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

ACC Bex Smith
Assistant Chief Constable
Major Crime, Public Protection and Local Crime
Police Scotland
Tulliallan Castle
Kincardine
Fife
FK10 4BE

By e-mail to ACC Smith

05 October 2023

Dear ACC Smith,

Scottish Biometrics Commissioner Act 2020, Code of Practice: DESC

The purpose of this letter is threefold. Firstly, it sets out my concerns about the potential risks that arise from sensitive biometric data being ingested by Police Scotland to the current Scottish Government DESC pilot in Dundee. Secondly, by setting out those concerns in writing, I hope to assist DESC partners with post-pilot evaluation, including considering whether ingesting Scottish biometric data to a 'U.S. Headquartered' public Cloud solution may potentially bring Police Scotland into conflict with the Scottish Code of Practice.

Thirdly, setting out my juristic concerns on this matter publicly is prudent in terms of facilitating full and frank discussion between us prior to Police Scotland completing its self-assessment return relative to compliance with the Scottish Code of Practice.

I should say at the outset that I am of course mindful that it was Scottish Government who initiated the procurement process to deliver the Digital Evidence Sharing Capability (DESC) in 2019 prior to the Parliament having approved the final shape of the Scottish Biometrics Commissioner Act 2020. Scottish Government subsequently awarded the contract to Axon Public Safety in October 2021, which was also more than a year before the Code of Practice was approved by the Parliament. However, the ingestion of biometric data to the DESC pilot in Dundee by Police Scotland then commenced in early 2023, after the Code was already in force.

As you are aware, on 16 November 2022, the statutory Code of Practice on the acquisition, retention, use, and destruction of biometric data for policing and criminal justice purposes took legal effect in Scotland after being approved by the Parliament and Scottish Ministers.

My 4-year Strategic Plan laid before the Scottish Parliament sets out my programme of assurance activity until 2025, including an annual programme of compliance assessments on the Code based on a validated self-assessment methodology.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

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

On 22 April 2023, I wrote to you formally enclosing an Information Notice under section 16 of the Scottish Biometrics Commissioners Act 2020 relative to the uploading of biometric data by Police Scotland to the Scottish Government Digital Evidence Sharing Capability (DESC) pilot in Dundee. In my letter of 22 April 2023, I highlighted concerns around data protection and data sovereignty that had been highlighted in an article in Computer Weekly about the DESC pilot having been launched despite 'unresolved major data protection issues'.

The purpose of an Information Notice under section 16 of the Act is to enable the Commissioner to gather information to determine whether persons who are legally required by section 9 (1) of the Act to comply with the Code of Practice (in this case Police Scotland) are doing so. I am grateful to Police Scotland for responding fully to the Information Notice.

In a follow up discussion on 21 August 2023 with Police Scotland Chief Digital Information Officer Andrew Hendry and Fiona Cameron, Scottish Government, I explained that the response from Police Scotland, although helpful, did not ameliorate my specific concerns that the uploading of sensitive biometric data to DESC could potentially breach Principle 10 of the Code of Practice which seeks to promote privacy enhancing technology.

Although some media sources have questioned the legality of using hyperscale public cloud infrastructure for law enforcement processing[1], it is of course solely for the UK Information Commissioner (ICO) to offer advice (or not) on the UK Police Cloud landscape in terms of adherence to the processing of law enforcement data under the Data Protection Act 2018, Part 3. These are reserved matters that are entirely distinct from questions around compliance with the statutory Code of Practice in Scotland.

At the meeting with Andrew and Fiona, I also indicated that I would be gathering additional information about the uploading of such data to DESC during the formal process of assessing compliance with the Code of Practice, and during a separate but related assurance review on the use of images over the autumn and winter months. Therefore, if the loading of biometric data in the current pilot is continued, extended, or expanded, I would anticipate reaching a determination on whether the uploading of biometric data to DESC by Police Scotland complies with the Code of Practice early in the New Year. Any determination that it does not, would require me to submit a report to the Scottish Parliament about the failure to do so, and potentially further action as detailed in sections 23 to 27 of the Scottish Biometrics Commissioner Act 2020.[2]

On 28 August 2023, I wrote to you requesting that Police Scotland initiate self-assessment activity based on the questionnaire and supporting guidance provided by my office. I also requested that Police Scotland should complete the initial self-assessment activity by no later than 29 November 2023. I am again grateful to Police Scotland for the early positive engagement that has taken place on this, and more broadly for the excellent levels of co-operation and support since my appointment in 2021.

[1] Data protection watchdog raises concerns over Police Scotland pilot scheme: Sunday Post, 20 August 2023.
[2] Section 23 to 27 are permissive (the Commissioner 'may') and are entirely at the discretion of the Commissioner.

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

I also sought to provide reassurance that I will debrief and review this validated self-assessment process early in 2024 capturing points of feedback from SPA Forensic Services, Police Scotland, and the PIRC. This will enable me to refine the process for subsequent years based on experience of what works well or not so well, and to ensure that in future years there is no need to answer questions in areas where there have been no material changes to the information provided in this initial baseline assessment from 2023/24.

Against this introductory context, Police Scotland will be aware that question number 18.4 in the Code self-assessment questionnaire seeks information on the use of any Cloud based solutions provided by 'U.S. Headquartered' companies or their processors or sub-processors to host biometric data. It also asks for confirmation on how the security and sovereignty of that data is protected.

The DESC solution contract was awarded by Scottish Government to Axon who are a 'U.S. Headquartered' technology company. Axon also partners with 'U.S. Headquartered' Microsoft Azure as the Cloud hosting solution. DESC is a £33 million Scottish Government initiative to digitally transform how evidence is managed across the justice system. I am of course fully supportive of the need for digital evidence sharing to improve the effectiveness and efficiency of the justice system in Scotland. I also support the proposition that sensitive biometric data should be shared electronically between criminal justice partners providing that it can be done both safely and securely, and in a way that adheres to the statutory Code of Practice in Scotland.

However, a primary concern is that by Scottish Government opting for a 'U.S. Headquartered' solution provider (rather than a UK or EU Cloud provider, or a non-Cloud solution) to host sensitive biometric data (and other law enforcement data), and by sanctioning the holding of the data encryption keys for that data by Axon (rather than by Police Scotland), then such data is fully exposed to the provisions of The Clarifying Lawful Overseas Use of Data Act 2018 (US Cloud Act), and the related U.S. and UK data access agreement. The U.S. and UK agreement of course includes appropriate UKG oversight on the use of these legitimate investigatory powers, but there are also distinct devolution consequences for Scotland.

Data Sovereignty

My first concern is that data stored in DESC by Police Scotland will be under the authority of more than one country's laws. This will certainly be the case due to Scottish Government not selecting a UK or EU Cloud option (with common data protection and human rights frameworks and laws) or indeed a non-Cloud solution, and instead using a 'U.S. Headquartered' solution provider and a 'U.S. Headquartered' Cloud hosting solution.

Such UK/U.S. arrangements inevitably involve different legal requirements regarding data security, data privacy, and breach notification. You will also be aware that the reach of the U.S. Cloud Act extends anywhere in the world, and so the fact that DESC servers hosting Police Scotland data may be physically located in the UK is irrelevant.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

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

I am also aware that the Biometrics and Surveillance Camera Commissioner for England and Wales, Professor Fraser Sampson, has also expressed similar concerns about the lawfulness of using the public Cloud infrastructure for Part 3 DPA law enforcement processing, and that the Police Digital Service (PDS) and Home Office Biometrics (HOB) have introduced the 'PDS Xchange Programme' powered by 'U.S. Headquartered' Amazon Web Services which is now integrated with the UK law enforcement fingerprints database (IDENT1). Again, it is for the ICO to give advice on such matters relating to compliance with UK data protection law, however as there are more than 831,000 Scottish fingerprint forms within IDENT1, and Scottish access to the entire system, such UK decisions to 'offshore' biometric data in a 'U.S. Headquartered' Cloud solution also has potential devolution consequences for Scotland.

In my 2021/22 Annual Report and Accounts, and touching on the theme of data sovereignty, I made the following recommendation:

Recommendation 3: In contributing biometric or forensic data to UK policing systems, Police Scotland and the Scottish Police Authority should ensure they have the functionality to administer and maintain that Scottish data, in compliance with Scottish legislation and any Codes of Practice in terms of its use.

(Scottish Biometrics Commissioner Annual Report 2021/22, page 8, and page 55).

Therefore, I am concerned about the sovereignty of Scottish biometric data once ingested to DESC due to it being effectively 'offshored' in the U.S. Cloud, as this means that it cannot be fully administered from Scotland. For example, if U.S. federal authorities were to issue a warrant or subpoena together with a non-disclosure instruction to Axon and/or Microsoft for the surrender of Scottish biometric data under the provisions of the U.S. Cloud Act, then Police Scotland would presumably not even know that their data (the sensitive data of a person or persons) had been accessed and indeed acquired by a foreign state.

Therefore, if Police Scotland biometric data was to be accessed without the knowledge and/or authority of Police Scotland (even if lawful under U.S. law and the terms of the U.S. and UK agreement) then (regardless of what view the ICO might take on DPA 2018, if any) that data is almost certainly not properly protected from unauthorised disclosure in terms of the Scottish Code of Practice. I am sure that you will agree that no third-party should be able to access biometric data belonging to Police Scotland without the knowledge, agreement, or explicit consent of Police Scotland. This is a necessary safeguard to prevent biometric data belonging to Police Scotland being surrendered by a third-party contractor in response to the legal requirements and non-disclosure instructions of a foreign jurisdiction.

Data Security

I also have concerns (regardless of any decision by the ICO on adherence to UK data protection law, or no decision) about the security of highly sensitive Scottish biometric data being stored on the public Cloud infrastructure in circumstances where Police Scotland does not retain full control (or in this case any control) of the data encryption keys within DESC. This extremely sensitive biometric data may include images of victims of crime, for

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

example the injuries of a victim of rape or sexual assault, as well as images of persons who may have been charged but not yet convicted of any crime or offence.

DESC is being hosted by Axon on the Microsoft Azure platform, and as recently as 12 July 2023, Microsoft disclosed a major breach targeting its Azure platform, which it claims to have traced to a Chinese hacking group known as Storm-0588. The attack affected around twenty-five different organisations, including multiple U.S. government agencies, and resulted in the theft of sensitive emails from U.S. government officials.

It was reported in the media that Microsoft has demonstrated a "repeat pattern of negligent cybersecurity practices".

In October 2022, Microsoft had similar data security failings when the data of more than 548,000 users was exposed in the BlueBleed data leak. In March 2022, the Lapsus$ hacker group claimed to have breached Microsoft. In August 2021 misconfigured Microsoft Power Apps resulted in thirty-eight million company records being exposed. The issue was discovered by UpGuard, a cybersecurity firm. The misconfiguration was caused by third parties in the supply chain. In August 2021, security professionals at Wiz announced that they were able to access customer databases and accounts hosted on Microsoft Azure. In April 2021, 500 million LinkedIn Users' data was scraped from the Cloud and sold. In January 2021, Microsoft Exchange server vulnerability resulted in over 60,000 hacks. The Biden administration said that the attacks were traced back to Hafnium, a Chinese hacker group. In December 2019, over 250 million Microsoft customer records were exposed from an internal customer support database.

These examples demonstrate that there are major risks to be considered when storing 'any' sensitive data on the public Cloud infrastructure. Given ongoing global geopolitical tensions, it is safe to assume that any major 'U.S. Headquartered' technology provider or Cloud provider will continue to be regarded as a 'high value' target by hostile foreign states and hackers. This raises legitimate questions about the selection of a 'U.S. Headquartered' Cloud hosting solution to host/offshore sensitive Scottish law enforcement data, including Scottish biometric data. It is also worth placing on public record that when Scottish Government announced that it had awarded the DESC contract to Axon in October 2021, there had been no prior contact between Scottish Government officials and my office about the implications of potentially uploading Police Scotland, SPA, or PIRC biometric data to DESC.

I appreciate that Police Scotland (and other DESC partners) are the recipients of Scottish Government procurement decisions in this case, however I am sure that you will agree that the reputational damage to Police Scotland (and Scottish Government, and the Scottish Police Authority) would be substantial should sensitive biometric (and/or any criminal offence data) within DESC not to be properly protected from unauthorised access or unauthorised disclosure by contractors and sub-contractors in the supply chain.

More broadly, you will also be aware of recent cyber-attacks on UK policing involving Cloud and non-Cloud infrastructure where third-party contractor security vulnerabilities have damaged the reputation of policing. This has included Scotland-based IT support contractors

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

such as the Dacoll Group which provides support to the UK Police National Computer (PNC). In 2021, Dacoll were phished successfully by Russian hackers who were able to access 13 million UK police records.

In March 2023, the ACRO criminal records office was hacked leading to major disruption in England and Wales, and most recently a contractor to the Metropolitan Police was hacked resulting in officers' and workers' details being acquired.

I mention these cases to provide empirical evidence that 'outsourcing' data, and especially law enforcement data such as sensitive biometric data to external contractors is an exceptionally risky endeavour.

Reach of the Code of Practice

My final concern does not relate to Police Scotland, but it is worthy of mention for completeness. In both my annual report and accounts and my annual operational report to the Scottish Parliament covering the fiscal year 2022/23, I highlight that the functions of the Scottish Biometrics Commissioner, and therefore the reach and protections of the Code of Practice extends solely to Police Scotland, the SPA, and the PIRC.

Yet biometric data is shared extensively throughout the entire criminal justice ecosystem in Scotland, including in prisons, in criminal prosecutions, and in the multi-agency arrangements for the management of violent and sexual offenders, and now in DESC. Therefore, once biometric data is ingested to DESC by Police Scotland, the subsequent retention and use of that data within the wider DESC ecosystem by other parties (including contractors) does not fall within my authority or the protection of the Scottish Code of Practice. I have already highlighted in my annual reports to the Parliament that this is a significant risk which could undermine public confidence and trust in the criminal justice ecosystem in Scotland.

I hope that this information is of assistance to Police Scotland in terms of facilitating our forthcoming meeting and subsequently evaluating DESC at the conclusion of the current pilot phase. It may also be helpful to Police Scotland in terms of assessing next steps including responding in sufficient depth to the Code self-assessment questionnaire.

Due to wider public interest considerations, a copy of this letter will be published on my website at the right time in accordance with the terms of my Publication Scheme.

Yours sincerely

Brian Plastow

Dr Brian Plastow
Scottish Biometrics Commissioner