20 January 2022

Gary Pugh

Forensic Science Regulator
c/o Home Office Science
Long Corridor
14th Floor
Lunar House
40 Wellesley Road
Croydon
CR9 2BY
United Kingdom

Sent by email: FSREnquiries@homeoffice.gov.uk

Dear Mr Pugh,

RE: Use of forensics in the Home Office's asylum, immigration and nationality functions

Congratulations on your appointment to Forensic Science Regulator. This letter is sent by Privacy International together with Bail For Immigration Detainees, Open Rights Group, the3million, The William Gomes Podcast, CARAS (Community Action for Refugees and Asylum Seekers), RAMFEL (Refugee and Migrant Forum Essex and London) and Fair Trials International.

As you work towards the commencement of the Forensic Science Regulator Act 2021, we seek to draw your attention to issues concerning **the quality of digital evidence with relevance to Immigration Officers** and broader use by the Home Office.

Your role relates to the criminal justice system encompasses activities carried out by Immigration Officers. For example, the Memorandum of Understanding between Immigration Enforcement ("IE") and the Crown Prosecution Service[1], created considering Home Office policy on investigating immigration crime within the remit of Immigration

[1] https://www.cps.gov.uk/publication/memorandum-understanding-between-immigration-enforcement-ie-and-crown-prosecution

Enforcement, sets out the responsibilities of IE for the purpose of the MOU[2]. This includes the 'collection of admissible evidence' and 'the quality of IE investigations'.

We further note the Guidance on criminal powers for officers dealing with immigration enforcement matters within the UK[3]. The Guidance on 'Clandestine illegal entrants'[4] refers to:

- CCU (Command and Control Units in Home Office) seizing mobile phones and sim cards.

- CFI (Criminal and Financial Investigations Unit in Home Office) commissioning expert analysis of electronic devices

The Guidance on 'Search and Seizure[5]' refers to:

> Search and seizure of electronic media: Paragraphs 15A, 25A and 25B of schedule 2 to the Immigration Act 2016 provide that where there are reasonable grounds to believe that relevant documents are at the premises, electronic devices (such as mobile phones, laptops or tablet computers), that may contain such documents for which the search is being conducted, may be searched and seized in certain circumstances.

We are concerned that whilst considerable work has been done to draw attention to quality and standards issues in relation to digital evidence in the policing context, there is a lack of transparency and associated risk in relation to use by the Home Office across asylum, immigration, and nationality functions. We primarily focus on device extraction and GPS location tagging in immigration bail. We include several other issues of concern at the end of our letter.

Having worked at the Home Office Forensic Science Service and MPS, we anticipate you will be familiar with some of the issues which we believe are a pressing concern for your office.

We, as PI and signatories, would welcome a meeting with the Forensic Science Regulator to understand in greater detail your plans for 2022. We would be grateful for elaboration

---

[2] For example, IE is responsible for: The enforcement policy in respect of breaches of immigration controls including the disruption of organised crime groups; The adoption of cases for criminal investigation; The collection of admissible evidence and the recording, retention and revelation to the prosecutor of relevant unused material; The quality of IE investigations

[3] https://www.gov.uk/government/publications/powers-and-operational-procedure

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/618085/Clandestine_Entrants_v1.pdf

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578886/Search-and-seizure_v3.pdf

of the areas you believe do and do not fall within your remit in relation to Immigration Officers.

About PI

Privacy International (PI) campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Privacy International has conducted ground-breaking research into technologies deployed by the Home Office, including mobile phone extraction and been a key stakeholder in Home Office consultation regarding the development and deployment of the National Law Enforcement Database Programme. We believe that data-intensive migration-related mechanisms must be auditable, transparent, and non-discriminatory.

Relevance of your responsibilities as Forensic Science Regulator

We note the following responsibilities of your office:

- **establishing, and monitoring compliance** with, quality standards in the provision of forensic science services to the police service and the wider Criminal Justice System (CJS)
- ensuring, where applicable, the **accreditation** of those supplying forensic science services to the police, including in-house police services and forensic suppliers to the wider CJS
- **setting and monitoring compliance** with quality standards applying to national forensic science intelligence databases
- providing **advice to Ministers**, CJS organisations, suppliers and others as seems appropriate, on matters related **to quality standards in forensic science**
- **dealing with complaints from stakeholders and members of the public in relation to quality standards in the provision of forensic science services**.

We note that it is within your remit to deal with complaints from stakeholders and members of the public in relation to quality standards in the provision of forensic science services. We are not making an official complaint but do wish to raise concerns in relation to quality standards.

We note your role in monitoring compliance with quality standards, accreditation, and advice to Ministers on matters relating to quality standards. We consider that these responsibilities are highly relevant to the Home Office use of device extraction and other digital evidence.

We are aware that you conduct visits to sites where extraction is taking place (note visits in Newsletter No.36 July 2021) and suggest that reviewing the device extraction practices in the asylum, immigration, nationality context could be a consideration for your work.

Digital Device Extractions: Current lack of transparency and quality concerns

We are concerned that the current use of data extraction from digital devices by immigration officers may fall short of quality standards. There has been little scrutiny of the use of digital device extractions by immigration officers, yet they are conducting a large volume of extractions.

In response to a request under the Freedom of Information Act submitted by Privacy International in June 2021 (attached), the Home Office confirmed that in 2020 Immigration Officers had conducted 4,925 extractions and that Immigration Enforcement had 104 officers "trained" to use such technology.

According to the Home Office's Immigration Enforcement Digital Device Extraction Policy[6], published in July 2021, "[Criminal and Financial Investigation/Immigration Enforcement] do not have ISO 17025 accreditation and have not been accredited to the Forensics Regulators Codes of Conduct."

We note that there was no policy in place prior to this policy, despite extractions taking place. We note that a subsequent response to request under the Freedom of Information Act submitted by Privacy International in November 2021 (attached) revealed no record keeping in relation to phones seized and extracted in relation to lorry drops and detention centres, which may highlight issues of due process which include forensic science matters. The response further revealed there is no policy for reporting and treating errors in the conduct of digital forensics by Immigration Enforcement[7].

It is not just the actions of Immigration Officers that are relevant to device extraction. Police Officers are also involved in digital forensics related to migration. Thus, we note that as of 2021 only 15 out of 36 police forces have accreditation for mobile phones data extraction and 7 forces are yet to have accreditation for extraction from computers[8].

This is in the context of the Information Commissioner, Law Commission and the former Forensic Science Regulator raising quality concerns in relation to device extraction, particularly in the law enforcement context. The Information Commissioner's Office review

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/1000530/digital-device-extraction-policy-v1.0-ext.pdf

[7] The response states that a policy is due to be finalised and published in early 2022.
[8] https://committees.parliament.uk/publications/7366/documents/78131/default/

into the use of mobile phone extraction tools by police forces concluded that there are inconsistent approaches and standards of compliance by forces, increasing "the risk of arbitrary intrusion and impact standards of compliance when processing personal data extracted from mobile devices."[9]

You are no doubt familiar with the findings of the House of Commons Justice Committee Report 20 July 2018[10] and House of Lords Science and Technology investigation.

If device extractions are happening at scale in the immigration context, it is not unreasonable to assume there may be concerns, that have not come to light, particularly given the lack of scrutiny and transparency. We are unaware whether any referrals to yourself involve use of digital evidence by Immigration Officers.

We note in relation to potential quality issues that the minutes of the Digital Forensics Specialist Group highlights 'Error Investigation' and notes an increase in referrals to the Regulator concerning digital forensics[11].

1.1 There had been an increase of referrals to the Regulator concerning digital forensics. Due to the number of different referrals for digital forensics, it was decided more lessons learnt documents should be produced; five lessons learnt documents had been produced to date, and several were directly concerning digital forensics.

1.2 The types of issues raised to the Regulator concerning digital forensics, included inaccuracies, misinterpretation, evidence handling which included loss of data, overwriting of data, and sending data to the wrong individuals or organisations.

1.3 Issues had also been raised about the tools used when analysing digital forensics. An example was given where a software tool used had produced results that were later shown to be incorrect. Further investigation by the software provider revealed an error in the software that was subsequently fixed.

The Annual Report dated 13 January 2021[12] states that "Digital forensics has, in the last year, overtaken the number of referrals for biology and DNA."

---

[9] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

[10] https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881164/DFSG_2019_06_13_Minutes.pdf

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950087/FSR_Annual_Report_2019-2020_Issue_1.pdf

The minutes of the Forensic Science Advisory Council[13], February 2021 further stated that:

> "The risk to the quality of evidence and risks to justice from digital methods that were being widely deployed to police officers, such as radio frequency surveys, with little or no validation to ensure the methods were fit for purpose and a lack of understanding of the boundary between factual and opinion evidence."
>
> "The lack of capacity for toxicology and digital forensic cases … and there was a large backlog of digital devices awaiting analysis despite the fact that there were accredited suppliers that were not being fully used. Issues with capacity also made it difficult to implement quality systems, respond well to challenges to delivery of quality and increased the likelihood of quality issues occurring."

The use of mobile phone extraction by Immigration Officers has, prior to the FOIA response above and the information that has come to light during the passage of the Police, Crime, Sentencing and Courts Bill, operated under a veil of secrecy. In relation to what is in the public domain, we note:

1. David Anderson QC reports as Reviewer of Terrorism Legislation[14] in relation to the exercise of Schedule 7 Terrorism Act 2000 powers to search mobile phones at borders.

2. Independent Chief Inspector of Borders and Immigration report May 2019 – December 2019[15]

---

13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985298/FSAC_Minutes_Feb_2021_final.pdf

14 David Anderson QC (June 2012) The Terrorism Acts in 2011 [Online]. Available from: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228552/9780108511769.pdf*; David Anderson QC (July 2013) The Terrorism Acts in 2012 [Online]. Available from: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243472/9780108512629.pdf*; David Anderson QC (July 2014) The Terrorism Acts in 2013 [Online]. Available from: *https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2014/07/Independent-Review-of-Terrorism-Report-2014-print2.pdf*; David Anderson QC (December 2016) The Terrorism Acts in 2015 [Online]. Available from: *https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/12/TERRORISM-ACTS-REPORT-1-Dec-2016-1.pdf*; Jonathan Hall QC (March 2020) The Terrorism Acts in 2018 [Online]. Available from: *https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/03/Terrorism-Acts-in-2018-Report-1.pdf*.

15 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933953/An_inspection_of_the_Home_Office_s_response_to_in-country_clandestine_arrivals__lorry_drops__and_to_irregular_migrants_arriving_via_small_boats_.pdf

3. Home Office contracting information[16]

More recently, additional information has come to light including in November 2020 the Home Office responding to parliamentary questions[17] that their intention is to seize and search the mobile phones of all migrants, at least those who arrive at Tug Haven, Dover.

The Police, Crime, Sentencing and Courts Bill[18], which is currently at House of Lords Committee stage, includes the provision for an authorised person, which includes Immigration Officers, to extract data from electronic devices if the user of a device has voluntarily provided it and has agreed to the extraction of data from that device.

We believe that without quality standards supported by robust accreditation and adherence to the Codes of Conduct, there exists a grave potential for misuse of such techniques leading to severe implications for people subject to the use of such powers. This includes but is not limited to potential miscarriages of justice and inaccurate asylum determinations, thereby jeopardising people's right to claim asylum and their lives.

Other forensic services

[16] A contract dated **19 September 2014** between The Home Office and **Cellebrite UK Ltd** for 'RM3858 SB-1969 Provision of Mobile Forensic Equipment in Schedule Four Contract Pricing Matrix refers to new licences indicating that they had already purchased the hardware. The total cost is £39,250 for 1 year, £73,597 for 2 years and £81,017.50 for three years.

Schedule Two refers to requirement of "**Rugged Mobile Forensic Tactical Kits**" to examine phones at a scene to retrieve messages, images and contacts." It goes on to state "The requirement is for the supply of five (5) new UFED's in order to analyse material…The Authority requires five (5) new devices that can produce physical and logical extraction of data from mobile phones. The devices will be required to extract data from applications, SMS messages, e-mails, videos, call logs, audio and calendars." The Home Office requires a file extraction system, ability to extract deleted data, ability to bypass lock screens. https://data.gov.uk/data/contracts-finder-archive/download/1647795/7871b994-0147-4c80-a016-39ec012a989d and https://data.gov.uk/data/contracts-finder-archive/contract/1647795/

In **May 2018** the UK Home Office's Immigration Enforcement authority made a payment of £45,000 to Cellebrite.

In **2018,** the UK Border Force and Immigration Enforcement made payments of £133,000 to Cellebrite, while the Border Force, Immigration Enforcement, and UKVI paid £335,000 to Micro Systemation, a similar extraction company based in Sweden. In August 2018 the Home Office contracted with Cellebrite for "2x UFED Touch 2 ruggedised units and 1x UFED 4PC TK CF54 Ultimate System."
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741541/Home-Office-Spending-25000-May-2018-CSV.csv/preview
https://data.gov.uk/dataset/ecc70eba-dbf2-4bba-9f04-415cbe845118/spend-over-25-000-in-the-home-office
https://www.contractsfinder.service.gov.uk/notice/ff6229ae-f9d8-415c-8bb5-2cb2429f881a?.

Chorus is a data analytics software programme. It appears to have been awarded a £19.5K contract by the **Home Office from 5 November 2020 until November 2021.**
https://www.contractsfinder.service.gov.uk/Notice/85c416a4-bc26-4a65-9474-ed40edc04e86

[17] https://questions-statements.parliament.uk/written-questions/detail/2020-11-11/114198
[18] https://privacyinternational.org/news-analysis/4586/policing-bill-unsatisfactory-debut-statute-books-mobile-phone-extraction

We are also concerned that immigration officers may be conducting other forensic services without adherence to quality standards.

Electronic Monitoring in immigration bail and immigration cases: The government introduced mandatory electronic monitoring using GPS tags, on 21 August 2021 through a commencement order laid by the government three weeks previously, which introduced the remaining parts of paragraph 2, schedule 10 of the Immigration Act 2016.

This means that every individual categorised as a 'Foreign National Offender' and facing deportation, must be made subject to electronic monitoring, unless the Secretary of State (and not the Tribunal granting bail) considers that it would be impractical or contrary to their Convention rights. At present the Home Office are tagging people who are released from detention, however from January 2022 there are plans to tag people who are living in the community.

We are concerned that there has been insufficient consideration of the quality of evidence provided by GPS location tagging, related to GPS limitations[19]. We are not aware what safeguards are in place and relevant guidance/policies that relate to quality concerns.

This is particularly pertinent given the proposed use of location data for Article 8 human rights claims and the potential for the Home Office to enrich location data with other data, or to use location data for other purposes.

We are concerned that this data may be relied upon by the Home Office when refusing claimants permission to remain on human rights grounds, with the absence of policy regarding the identification of data and its disclosure compounding concerns.

The Home Office guidance on Immigration Bail states:

> "trail data will be held by the EM contractor but may be accessed by the Home Office …where it may be relevant to a claim by the individual under Article 8 ECHR … to be shared with law enforcement agencies where they make a legitimate and specific request for access to that data."

We note the potential, as set out by Essex Police[20], to use location data in investigations whereby Police ask Capita for tags in a particular area during a timeframe; to view and overlay data; to conduct live surveillance; to conduct analytical work which could show tagged people associating together or hotspot areas frequented by tagged people.

[19] https://privacyinternational.org/explainer/3753/gps-tracking-and-covid-19-tech-primer
[20] https://www.essex.police.uk/foi-ai/essex-police/our-policies-and-procedures/e/e0108-procedure---electronic-monitoring/

Fingerprint comparison: It is unclear to what standards fingerprint comparison by immigration authorities is currently being conducted. This includes the collection of records by UK authorities themselves, for example in the Channel, but also concerns the collection of records by foreign government agencies which are used by UK authorities. For example, under the Five Country Conference (FCC) Data-Sharing Protocol agreed in 2009 between the UK, Australia, Canada, New Zealand and United States, arrangements are in place to share the fingerprints of up to 3,000 individuals between each participating country per year. Such information may adversely affect a person's asylum claim and be interpreted as evidence of criminality.[21]

Cell-Site Analysis & Communications Data: Immigration Enforcement has access to communications data: in 2019 it received 7146 line items from targeted communications data authorisations.[22] It is unknown whether this data was obtained from telecommunications operators or whether it was acquired directly by relevant Home Office bodies, whether cell site analysis has been conducted, or whether private third party providers of communications analysis have been used.

Internet intelligence and investigation: There is little information publicly available which outlines under what circumstances, powers, and how immigration officers conduct investigations online, including the use of Open-Source intelligence gathering. We may presume however that techniques which fall within the definition established within the Codes of Practice and Conduct are being used: in 2019/20 Immigration Enforcement International, a unit which provides capacity-building to foreign border control and immigration enforcement units, stated that it has provided training "in specialist areas such as Open Source, Arrest Training and Investigation skills" to some 7000 people in 39 countries.[23]

SOCMINT/OSINT: There is a lack of public information about the use of SOCMINT/OSINT by the Home Office. We note our investigation into use by local authorities[24]. The wealth of information hosted on social media platforms can range from names and photos to political and religious views; and the physical and mental health of users and their families or friends. Such investigation can take various forms and usually involves the manual or automatic review of content posted in public or private groups or pages; review of results of searches and queries of users; review of activities or types of content users post; or *"scraping"* (extracting data, including the content of a web page, and replicating it in a form the investigator can use). The details lifted from social media can then be integrated with the analysis of data from an extracted phone. The

[21] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf
[22] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf
[23] https://devflow.northeurope.cloudapp.azure.com/files/documents/IEI-Concept-note---final-update-20200611070638.docx
[24] https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target

Forensic Science regulator has previously noted issues to be explored regarding open-source intelligence practices[25], also known as internet intelligence and online investigations.

Aerial surveillance: As explored by Privacy International[26], there has been an increasing level of aerial surveillance which enable monitoring of migrants as they cross the Channel.[27]

Other forensic services: Immigration and other government authorities may be conducting other forensic services which require adherence to quality standards. For example, language analysis services[28] which seek to establish a person's place of origin and x-ray and dental assessments[29] which seek to verify a person's age have been performed by immigration authorities and local authorities, including using private third-party providers.

Request

We would welcome a discussion with you about the matters we have raised in our correspondence.

We urge therefore that within your remit to promote forensic quality standards across the wider criminal justice system that you:

- Conduct a review into the conduct of digital forensic activities by immigration officers and across the Home Office's immigration, asylum and nationality functions.

- Confirm which services require adherence to the Codes of Practice and Conduct and other standards.

- Confirm whether the use by relevant authorities themselves or third-party providers currently meets these standards.

---

25 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881164/DFSG_2019_06_13_Minutes.pdf & https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877607/20200225_FSR_Annual_Report_2019_Final.pdf

26 https://privacyinternational.org/explainer/4595/satellite-and-aerial-surveillance-migration-tech-primer

27 Meaker, M. (10 January 2020) Here's proof the UK is using drones to patrol the English Channel (Wired) [Online]. Available from: *https://www.wired.co.uk/article/uk-drones-migrants-english-channel*; BBC News (5 December 2019) Drones monitor south coast of England for migrant boats [Online] Available from: *https://www.bbc.co.uk/news/uk-england-kent-50673241; {*UAS Systems, Tekever AR5 [Online]. Available from: *http://uas.tekever.com/ar5/*

28 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685203/Language-analysis-AI-v21.0EXT.pdf

29 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947800/assessing-age-asylum-instruction-v4.0ext.pdf

- Confirm whether the Regulator will seek to ensure that any such use of forensic services and/or digital forensic activities across the Home Office's immigration, asylum, and nationality functions does meet relevant quality standards and if so by when.

- Confirm whether you will issue any compliance notices to relevant bodies to cease operations if they fail to have the necessary accreditation in place.

- Providing advice to Ministers, CJS organisations, suppliers and others as seems appropriate, on matters related to quality standards in forensic science related to use by the Home Office in immigration, asylum and nationality functions.

We look forward to a response and stand ready to answer any questions you may have.

Yours sincerely,

Privacy International, Camilla Graham Wood, Senior Legal Officer

Open Rights Group, Sahdya Darr, Immigration Policy Manager

Bail For Immigration Detainees, Pierre Makhlouf, Legal Director

the3Million, Nicolas Hatton, CEO

CARAS, Eleanor Brown, Managing Director

RAMFEL, Nick Beales, Lead Immigration Adviser

The William Gomes Podcast, William Gomes, Director

Fair Trials International, Griff Ferris, Legal and Policy Officer