact of online child abuse, grooming, and exploitation is difficult to ascertain. There are however three things of which we can be certain. The first is that all available evidence suggests that such offending is on an upwards trajectory. The second is that whilst online child sexual abuse takes many forms, all are unquestionably child abuse. The third is that the scale of the challenge cannot be met by law enforcement alone.

In February 2020, HMICS published a strategic review of Police Scotland's response to online child sexual abuse.[1] This was followed up in August 2021 with a progress review against the ten recommendations previously made.[2] These reports by HMICS more than adequately capture areas where there is room for improvement in the policing of such matters.

In relation to the investigation of such offences, Police Scotland will regularly acquire, retain, use, and destroy materials constituting biometric data within the definition of section 34 of the Scottish Biometrics Commissioner Act 2020, primarily images and recordings. As highlighted by HMICS in 2020, there are over fourteen million images in the UK Child Abuse Image Database (CAID) alone and over 250,000 videos. Police Scotland is a user of, and contributor to that database.

Where Police Scotland use such data as part of overt policing activity then such data would fall within the oversight of the Scottish Biometrics Commissioner. However, my remit does not extend to biometric data obtained through covert policing activity under the Regulation of Investigatory Powers (Scotland) Act 2020, as these are reserved matters within the

[1] HMICS Strategic review of Police Scotland's response to online child sexual abuse, February 2020: https://www.hmics.scot/sites/default/files/publications/HMICS20200226PUB.pdf
[2] HMCS Progress review of Police Scotland's response to online child sexual abuse, August 2021: https://www.hmics.scot/sites/default/files/publications/HMICS%20Progress%20Review%20of%20Police%20Scotland%27s%20response%20to%20online%20child%20sexual%20abuse%20and%20exploitation.pdf

Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh EH7 4NL

authority of the UK Investigatory Powers Commissioner (IPCO). I also have no authority over biometric data collected by UK-wide bodies operating in Scotland.

One area of concern that is widely acknowledged around such investigations whether overt or covert is that of demand outstripping capacity in relation to evidential recovery through digital forensics techniques. Another is the absence of accreditation of the techniques deployed in Scotland in relation to digital forensics laboratory work.

Both HMICS and the SPA have previously recommended that Police Scotland should pursue accreditation of its digital forensics' laboratory work. In 2020, the SPA Digital Forensics Working Group recommended that Police Scotland should adopt the ISO 17025 quality standard by 2022. Police Scotland subsequently agreed to pursue this in May 2021, but I understand that it is likely to be 2024 before compliance is achieved.

My concern is that where digital material constituting 'biometric data' (primarily face and voice) is recovered in circumstances where it has the potential to enter the evidential chain from crime scene to court then it is essential that the scientific validity and reliability of the underpinning techniques deployed are beyond reproach. This is necessary to ensure that exculpatory evidence essential to the defence is not inadvertently overlooked.

To illustrate the complexity of such cases, I would draw the Committee's attention to the two case studies relative to online child abuse contained within page 15 of the SPA Digital Forensic Working Group report: https://www.spa.police.uk/media/flediwqv/rep-b-20200424-item-8-digital-forensics-wg-report.pdf as these illustrate the often industrial scale of offending in such cases.

As intimated at the outset, the nature and extent of this problem is such that it cannot be met by law enforcement alone. For me there are three key prevention areas which would deliver the greatest return on investment beyond policing. Those are:

1. Online safety education and training for children, young people and parents or guardians.
2. Technical solutions such as parental controls.
3. A duty of care and legal responsibility for website hosts and social media platforms who clearly have the technical capacity and capability to do more

I trust that these brief comments are of assistance.

Yours sincerely

Brian Plastow

Dr Brian Plastow
Scottish Biometrics Commissioner
Visit our website: https://www.biometricscommissioner.scot/