Statement on behalf of: Privacy International
Witness: Camilla Graham Wood (CGW)
Statement: First
Exhibit: CGW1
Date: 1 November 2021

IN THE HIGH COURT OF JUSTICE **CO/4793/2020**
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

B E T W E E N:

THE QUEEN
(on the application of HM)

Claimant

- and -

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

- and-

PRIVACY INTERNATIONAL

Proposed Intervener

FIRST WITNESS STATEMENT OF CAMILLA GRAHAM WOOD

(PRIVACY INTERNATIONAL)

I, Camilla Graham Wood, Solicitor of Privacy International, 62 Britton Street, London EC1M 5UY SAY AS FOLLOWS:

A. INTRODUCTION

1. I make this statement in support of Privacy International's proposed intervention and to assist the Court by providing factual information and context about the mobile phone extraction (**"MPE"**) technology relevant to this claim.

2. I am a solicitor and senior legal officer at Privacy International (**"PI"**). I was admitted as a solicitor on 3 October 2011. I have a First-Class Honours degree in Computer Science. I have been employed at PI since 2015 and I am currently Programme Lead for our migration project. I am responsible for

our work on MPE and led our investigations which resulted in the Information Commissioner's 2020 Report into the use of mobile phone extraction by police forces in the UK.

3. I am authorised to make this statement on behalf of PI. Where I rely on sources other than my own knowledge, I identify them below.

4. Where the facts and matters to which I refer in this statement are within my own knowledge, I confirm that they are true. Where they are based on information obtained from other sources (which sources I shall endeavour to identify), I confirm that they are true to the best of my knowledge and belief. This statement has been prepared following discussions taking place over phone and video conferencing and also through correspondence with PI's external solicitors and counsel. No privilege is waived over those discussions and correspondence.

5. In this statement, I refer to a bundle of copy documents, which is now produced and shown to me marked "**CGW1**". Where the documents I refer to are particularly lengthy and/or technical in nature, I have exhibited only the relevant extracts. Tab and page references in this statement are references to either:

    5.1. the page numbers in the bottom right of the documents in the bundle "**CGW1**"; or

    5.2. the page numbers indicated in the Claimant's re-amended permission bundle.

6. This statement addresses the following topics:

    6.1. Section B provides evidence in support of PI's application to intervene;

    6.2. Section C explains how data is extracted from mobile phones by MPE, and the different methods of MPE which exist;

    6.3. Section D explains how that data is analysed to provide information to officials, and sets out what scale and kinds of private information might be recovered through MPE;

6.4. Section E explains how MPE can allow private data not on the phone to be accessed through "*Cloud extraction*"; and

6.5. Section F analyses the privacy consequences of MPE and the reliability of data obtained using this method.

B. PRIVACY INTERNATIONAL'S APPLICATION TO INTERVENE

7. PI is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and the United Nations.

8. PI has been researching MPE since 2017. It has been involved in investigating the use of these tools by law enforcement and making submissions to regulatory and oversight bodies including the Information Commissioner's Office (the "**ICO**"), the Law Commission and the Investigatory Powers Commissioner's Office:

8.1. PI published its "*Digital Stop and Search Report*"[1] in March 2018 and, in April 2018, made a complaint to the ICO in relation to the use of MPE technology by police forces.[2]

[1] Privacy International (March 2018) Digital Stop and Search: How the UK Police can Secretly Download Everything from Your Mobile Phone [Online]. Available from: *https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.*
[2] Privacy International (26 April 2018) Complaint to the ICO [Online]. Available from: *https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf* **[CGW1/28/248]**; See also the ICO Report, *Mobile Phone Data Extraction by Police Forces in England and Wales* (June 2020) at DM/16 **[CB/2/G/596].**

8.2. PI has been involved in extensive engagement with Police Scotland regarding the legality of the rollout of MPE kiosks[3] as a member of the Cyber Kiosk Stakeholder and External Reference Group.

8.3. PI has been asked to speak about MPE at multiple events including at the National Police Chiefs' Council ("**NPCC**") Information Practitioner Professional Development & Training Event on 17 June 2019 and at a City Forum event on 24 October 2019 on Transforming Forensics with the Home Office, private sector, and others.[4]

8.4. PI has worked with academics on the topic of MPE, including the UCL-JDI Department of Security and Crime Science.

8.5. In July 2019, Bedfordshire Police sought to engage with PI on their project considering cloud data and law enforcement.

8.6. PI is a member of the Home Office Open Space initiative, a group of civil society organisations and other stakeholders who meet with the Home Office, the College of Policing, and other relevant bodies to discuss ongoing issues in relation to MPE technology.

9. PI has specific expertise in the context of privacy rights in migrant communities:

9.1. In July 2019, PI joined migrant organisations in a formal complaint filed by the Platform for International Cooperation on Undocumented Migrants against the UK for breaching the General Data Protection Regulation by including the *"immigration control"* exemption in the Data Protection Act 2018.

9.2. In November 2020, PI obtained documents from EU agencies evidencing the outsourcing of border surveillance and controls by the

[3] For example, Privacy International (12 September 2019) Old Law, New Tech and Continued Opacity: Police Scotland's use of Mobile Phone Extraction [Online]. Available from: *https://privacyinternational.org/report/3202/old-law-new-tech-and-continue-opacity-police-scotlands-use-mobile-phone-extraction*. See also Privacy International (10 March 2020) Submission to Police Scotland on Cyber Kiosks [Online]. Available from: *https://privacyinternational.org/node/3394.*

[4] City forum, Towards a future vision for Digital Forensics event page [Online]. Available from: *https://www.cityforum.co.uk/event/forensics-round-table/.*

EU to neighbouring countries,[5] and wrote to the European Commission calling for stricter safeguards and oversight of aid funds.[6]

9.3. In February 2021, PI published a report on the UK's migration surveillance regime.[7] This report resulted from extensive research and investigations into the use of surveillance systems and tools (including MPE) by HM Government to police the UK's borders, using procurement, contractual and other open-source data.

9.4. PI also regularly publishes various analyses of threats to the privacy of migrant communities[8] or primers on technologies used for migration surveillance[9].

10. PI is a responsible and experienced party to litigation. It has acted as claimant or intervener in many cases involving the right to privacy in the courts of the United Kingdom (especially in the Investigatory Powers Tribunal and on appeal, reference or application or reference to the Supreme Court, CJEU and European Court of Human Rights[10]), Colombia, Kenya, France, Germany,

---

[5] Privacy International (November 2020) Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls [Online]. Available from: *https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border* **[CGW1/8/45]**.

[6] Privacy International (November 2020) Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes [Online]. Available from: *https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes* **[CGW1/9/55]**.

[7] Privacy International (February 2021) The UK's Privatised Migration Surveillance Regime: A Rough Guide for Civil Society [Online]. Available from: *https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf* **[CGW1/5/30]**.

[8] Privacy International (8 July 2020) 10 threats to migrants and refugees [Online]. Available from: *https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees.*

[9] Privacy International (21 July 2021) Satellite and aerial surveillance for migration: a tech primer [Online]. Available from: *https://privacyinternational.org/explainer/4595/satellite-and-aerial-surveillance-migration-tech-primer.*

[10] PI has been a party to most of the substantial Investigatory Powers Tribunal cases in the last decade, including, for example: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2016] UKIPTrib 15/110/CH; *Privacy International & GreenNet Limited & Ors v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2016] UKIPTrib 14/85/CH & 14/120-126/CH; *Liberty (The National Council of Civil Liberties) & Ors v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2015] UKIPTrib 13/77/H, *Privacy International v Secretary of State for the Foreign and Commonwealth Office & Ors* [2014] UKIPTrib 13/77/H. Subsequently, many of those cases have been heard in the higher courts. See, for example, *R (Privacy International) v IPT* [2019] 2 WLR 1219, *Privacy International v SSFCA* [2021] 2 WLR 1333.

South Korea, the United States, and the European Union, as well as the European Court of Human Rights[11].

11. If granted permission to intervene, PI would seek to assist the Court by adducing this statement as evidence. If the Court would be assisted, PI also proposes to make brief written and (if appropriate) oral submissions.

C. EXTRACTION OF DATA FROM MOBILE PHONES

12. Mobile device forensics involves a two-part process: data extraction followed by data analysis. The level of information which can be acquired depends both on what data can be extracted, *and* how effectively that data is analysed and integrated with information already known. Most digital forensics companies offer both extraction and analytics software. MPE has rapidly expanded in recent years as a tool used by law enforcement to obtain intelligence and evidence.[12]

13. This section deals with the extraction of data. The next deals with how the data extracted is analysed, the uses to which it can be put, and the capabilities it grants.

(1) The Process of Data Extraction

14. In general, data is extracted from a phone by physically connecting it by cable to a computer, laptop or touch screen device with specific software that enables extraction, for which the police or other authorities buy licences.[13] Various types of MPE software are referred to within the vendor training manuals and Standard Operating Procedure ("**SOP**") guidance notes included in the Defendant's disclosure, including: XRY viewer[14], UFED

[11] In particular, PI intervened in: Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson* [2017] QC 771 (leading case on the use of communications data in the Grand Chamber of the CJEU on a reference from the UK), *S and Marper v UK* (2009) 48 EHRR 50 (ECHR Grand Chamber decision on lawfulness of blanket retention of DNA samples), *Catt v UK* (2019) ECHR 76 (on the retention by the police of peaceful protest data in an "*extremism database*") and Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* [2021] 1 CMLR 31 (national security data retention and analysis, CJEU Grand Chamber) and *Big Brother Watch v UK* [2021 ECHR 429 (Grand Chamber, ECtHR).

[12] DM/8 "Level 1 Data Extraction (Information or evidential)" **[CB/2/G/401].**

[13] Purchase of Licence by MPS for Cellebrite Premium, available here: https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/mopac-decisions-0/licences-and-ongoing-support-cellebrite-premium-tool **[CGW1/12/93]**.

[14] DM/2 **[CB/2/G/292].**

Touch Unit[15], Cellebrite Software version 6.2.1.17[16], UFED Analyzer Version 6.2.6.2[17], XRY Software version 7.1 (provided by MSAB)[18], Panasonic Laptop[19], Field Kit. MSAB software is mentioned in the Data Protection Impact Assessment ("**DPIA**") provided in respect of the Kiosk System.[20] I explain how these types of software operate in further detail below.

15. Once the phone is plugged in to the device, the data extraction software can identify the phone[21] and prompt the individual to choose the kind of extraction to be performed (and sometimes the categories of data to be extracted: I discuss this type of "*selective extraction*" below). The device will then perform the requested extraction and collate the data contained on the phone. This is how almost all basic MPE is conducted. It requires only a piece of hardware (be it a 'cyber kiosk' (i.e. a desktop computer) or laptop/tablet) and specialist software. However, MPE is sometimes conducted offsite in laboratories or on the premises of private MPE providers. The NPCC identifies typically three levels of digital forensic services,[22] (although this classification is not rigid, and is most useful as a heuristic):

    15.1. **Level 1:** Undertaken by frontline staff or non-data forensics practitioners, frequently involving the use of 'self-service' kiosks. The operator is usually not a digital forensic practitioner, but should be trained to follow a preconfigured workflow on the forensic equipment.[23]

    15.2. **Level 2:** Undertaken by digital forensics practitioners, predominantly in digital forensic hubs or laboratories or by forensic

[15] DM/5A **[CB/2/G/299]**.
[16] Ibid; DM/5B **[CB/2/G/306].**
[17] Ibid.
[18] DM/5C **[CB/2/G/312]** and DM/5F **[CB/2/G/331].**
[19] Ibid.
[20] NJ/005 **[CB/2/G/997].**
[21] See DM/5D, the Standard Operating Procedure which describes a manual search to identify handsets using the XRY device manual **[CB/2/G/322].**
[22] NPCC, Digital Forensic Science Strategy (July 2020) [Online]. Available from: https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf **[CGW1/13/105]**.
[23] See the "Process Steps" sections of the SOPs contained in DM/5A **[CB/2/G/300]** and DM/5J **[CB/2/G/361]**; see also DM /9: "*The downloading officer will conduct the download following the workflow on the Kiosk.*" **[CB/2/G/411].**

service providers. It involves more skilled digital forensics work, including some kinds of logical extraction, file system extraction and physical extraction (each of which I describe under "*Methods of Data Extraction*" below). In addition, there are some more "*destructive*"[24] methods of MPE which involve specialist skill and require disassembly of the phone in laboratory conditions.

15.3. **Level 3:** Undertaken by digital forensic specialists, predominantly in Central Digital Forensics Laboratories or by Forensic Service Providers. The disclosure refers to procedures used by the Defendant for requesting forensic work other than by kiosk i.e., using external services for complex work.[25] There are several reasons for using external services, including, as referenced in the witness statements of David Magrath and Nicholas Jupp, for extraction requiring specialist skills or more advanced techniques.[26] For instance, there are some forms of MPE which involve software, exploits or techniques which are so valuable or sensitive that the provider does not release the software or equipment to law enforcement, but rather requires phones to be sent to the provider's own facility for extraction.[27] External providers may also be used where demand exceeds in-house capacity.[28]

---

[24] Destructive methods refer to when a device is physically broken and cannot be restored back to normal working condition. Destructive or invasive methods are used when the device is non-functioning because of severe physical damage. These methods are time-consuming and complex.
[25] The First Witness Statement of David Magrath explains that the document which was used to request external services was entitled "IE22", at DM/6, 'Authorisation for work by a forensic service provider' **[CB/2/G/367].** See also section 4 of the process document at DM/9 which details the approval process for requesting forensic work 'other than Kiosk' **[CB/2/G/417].**
[26] The Data Protection Policy dated 18 August 2020 at NJ/001 states, "*Some data relating to some **specialist capabilities** in connection with covert, digital, forensic enquiries or analysis and financial processes [redacted] will be processed on separate systems. Data will also be processed under contract by external forensic providers and within the [redacted] prior to transfer to the CPS.*" (emphasis added) **[CB/2/G/923];** the First Witness Statement of David Magrath states that "*[digital forensics] began as a mix of in-house technology… and the utilisation of external forensic service providers **for anything needing more advanced extraction techniques**.*" (emphasis added) **[CB/2/G/279].**
[27] Cellebrite, Cellebrite Advanced Services [Online]. Available from: *https://www.cellebrite.com/en/advanced-services* **[CGW1/29/275]**.
[28] See for example the National Police Chief's Council and Association of Police and Crime Commissioners joint Forensics Review report, April 2019 available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/911660/Joint_review_of_forensics_and_implementation_plan__accessible_.pdf.

16. During the extraction, an individual may have to interact with the phone, as directed, to place it in a particular mode or state to enable extraction. For example, the SOPs for Logical Extraction of Apple iPhone and iPhone SE Handsets direct that "*[t]he exhibiting officer must ensure that the handsets entering the downloading process are switched off*", or that the exhibiting officer should "*take out SIM card. Activate the handset, unlock the main screen if requested, the handset will confirm that no SIM is present. Access settings confirming 'airplane mode' is switched on and Wi-Fi and Bluetooth are turned off.*"[29]

(2) <u>Bypassing of Security Measures</u>

17. Smartphones are protected by a complex suite of security measures, including security chips, encryption, PIN-protection and facial or fingerprint recognition. Manufacturers seek to make their phones as secure as possible. This can present an impediment to data extraction.

18. Whether a phone is password protected or not is a key determinant as to how quick and simple extraction is, particularly for newer phones. Whilst it is possible to attempt brute force extraction (which the Defendant appears to have used)[30] (i.e., trying as many passwords as possible), there are problems with doing so. Many phones use tamper-resistant security chips that only allow a small number of password attempts before locking and eventually deleting the data on the phone. Some companies offer products which they claim can brute force passwords[31] and get around aspects of the phone designed to protect from brute force attacks, although this is time-intensive, and success is not guaranteed. GrayKey is one such product, and it is

[29] See the vendor training and SOPs at DM/5B **[CB/2/G/307]** and paragraphs 2.4 and 6 of DM/5C **[CB/2/G/313].**

[30] The Investigation Record at SMB/05 states "*IE22 submitted to Sheffield Digital Forensics lab to continue the Brute Force process for JF/01 (device seized from [REDACTED]) by HMRC as part of Op Chariot)*" **[CB/2/G/829].**

[31] AppleInsider, iPhone hacking tool GrayKey techniques outlined in leaked instructions (June 2021) [Online]. Available at: *https://appleinsider.com/articles/21/06/22/iphone-hacking-tool-graykey-techniques-outlined-in-leaked-instructions* **[CGW1/1/5]**.

supported by some extraction software, including MSAB XRY,[32] which the disclosure reveals the Defendant uses.[33]

19. Accordingly, an authority seeking to carry out MPE will always try and obtain the phone's password to gain easy access to the phone. This may be achieved by asking the user to volunteer the password,[34] surveillance, or by imposing a legal obligation to disclose the password. With the password, it is generally, but not always, relatively straightforward to download much of the data on a phone.

20. Nevertheless, it is possible in some circumstances for data extraction software to bypass a phone's security features by taking advantage of security flaws or built-in diagnostic or development tools. Whether it is possible to bypass security features or not will depend on a number of variables, primarily the make, model and operating system of the phone:

    20.1. **The phone's hardware/type of phone.** For example, some devices with a Qualcomm chipset (typically phones that use the Android operating system, such as those made by Samsung and Google) can be placed in "*Emergency Download Mode*" ("**EDL**"), to enable extraction. This is a mode designed to allow manufacturers to run diagnostics and repair without the need for the device's password. The method to switch a phone into EDL is different for each phone but usually involves pressing a combination of keys.

    20.2. **Date of most recent update.** Smartphone operating systems need to be updated regularly to patch vulnerabilities and exploits. The further back in time the phone was most recently updated, the greater the risk of an unpatched vulnerability in the software, which the data extraction devices can exploit.

[32] MSAB, XRY 7.7.1, Kiosk and Tablet 7.7.1 release notes [Online]. Available from: *https://www.msab.com/2018/05/03/released-today-xry-kiosk-tablet-7-7-1*; **[CGW1/27/246]**

[33] In relation to the Defendant's use of this software, see the vendor training and SOPs at DM/5C **[CB/2/G/312]** and DM/5F **[CB/2/G/331]**.

[34] See DM/11, "*Any officers in possession of a device containing PEI which they are unable to gain access toshould request the key from the subject.*" **[CB/2/G/445].**

20.3. The **type of operating system.** The type of operating system affects the likelihood of the system being up-to-date in the sense described above. For example, modern Apple (iOS) devices are more likely to have the latest updates installed, because, unlike Android manufacturers, Apple both manufactures its devices *and* develops the Operating System, allowing the company to exercise very tight control over its security. This means Apple devices remain up-to-date for longer and receive security updates as soon as they are available. Without the password, it is difficult to extract anything from a modern iOS device.

20.4. **Whether the smartphone has been handled by the individual seeking to extract the data in such a way as would trigger additional security measures.** The policy decisions included in the Defendant's disclosure refer to the bagging of seized phones[35] and the Good Practice Guide for Digital Evidence included in the Defendant's disclosure refers to placing handsets in a Faraday environment[36] to prevent signal reception.[37]

20.5. **Extraction software version**. The success of an extraction and the ability to bypass security measures will also depend on the version of the extraction software used.

21. There is something of an 'arms race' between providers of data extraction tools and phone operating system designers to, respectively, overcome and strengthen the security measures on smartphones. Each new operating system update on an electronic device may require a revision of the software on data extraction devices to defeat its security. Whether a particular vulnerability can be exploited depends on the capabilities of the data extraction tools, as much as it does on the security measures on the phone.

[35] See, for example, the Decision of Jeremy Clark of on 22 July 2020 in DM/18 **[CB/2/G/661]** and the SIO Decision at DM/20 **[CB/2/G/667].**
[36] See The Association of Chief Police Officers' ("**ACPO**") Good Practice Guide for Digital Evidence at DM/13 **[CB/2/G/582].**
[37] See the Review of MPE included at DM/40 **[CB/2/G/1279].**

22. The Defendant's disclosure indicates that the kiosks it uses cannot conduct extractions without the device's password:[38]

22.1. The older vendor training manuals from 2016 disclosed by the Defendant (which pre-date the SOPs issued following the creation of a digital forensics lab within the Criminal and Financial Investigation ("**CFI**") department in 2019) state that the *"handset will have to be unlocked using the PIN number"*.[39] This would need to be obtained from the individual either voluntarily or pursuant to s. 49 RIPA 2000. The reliance on consent by extracting authorities has been subject to criticism by PI, given the asymmetry of power between the individual and the requesting officer.[40]

22.2. The 2019 Kiosk SOP included in the Defendant's disclosure (issued following the installation of the internal digital forensics laboratory) states that the kiosk operator will "*carry out research to determine if an extraction is possible on the Kiosk*".[41] It is unclear whether this research includes checking if a passcode can be bypassed, depending on the make and model of the device.

23. If the device cannot be unlocked, the SOPs disclosed by the Defendant indicate that extraction can be escalated to the "*Digital Forensics Hub*".[42]

(3) <u>Methods of Data Extraction</u>

24. There are several different methods of MPE, each of which, depending on the phone and operating system,[43] uses different techniques and exploits[44] to

[38] See, for example, paragraph 2.5.3 of the Kiosk SOP at DM/7, which suggests advising the investigating officer to escalate the device to the "*Digital Forensics Hub*" if the device is locked **[CB/2/G/ 382].**
[39] See, for example, SOP for SIM card extraction, DM/5J, paragraphs 6.21-22 **[CB/2/G/362].**
[40] Privacy International's Submission to the Joint Committee on Human Rights in respect of the Draft Police, Crime, Sentencing and Courts Bill 2021 (May 2021) [Online], paragraphs 21-33, available at: *https://privacyinternational.org/sites/default/files/2021-06/PI%20Submission%20to%20JCHR%20re%20PCSC%20Bill_Final_0.pdf* **[CGW1/3/16-17]**.
[41] See DM/7, Kiosk SOP, at paragraph 2.2 **[CB/2/G/381].**
[42] Ibid; see also DM/11, Investigation of a protected electronic information policy **[CB/2/G/445].**
[43] See DM/5B, Cellebrite SOP for Logical Extraction of Apple iPhone Handset, at paragraph 6.11: "The available types of extracted data may vary depending on the source device, manufacturer and model." **[CB/2/G/308].**
[44] See DM/11 "The Digital Forensic Lab Manager will provide in writing … the dates of the period of attempts to access the information and details of exploits carried out." **[CB/2/G/446].**

extract different levels of personal data from mobile phones. The methods vary in their technicality,[45] in the type and volume of data they can extract, and in their ability to overcome the security features I described above. Data extraction tools are continuously being developed and refined, and different providers and agencies describe different processes in different ways, so the taxonomy I set out here is only an indication of what is possible.

25. It should be made clear that no one technology can access and extract all data from all phones. MPE is not either "*successful*" or "*unsuccessful*": different techniques can access different kinds of information and overcome different security features. Indeed, the NPCC warns that terms such as "*full*" extractions should be avoided, as they can easily lead to assumptions and misinterpretation of the actual method(s) of examination.[46] This is reflected (to an extent) in the Defendant's disclosure, which refers to four possible outcomes from a request for a kiosk extraction:[47]

    25.1. **Full extraction**, where the software extracts everything that is available, which allows the investigating officer to conduct a full review. As set out above, this is not ideal terminology.

    25.2. **Partial extraction**, where the software cannot extract everything that is available. The investigating officer should conduct an initial review of the material to establish whether there is enough information to assist in the investigation. If the investigating officer is not content, escalation to the Digital Forensic Hub is possible.

    25.3. **Failed extraction**, where the kiosk fails to extract any data. Escalation to the Digital Forensic Hub is possible.

    25.4. **No attempt made**, where the kiosk operator has identified that the data cannot be extracted on the kiosk. This could be due to the device

[45] See NJ/001, Data Protection Policy: CFI, Immigration Enforcement, 18 August 2020: "*MPE is currently undertaken by suitably trained officers using the Kiosk system where there is a clear investigative need to access data quickly or by the specialist digital capabilities team which is able to undertake a more in-depth examination*." **[CB/2/G/926].**

[46] CPS on Disclosure – A Guide to "Reasonable Lines of Enquiry" and Communications Evidence (24 July 2018), at paragraph 7 [Online]. Available from: *https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence* **[CGW1/24/220]**.

[47] See 'Guidance for completion of a kiosk extraction' at DM/7 **[CB/2/G/383-384];** and 'Procedure for requesting forensic work via Kiosk' at DM/9 **[CB/2/G/411-412].**

not being supported, the device being PIN-locked or the device being damaged in such a way that repair would be needed.[48] Discussions with the Digital Forensic Hub will be required to decide next steps.

(a) Manual Extraction

26. Manual extraction is the *"simplest"* way in which information can be retrieved from a phone. It involves viewing data on the unlocked device and documenting the information found through screenshots or photographs of the phone's screen. The information can then be photographed or otherwise recorded to document it. Manual extraction has many limitations. If the device is locked by password or PIN, manual extraction will not be so easy. It cannot extract many artifacts, metadata, log files and deleted data. It may also change the device's state (e.g., the status of unread messages may change to "*read*").

(b) Logical Extraction

27. Logical extraction is the quickest[49] but most limited (in terms of the volume of data extracted) form of MPE by comparison to other methods. It is *"Level 1"* extraction.[50] The phone is connected to the forensic hardware using a particular cable,[51] and the proprietary forensic software then communicates with the phone's operating system, sending a command to the device to deliver data to the forensic hardware, or alternatively installing an agent programme[52] on the device to extract data.[53] The vendor training manuals provided in the Defendant's disclosure indicate the generic steps to be taken in the process of logical extraction.[54] Logical extraction will generally take

[48] See, for example, **DM/8 [CB/2/G/402].**
[49] SMB/07 suggests a total processing time of 41 minutes, 16 seconds to get a significant amount of data. **[CB/2/G/905].**
[50] ICO Report (June 2020) **[CB/2/G/632];** see also CPS, Disclosure – A Guide to "Reasonable Lines of Enquiry" and Communications Evidence **[CGW1/24/221]**.
[51] DM/5C, at paragraph 6.4"*If the service cable is unavailable or cannot be sourced, reseal handset in a new evidence bag and return to transit store and advise OIC of inability to download the handset via logical extraction*." **[CB/2/G/314].**
[52] Exhibit DM/5F 6.19: "'select 'Agent' for the second extraction." An agent programme is a very small application that is temporarily installed. It is read-only meaning that it cannot write to the phone, alter the data, or overwrite any data. It acts like a third-party application and provides enough access to the device's file system to allow forensics software to extract data. **[CB/2/G/334].**
[53] See DM/5C **[CB/2/G/314]** and SMB/07/2021 **[CB/2/G/895]:** "Android Extraction Options: If device IS NOT rooted – file system, back up, agent…" "Installing Agent Version 4", "Executing Agent."
[54] DM/5A-C **[CB/2/G/299-319].**

place using hardware and software on site, unless the exploits involved are so sensitive that a provider requires it to take place at the provider's premises.

28. Logical extraction often works by exploiting the mechanism by which commercial third-party apps communicate with the device's operating system. Experience is required for handling the extraction as it may, for example, involve putting the device into certain states or pushing various specific combinations of keys.[55]

29. An example of this is to enable *"USB debugging"*. USB debugging relates to Android phones. The disclosure reveals that it is used by the Defendant, and the process for doing so is referred to in DM5F *"Logical Extraction of Android Motorola G4 handset"*. USB debugging mode is a developer mode in Android phones that allows newly programmed apps to be copied via USB to the device for testing. It allows an Android device to receive commands, files and the like from a computer and allows the computer to pull crucial information such as log files from the Android device. Different steps are required to activate USB debugging mode, depending on what version of Android is being used. USB debugging requires the passcode.

30. A further example is *"downgrading"* an application to a previous version which had exploitable vulnerabilities, and then exploiting them to acquire further data.[56] An MPE audit log included in the Defendant's disclosure appears to show that this method may have been deployed. The Audit Log records: *"App downgrade"*, *"Twitter version 8.35.0 – release 03"*; *"Uninstalling current version of application Twitter"*; *"Installing older version of application Twitter"*.[57]

31. Logical extraction only allows for data that is accessible <u>via the device's own software</u> to be interrogated and extracted, i.e. only the data a user would be able to see on manual examination of the (unlocked) device. It cannot

[55] DM/5F, see section 6, 'Process' **[CB/2/G/332].**
[56] DM/5F , paragraph 6.18: "Select 'Backup' for first extraction. This will open a further confirmation screen … which states 'Do you want XRY to downgrade the application'… 'You may retrieve more data but will make changes to the device.'" **[CB/2/G/334]**
[57] SMB/07 **[CB/2/G/902].**

therefore generally recover deleted data.[58] It creates a copy of data such as the phone's phonebook, call logs, contacts, SMS, photos, videos, some application data (depending on where the data is backed up on the phone) and other data one might expect to retrieve from an iTunes or Android backup. The data requested is retrieved from the device's memory and sent back to the forensic hardware. The examiner can then view the extracted data.

(c) File System Extraction

32. The Defendant's disclosure includes options for "file system extraction",[59] which is a variant of the logical extraction method I described at section (b) above.

33. A file system is the structure in which data is stored on a phone. The file system contains the files and folders that the device uses to populate applications (e.g. social media applications), system configurations and user configurations (e.g. WiFi connectivity settings) along with user storage areas[60] (e.g. in respect of different apps and media).

34. Access to certain partitions on a device is not usually provided to regular users, to prevent them from damaging the operating system. When individuals seek complete access to everything in the operating system they seek to "*root*" their device. Whereas a user is allowed to do certain things on their device, a root user or "*super user*" has permission to do anything to any file anywhere in the system.

35. File system extraction usually requires root user access to the phone in order to access the file system.[61] As such, to carry out the extraction, the software

[58] Although it may be possible to recover deleted records including SMS, chats and browsing history if SQLite databases (or other simplistic storage technique) are used to store the data. An SQLite database is a structure found in Android and other devices. Apps might use these solutions to keep a record of the deleted data (as to allow the user to recover it). These records could then be accessible for an extraction, unlike deleted data more generally. Which is why you would be able to recover some deleted data. See for example SMB/07 "Get deleted SQL Data" **[CB/2/G/899].**
[59] See DM/5A, SOP for Sim Card Extraction, 6 July 2017 **[CB/2/G/ 302];** SMB/07Audit Trail Activity **[CB/2/G/895-898].**
[60] For an example of searching files and folders, see SMB/07, Extraction Log: 'file/system/build.prop'; 'file/system/bin/secilc'; 'file/system/bin/sendevent' **[CB/2/G/895].**
[61] Ibid.

will seek to root the phone, which may involve the examiner pressing certain keys and manipulating the phone as directed.

36. File system extraction is slightly more data rich than a logical extraction (although as with all forms of extraction, the capabilities of a file system extraction will be device-specific). It can include system files, user databases, media, user files, logs, and user settings, and can even recover files that are hidden on the system. Such files could include data such as logs showing when applications were installed, used and deleted and how often they were used; when a device was locked or unlocked; when a message was viewed; whether a Bluetooth device was connected; what other Bluetooth devices were in the vicinity of the device; wireless networks connected to; or mobile phone cell towers connected to.

(d) Physical Extraction

37. Physical extraction is referred to in the Investigation Record in the Defendant's disclosure.[62] It involves a *"bit-by-bit"* copy of the physical storage, entire file system or device memory. It extracts the raw memory or raw data from the device's storage. This allows access to data not available through logical extraction, including potentially deleted data[63] and other data not immediately accessible to the user, such as system and user files. It is a more technically difficult form of MPE (it is *"Level 2"* extraction), but it can deliver more data.

38. Physical extraction requires that the phone be put into recovery, rescue or download mode. In this mode the phone may allow the insertion of a small piece of code, called a bootloader, during the start-up process. This will read the contents of the device's memory and send it back to the extraction device. For some phones it may be necessary to turn off the phone, remove the battery and use special cables to connect to the forensic device. Physical extraction may take place on site (unless a private provider requires it to take place at their premises for security reasons).

[62] SMB/05 states: "*4x Physical downloads attempted on android phones seized with no PIN numbers obtained. 1 successful extraction*." **[CB/2/G/832].**

[63] As explained above, it should be noted that logical extraction can sometimes reveal deleted data.

(e) Sim Card Extraction

39. The Defendant's disclosure refers to Sim Card Extraction, conducted using "UFED Touch Unit" software and "Cellebrite Software version 6.2.1.17".[64] In general, modern phones store data in the device's memory and SIM cards are used only to identify subscribers in cellular networks. However, some modern cheap phones with limited memory capability store phone owners' data in the SIM card.

(f) More Complex Forms of Extraction

40. There are a number of other forms of extraction which are more complex and require the disassembly of the phone. They generally involve the use of expert or bespoke methods to tackle damaged devices. These methods of extraction will invariably take place in digital forensics laboratories[65].

40.1. **JTAG:** JTAG involves the disassembly of a mobile phone and connection of forensic hardware to test points or components on the motherboard in order to read data from the handset. Connection can be made using specialist adapters, by micro-soldering wires or a combination of the two. Wires can be de-soldered after data extraction to return the handset to its prior state. Using this method, data can be extracted from handsets unsupported by forensic software, along with PIN, swipe pattern or password protected phones.

40.2. **Chip-off:** This is a destructive method, which means that the device is physically broken and cannot be restored back to its normal working condition. Destructive methods are used when the device is non-functioning because of severe physical damage. Chip-Off involves the removal of the flash memory chip from a mobile phone and the use of specialist hardware and software to read the data from it. This process is intricate, and it is possible to damage the chip in such a way that getting the data would be difficult or impossible.

[64] DM/5A, SOP for SIM Card Extraction dated 6 July 2017 **[CB/2/G/299].**
[65] ICO Report **[CB/2/G/595];** See also the ACPO Good Practice Guide *"…potentially the physical removal and examination of memory chips (level 4). These examination levels are outlined in the CPIA mobile phone SOPs."* **[CB/2/G/560].**

Once the memory chip is physically removed, the raw data is acquired or imaged from the chip using specialised chip programmers and adapters. The raw information retrieved from the memory needs to be parsed, decoded and interpreted.

40.3. **ISP:** ISP *"In-System Programming"* involves connecting to an eMMC or eMCP flash memory chip to download a device's complete memory. eMMC and eMCP are the standard in today's smartphones, and ISP enables examiners to recover the complete data directly without removing the chip and destroying the device. ISP involves the disassembly of the device to get to the motherboard or circuit board. By soldering conductors to Test Access Points (the solder balls on the surface of a memory chip), the phone can be connected to a device which can read the data from the memory chip.

(g) Extraction without Access to Mobile Phone

41. For completeness, I note that it is possible to obtain data held on mobile phones without physical access to the device. However, this would require techniques that are associated with equipment interference (also known as *"hacking"*), such as installing malware on a phone to enable remote access.[66] MPE in the sense relevant to this case requires access to the physical device, which can then be connected to a data extraction device. I note that the Defendant's disclosure includes a review of MPE dated 13 December 2020 which refers to *"[t]he Intelligence Joint Debriefing Team (JDT) viewing material on digital devices prior to seizure (risk of interception of communication)".*[67]

D. ANALYSIS OF DATA EXTRACTED BY MPE

42. Having described how data can be extracted, I will now explain how that data can be analysed, and to what information, in simple terms, the MPE described in the disclosure will permit the extracting agency to have access.

[66] DM/36, at paragraph 12: ". November: Working with international law enforcement partners and the North West Regional Organised Crime Unit, the NCA coordinated the UK effort against an online site selling a popular hacking tool. The Imminent Monitor Remote Access Trojan, once covertly installed on a victim's computer, allowed the hacker full access to the infected device, enabling them to disable anti-virus software, steal data or passwords, record key strokes and watch victims via their webcams." **[CB/2/G/1203].**
[67] DM/40 **[CB/2/G/1274].**

(1) Capabilities of Data Analysis Software

43. Once an agency obtains data from a device, they can use software to cleanse, analyse and visualise the data. Analytics software can facilitate the use of the data extracted by officers in at least the following ways.

43.1. It can organise data extracted into different file types from XML, CSV, TXT to CDR, media, and text, as well as conduct keyword searches of extracted data or search by image classification.

43.2. It can use visualisation tools to make the data easier to read – by, for example, displaying text conversations as a chat instead of individual messages in a database; tracing a user's location or activities on a map or chronological timeline; sorting data by file type regardless of its location on the phone; or creating network graphs to infer social relationships using contact data.

43.3. It can conduct link analysis to analyse phone calls, emails, text messages and location data to discover associations between individuals via different types of data. This can demonstrate the frequency of contacts between phone numbers and between IP addresses over time, financial transactions and chronologies of events, among other things.[68]

43.4. It can bring together datasets from different devices[69] to find links across the devices, like common contacts, call or text records, or account information. Common geolocation or purchase data between

[68] Sommer, P. (19 November 2018) Professor Peter Sommer – Supplementary written evidence (FRS0098): Artificial Intelligence and digital forensics [Online] para 3. Available at: *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/92608.html* **[CGW1/22/195]**.

[69] This is used as a selling point by companies providing the software. The UK data company Chorus Intelligence, which received £684,552 in payments from Immigration Enforcement in 2018, claims that one of its products is able to find "previously hidden connections and [open] up new lines of enquiry, putting actionable intelligence in the hands of Investigators fast." – see Chorus , Data Cleansing and Analysis for Law Enforcement (2019) [Online]. Available at: *https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/581236/668104362664570-service-definition-document-2019-07-03-1102.pdf* **[CGW1/17/155]**; see also Basis Technology, Watchlisting for Secure Borders [Online]. Available at: *https://www.basistech.com/solutions/watchlisting-for-secure-borders/* **[CGW1/19/172]**.

phones could be used to show the phones were at the same point near each other to buy things at the same point in time.

(2) Intrusiveness of Information which Data Analysis can Reveal

44. Smartphones contain a huge amount of information and hold extraordinarily intimate data about our lives and those of third parties. According to the ICO:

> *Our smart phones are powerful repositories of highly sensitive personal information, including our intimate conversations, family photographs, location history, browsing history, biometric, medical and financial data. They reveal patterns of our daily personal and professional lives and enable penetrative insights into our actions, behaviour, beliefs, and state of mind. It is no exaggeration to say that the personal data found in our mobile phones richly depict our lives.*
> …
> *Today, people see mobile phones as extensions of themselves; they have become unique repositories of our personal information, generating huge amounts of data and often hold the most intimate and private details of our everyday lives. Mobile phone usage continues to grow exponentially with all generations routinely interacting through phones and applications. Mobile phones are used in such a range of activities that even a cursory analysis of their contents can reveal detailed insights into thoughts, movements and personal preferences.*
> …
> *The extent to which these devices effectively record a user's everyday activities, whether it be their movements, their associations, their personal preferences, or the services they access online, is unprecedented.*
>
> *There can be few aspects of day-to-day life that do not involve the use of mobile devices, ranging from formal business communications to accessing sensitive financial records, recording family holiday memories, or having intimate exchanges with loved ones. The ever-expanding capacity to generate and store data means that a significant history and amount of personal data is held on most devices, including what we might consider to be our most private and sensitive information.*[70]

45. Put in simple terms, this means that the data analysis described above can enable a minute-by-minute analysis of someone's activities.

46. Further, unlike a diary, where the owner has full control and knowledge of its contents, users do not initiate or even know about all the processing

[70] ICO Report (June 2020), **[CB/2/G/596-607].**

taking place on the smartphone, much of which occurs without any interaction with the user.[71] Apps can record data such as location history; browsing data; cookies; app usage; Wi-Fi connection history; when applications were installed, used and deleted and how often they were used; when a device was locked or unlocked; when a message was viewed; whether a Bluetooth device was connected; what other Bluetooth devices were in the vicinity of the device; wireless networks and cell towers connected to; words added to a user's dictionary; and notifications. As a consequence, it is possible to extract data which the user is unlikely to be aware of, including logs permitting a reconstruction of their lives of the sort described above.

47. Users may not even have control over what appears on their device: apps such as WhatsApp will push media sent by someone else onto the device, perhaps without the recipient's knowledge or explicit acceptance.[72]

(3) <u>Types of Information which Data Analysis can Reveal</u>

48. The data that can be obtained from a successful extraction is far broader than communications data alone. While Nicholas Jupp refers to <u>communications data</u> as being of key evidential value,[73] framing the data to be extracted from devices as purely communications data is an understatement. I have set out in the table below a list of the types of data that I am aware the most common MPE software is able to extract (first column) and indicated examples of places in the Defendant's disclosure evidencing the extraction or potential for extraction of such data by the Defendant (second column).

Data Type	**Disclosure**
Address book (contact names, numbers, email & postal addresses etc)	DM/2 **[CB/2/G/294]** DM/5A **[CB/2/G/303]** SMB/07 **[CB/2/G/904]**
Call history (dialled, received, missed, duration, date/time)	First Witness Statement of Stephen Blackwell **[CB/2/G/692-696]** DM/2 **[CB/2/G/294]**

[71] Ibid.
[72] Ibid.
[73] First Witness statement of Nicholas Jupp, 20 April 2021, para 11 **[CB/2/G/909].**

	DM/5A **[CB/2/G/303]**
SMS/MMS messages (contents)	First Witness Statement of Stephen Blackwell **[CB/2/G/692-696]** DM/2 **[CB/2/G/294]** DM/5A **[CB/2/G/303]** NJ/005 **[CB/2/G/1002]**
Emails	First Witness Statement of Stephen Blackwell, **[CB/2/G/692-696] DM/5A [CB/2/G/303]**
Web browser history, bookmarks, cache, cookies	**DM/2 [CB/2/G/294]** **DM/5A [CB/2/G/303]** **SMB/07[CB/2/G/899]**
Media (photos, videos, audio recordings – often with date/time stamp and geolocation i.e. metadata)	First Witness Statement of Stephen Blackwell, **[CB/2/G/692-696]** DM/2 **[CB/2/G/294]** DM/5A **[CB/2/G/303]** NJ/**005 [CB/2/G/1002]** SMB/07 **[CB/2/G/903-904]**
Applications data (which can include social networking data, health & activity data, financial data, bio data, friends and family's movements etc, potentially other sensitive data)[74]	NJ/005 **[CB/2/G/1002]** DM/5A **[CB/2/G/303]** SMB/07 **[CB/2/G/891-905]**
GPS Location data (including historical)	First Witness Statement of Stephen Blackwell **[CB/2/G/696]** NJ/005 **[CB/2/G/1002]** DM/2 **[CB/2/G/294]**

[74] e.g. see SMB/07, list of applications analyzed: AliExpress Shopping App, Amaz, Badoo, Coffee Meets Bagel, Facebook, Garmin, Grindr, Fantasy Football, Calorie Counter, UberDriver, calls, contacts, messages/sms, MMS, emails, calendar events, web bookmarks, web history, web searches, keyboard cache, Chrome, Facebook, Google Maps, Telegram, Twitter, browser, lock pattern, wifi, location cache, cookies, cookie analyzer, google mobile services, thumbdata, etc. **[CB/2/G/891-905].**

Social Media (as discussed below)	NJ/003 **[CB/2/G/986]**[75] First Witness Statement of Stephen Blackwell, para 49, **[CB/2/G/691]**
Calendar	DM/5A **[CB/2/G/310]**
User dictionary	DM/5A **[CB/2/G/303]**
Documents (stored locally and on the cloud)	SMB/07 **[CB/2/G/903]**
Swipe Patterns	DM/2 **[CB/2/G/295]**
Autofill and keyboard cache	SMB/07 **[CB/2/G/896]**
Bluetooth connections	PI's own extraction carried out in 2018 using Cellebrite UFED demonstrates this capability **[CGW1/16/123]**; [76] although there are no specific examples of retrieval of Bluetooth data in the disclosure, the Defendant uses Cellebrite UFED software, as explained elsewhere in this statement.
Cell Tower connections	As above, Cellebrite UFED software demonstrates this capability **[CGW1/16/140]**.[77]
Wi-Fi networks	As above, Cellebrite UFED software demonstrates this capability **[CGW1/16/123], [CGW1/16/130].**[78]
Deleted data	SMB/07 **[CB/2/G/899]**
Metadata and logs	NJ/007 **[CB/2/G/ 1036]**

[75] The document states: '*Social Media, Recovery and Review. Set out why it is you are investigating social media as part of in this case. What are you expecting to find and why? Define all reasonable lines of enquiry, keyword/phrase searches and time parameters. Have the defence highlighted any reasonable lines of enquiry for you to follow? Document and explain any lines of enquiry you considered but did not follow.*'
[76] See Privacy International, at Figures 9 and 13 [Online]. Available at: https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf.
[77] Ibid, Figure 18.
[78] Ibid, Figures 9 and 13.

(4) How the Defendant analyses the MPE data and integrates it with other data

49. The Defendant analyses the extracted data in several ways.

50. An initial analysis is presented on the kiosk itself when data is extracted,[79] which presents the data in a certain way and enables reviewing. The digital strategy for investigation directs the extraction of data using the kiosk system.[80] Previously, extracted data was stored on a USB Flash drive, SD card or PC.[81] The kiosk system replaced the "*current system which uses the same software but stores data on non-encrypted USB drives. There is with the current system no control over how many copies can then be made from any one USB drive and as such less assurance around DP compliance*."[82] The absence of protection for what is often sensitive and intimate personal information is notable.

51. Once data has been extracted by the kiosk, the following complementary systems are used to analyse the data.

(a) Processing

52. **Clue 3** and **Black Rainbow** process the data. **Clue 3** is CFI's case management system, seemingly introduced at the time of publication of IE and CFI's Data Protection Policy on 18 August 2020.[83] It is described as "*The principal system for processing data relating to operations, investigations or enquiries undertaken by CFI […]*".[84]

53. From **September/October 2020**, data from extractions were stored in a database within an Amazon Web Services (i.e., Amazon's 'cloud' data processing and storage service) account managed by **Black Rainbow**,[85] a third party who provides the software and hosts the digital forensic case

[79] NJ/005, DPIA Kiosk System: "*The system will allow for the effective processing, including the reviewing and analysis of data which will support the investigation of crime and administration of investigation procedures in line with the CPIA. Hardware and software for the kiosk solution is provided by MSAB who a key player in the extraction and analysis of digital forensics are*." [sic] **[CB/2/G/1004].**
[80] Second witness statement of Nicholas Jupp, 7 June 2021, para 17 **[CB/2/G/1071].**
[81] DM/5A **[CB/2/G/302];** DM/5B **[CB/2/G/308].**
[82] NJ/005 **[CB/2/G/1005].**
[83] NJ/001 **[CB/2/G/917].**
[84] NJ/001 **[CB/2/G/923].**
[85] NJ/006 section 2.9, **[CB/2/G/1021].** See also NJ/001: "*Data controlled by CFI is processed on behalf of CFI by a number of third parties during the course of investigations. CFI make use of a number of external section DPA forensic service providers (EFPs) who process data on our behalf.*" **[CB/2/G/935].**

management system.[86] The software is used to record forensic case summaries, unique identifiers linked to a device, and digital strategies.[87]

(b) Analysis

54. **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.[88]

55. It processes the data obtained from mobile phone extraction. The system "*seeks to cleanse and analyse large volumes of data with the ultimate aim of assisting investigations detect and solve crime*."[89] It is used by Immigration and Intelligence Officers within IE,[90] and the system is also used by "*numerous Police forces, Counter Terrorism Policing and the NCA*".[91] It can also cross-reference across devices: the relevant DPIA states that Chorus "*is able to cross-reference day/date/time place information that will support the detection and prevention of crime. It can provide analysis of a person's movements and proximity to known criminal events, establish connections and contacts across criminal networks and provide court ready evidence in support of criminal prosecution.*"[92] The objectives of doing so are to "*Gather more intelligence and best evidence in the investigation of organised crime; Enhance capability to manage large data sets; identification of criminal association and links to organise crime; ability to share certain datasets with law enforcement partners*".[93]

56. Prior to the use of Chorus, the Home Office were using Excel spreadsheets.[94]

(c) Integration

57. The Defendant's disclosure reveals a high level of integration and cross-checking with bulk databases, so that the information extracted from a phone can be cross-checked against information held about the individual

[86] NJ/006 **[CB/2/G/1023].**
[87] NJ/006 **[CB/2/G/1020].**
[88] As indicated in the Government's Contracts Finder webpage, available at: https://www.contractsfinder.service.gov.uk/Notice/85c416a4-bc26-4a65-9474-ed40edc04e86 **[CGW1/7/43]**.
[89] NJ/007. **[CB/2/G/1041].**
[90] NJ/007 **[CB/2/G/1037].**
[91] NJ/007. **[CB/2/G/1041].**
[92] NJ/007 **[CB/2/G/1038].**
[93] NJ/007 **[CB/2/G/1041].**
[94] NJ/007 **[CB/2/G/1039].**

elsewhere and/or about associates of the relevant individual. Cross-checking to and integrating with other databases significantly increases the amount of information which MPE can reveal about a person. I explain below the specific techniques cited in the disclosure and the potential privacy implications.

(i) Washing

58. The Defendant's disclosure refers to *"washing"* against other databases[95] and it forms part of the 'Multi-Agency Clandestine Communication Data Strategy'[96] to "[wash] data through multi-agency databases. Identifying and analysing data of interest."

59. The process of washing appears to refer to data cleansing, i.e. tidying up the records in respect of an individual by detecting, correcting or removing corrupt or inaccurate records. The disclosure refers to data washing as part of the data enrichment stage[97].

60. Ministers appear to have been given assurances that <u>all</u> mobile phone data will be washed against the Data Analytics Competency Centre and National Digital Exploitation Centre databases.[98] It is apparent that there has been exploration of – and discussion with the National Crime Agency ("**NCA**") about – the possibility of bulk data washing.[99]

(ii)Project Sunshine

61. **Project Sunshine** refers to a dataset to which data was added until September 2020, and the project integrates extracted data. The Project Sunshine DPIA sets out the data to be processed: "*Phone downloads, phone billing and other forms of communications data collected in the response to the clandestine threat.*"[100] The DPIA indicates the scale of the operation: "*In the region of potentially 50,000 individual phone numbers, email addresses and social*

[95] DM/30 states: "*Downloaded data assessed, translated and disseminated to partners for data washing to identify offenders or because obvious evidence of offences exists*." **[CB/2/G/1170];** see also DM/33, "Graeme Davison will explore whether any bulk data washing against HO systems can be done so that we can cleanse the data somewhat before sharing." **[CB/2/G/1184].**
[96] GD/2 **[CB/2/G/1302].**
[97] GD/2 **[CB/2/G/1302].**
[98] DM/34 **[CB/2/G/1189].**
[99] DM/33 **[CB/2/G/1184-1185].**
[100] NJ/008, DPIA Template, Project Sunshine **[CB/2/G/1052].**

media accounts are expected to be processed annually (data collected over a three-month period in early 2020 has 28,000)."[101] The Defendant states that the purpose of the analysis is to target organised criminal groups.[102]

62. In **April 2020**, Graeme Davison was tasked with developing an analysis approach to utilising communications data to aid the small boats effort. The project ran until **September 2020** with the purpose to "*combine the communications data downloaded from mobile devices and generate organised immigration crime leads*".[103] It is apparent that, at the start, Project Sunshine involved a system of spreadsheets, which were collated together to create one master spreadsheet.[104]

63. From **May to August 2020,** the project identified associations across the data. "*This meant that phone numbers present in multiple mobile devices were identified. These associations were then subjected to automated enrichment through Home Office Data Services Analysis technology. The results of this where then assessed by the Sunshine team as worthy of further development and passed to the Gateway Multi-Agency Hub for further action.*"[105] 100 leads were generated but none resulted in operational activity.

64. A second approach started in **August 2020,** which "*saw the team enrich all the data and then attempt to establish activity from that position.*"[106] No leads were generated from this approach, "*which was difficult to work with*".[107]

65. The Project Description[108] refers to an intention to enrich from Home Office systems including ASYS; Biometric Residence Permit; Case Information Database; Central Reference System; GBD; Immigration Asylum Biometrics System; Intelligence Management System; IMSR; National Operations

[101] NJ/008 **[CB/2/G/1056].**
[102] First witness statement of David Magrath, para 16 **[CB/2/G/282]** ; see also Reply to Defendant's (1) acknowledgment of service and (2) objection to Claimant's application for Case Management Directions, 22 January 2021 in which the Claimant observes: "*…the Parliamentary Under-Secretary for the Home Department stated, in terms, on 2 November 2020, in response to a written Parliamentary question, that 'Phones are seized to gather evidence to establish Organised Crime Group links.'*" **[CB/1/A/57].**
[103] Witness Statement of Graeme Davison, para 6 **[CB/2/G/1296-97].**
[104] Witness Statement of Graeme Davison, paragraphs 8, 13 **[CB/2/G/1297-8].**
[105] Witness Statement of Graeme Davison, paragraph 9 **[CB/2/G/1297].**
[106] Ibid.
[107] Ibid.
[108] GD/2 **[CB/2/G/1306].**

Database; Points Based System; Single Intelligence Platform. And against NCA datasets [redacted] and wider NCA intelligence systems[109].

66. The Respondent's witness evidence states that no new data has been added to Project Sunshine since September 2020.

67. The Project Sunshine DPIA (completed on **11 November 2020**) refers to the enriching and analysis of data collected from migrants' phones in order to build up more complete intelligence pictures than would be available from the extraction of data from a single phone.[110]

68. As part of Project Sunshine, bulk metadata is being used to search for commonalities across different phones:

    68.1. Project Sunshine is designed to perform *"crime pattern analysis"* and *"identify associations and patterns that fit a profile of criminality"*[111] using *"big association and network analysis techniques"*.[112]

    68.2. The DPIA states: *"Data enriched against the numbers, emails and other contacts taken from the phones will capture name, date of birth, address, nationality, known aliases, other phone details, known financial information, immigration history, known criminal offences if those numbers and email addresses are known to and stored within law enforcement indices."*[113]

69. The sources for data to be integrated extend to a range of Home Office and NCA systems/databases, in order to *"attribute names, date of births, nationalities and other details from a range of Home Office and NCA systems to phone numbers and email accounts."*[114] A further source is *"phone billing information secured lawfully from communication companies"*.[115]

[109] GD/4 **[CB/2/G/1324].**
[110] NJ/008 **[CB/2/G/1052].**
[111] NJ/008 section 5.8 **[CB/2/G/1060].**
[112] NJ/008 **[CB/2/G/1061].**
[113] NJ/008 section 2.1 **[CB/2/G/1052].**
[114] NJ/008 **[CB/2/G/1055].**
[115] NJ/008 **[CB/2/G/1056].**

70. Access to Project Sunshine included staff working in the Home Office. This access extended to unique numbers collected, Home Office enrichment results and NCA enrichment results.[116]

(d) Sharing with Other Agencies

71. The extracted data are also processed by other agencies.[117] For example, the data is shared by email with the National Data Exploitation Capability in the NCA[118] and the Data Services and Analytics function in the Home Office.[119] The disclosure shows the NCA's interest in obtaining phone numbers for intelligence purposes "*in respect of the potentially illegal entry into the UK of the migrants and to investigate any SOC surrounding that*."[120] The revised CFI Data Protection Policy also provides that "*CFI intend to establish and implement an automated data sharing link between the Clue 3 case management system, and other Home Office databases, such as Entity and Atlas, managed by other departments within Immigration Enforcement and UK Visa and Immigration (UKVI).*"[121] It appears that further integration and analysis might take place after the data are shared: "*The results are then analysed and targets identified for UK based investigation and disseminated for overseas preventative activity.*" [122]

72. In this context, I note that a large number of databases[123] are used by various agencies across the UK's border, immigration and citizenship system. Many of these are intended for security purposes and not for immigration or border management.

73. Those databases include the National DNA Database (which holds around 6.3 million DNA profiles of subjects in criminal cases, some of whom have

---

[116] NJ/008 **[CB/2/G/1053-1059].**
[117] NJ/001 states: "*Some data relating to some specialist capabilities in connection with covert, digital, forensic enquiries or analysis and financial processes [redacted] will be processed on separate systems. Data will also be processed under contract by external forensic providers and within the [redacted] prior to transfer to the CPS*." **[CB/2/G/923].**
[118] NJ/008 **[CB/2/G/1055].**
[119] NJ/008 **[CB/2/G/1055].**
[120] DM/32 **[CB/2/G/1183].**
[121] NJ/002. **[CB/2/G/949].**
[122] NJ/008 **[CB/2/G/1056].**
[123] Privacy International (February 2021) The UK's Privatised Migration Surveillance Regime: A Rough Guide for Civil Society [Online]. Available from: *https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf* **[CGW1/5/32]**.

not been convicted of a crime, and profiles of victims); the Immigration and Asylum Biometric System (which holds around 25 million fingerprints and faces collected by (among others) UK Visas and Immigration); the Law Enforcement and Security Biometrics System (the main criminal fingerprinting database used by law enforcement in the UK, which in 2018 held the biometrics of around 8 million people); the Case Information Database (the main case-working and operational database at the Home Office, used throughout the Department "*to record personal details of all foreign nationals who pass through the immigration system*"); the Asylum Support System (containing details about asylum seekers applying for and receiving support); the Warnings Index (according to a whistle-blower, a watchlist developed originally in 1995 which tracks people with "*previous immigration history, those of interest to detection staff, police or matters of national security*", whose staff also have access to an IT system operated by MI5); Semaphore (a database in use since 2004 which compares data from air and other carriers against the Warnings Index for matches); and the Initial Status Analysis database (developed in 2015 as part of the Exit Checks Programme, and used to enable screening of people leaving the UK). Further, the Home Office is currently developing several large IT systems which will be used to replace existing systems that track individuals throughout the borders, immigration and customs system and enable the use of surveillance tools by relevant units and officers, including the National Law Enforcement Data Programme. PI is aware from engagement with the Home Office that this database was planned to include data extracted from mobile phones.[124]

(e) <u>*Conclusion on Data Analysis*</u>

74. As the above shows, the collection and review of data is significantly more extensive than pure collection and review of communications data on an asylum seeker's mobile phone. I question whether those who are surrendering their phones *"voluntarily"* are properly informed about the

[124] Engagement in 2020 as part of the LEDS Open Space initiative. Also confirmed in the Home Office's Law Enforcement Data Service – Privacy Impact Assessment Report (July 2018) [Online], at paragraphs 4.16 and 6.5, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf **[CGW1/26/243-245]**.

extent of this processing, especially at a time when seizures were conducted in a blanket manner. The sorts of systematic data analytics and bulk data integration revealed by the Defendant's disclosure represent a significant interference with the right to privacy, one which could only be proportionate in the most serious of circumstances.

E. CLOUD EXTRACTION

75. I note briefly that modern smartphones are designed to seamlessly store, share, backup and retrieve data held on the 'Cloud' (i.e. on remote servers usually controlled by a third-party provider). In addition, much of the functionality of smartphones involves accessing internet-based services, such as social media sites (most of which are now also running on the Cloud). It is possible for an extracting agency, once it has extracted keys (or "*tokens*"), such as login credentials or authentication tokens, from a mobile phone, to access data stored on the Cloud.

76. A vast amount of highly sensitive personal data is stored on the Cloud.[125] Access to the Cloud allows access to a suite of data which might not be available from even the most sophisticated extraction of data from the phone itself, including: data from social media, messaging apps, online retailers and files storage apps; as well as a history of searches, bookmarks, saved passwords, visited pages, voice search recordings and translations. Further, any user with their location history turned on in their Google account will have records of their location stored on the Cloud. These location records are precise and can span years, and many users do not realise this data is being stored. Most strikingly, once the login credentials are obtained, it is technically possible to not only extract the data but to continue tracking the online behaviour of the individual whose data has been accessed, even after the phone is returned, until such time as the individual changes their password.

[125] Patrizio, A. (3 December 2018) IDC: Expect 175 Zettabytes of Data Worldwide by 2025 (Network World) [Online]. Available from: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html **[CGW1/20/176]**.

77. Cloud extraction requires no special additional processes. The ability to access cloud stored data is generally sold as a software licence by providers and can form part of the same data extraction software package as MPE (so that when extracting data from the device, the software will also attempt to extract data from the Cloud).

78. The disclosure refers to "Analyzing Dropbox Tokens" and other tokens.[126] It is possible that this is referring to the obtaining of tokens in order to access cloud-stored data.

F. CONCERNS ABOUT MPE

79. MPE gives rise to a number of risks and concerns.

(5) Privacy

80. As set out above, MPE potentially provides access to large quantities of personal data. This raises serious privacy concerns on its own. However, those privacy concerns are heightened by the following factors.

(a) Excessive Data Extraction

81. **First**, the data collected is often excessive. It often cannot be (or if it can be, is not) limited to relevant material.[127] For example, extraction may be limited by date, time or other parameters.

82. The Defendant's disclosure demonstrates that options for selective extraction are very limited. For example, the 2016 vendor training and standard operating procedures only provide for selection of very broad categories of data,[128] and a "*Select All*" option is available.[129]

83. It seems that the Defendant's approach has indeed evolved over time: the ICO report led to a more focused and targeted approach to the extraction of data, which "*[i]n the context of the small boats issue, this limited the examination of data to the 30 days prior to arrival rather than downloading the whole of the*

[126] SMB/07 [CB/2/G/902-903]
[127] The ICO Report (June 2020) states: "*Firstly, many of the kiosks used in forces are configured in a way that does not allow the selection of specific data to be extracted at a very granular level*." **[CB/2/G/639].**
[128] DM5A **[CB/2/G/303].**
[129] DM5A **[CB/2/G/310].**

phone."[130] The foregoing indicates just how much material – including irrelevant, sensitive material – even a 30-day download could yield. The disclosed audit trail[131] demonstrates the volume of data actually extracted out of just one mobile phone: 100,128 Pictures, 95,250 Documents, data from 329 Installed Apps, amongst others. In any event, despite the 30-day download instructions, I have not seen options in the disclosed training materials that would allow for selective extraction by time and date.

84. If relevant selective extraction is not a possibility, then the only restrictions on access to the vast quantity of private and irrelevant data will be what the operator of the MPE technology chooses to search for or seek access to. The entire accessible dataset will have been extracted in any event. The standard deployment of the technology by law enforcement in the past has been to simply download the entire contents of a phone (or at least far more of it than was required), much of which will be irrelevant and highly private.[132] It is not clear from the Defendant's disclosure whether data is selectively extracted or just selectively reviewed.[133]

(b) Proportionality

85. **Second**, the volume of data extracted and the particularly private nature of this data calls into question the proportionality of the use of MPE on those arriving in small boats. Identifying associations between all communications data contained on extracted phones (as Project Sunshine was specifically designed to do) will inevitably result in the investigation of certain common relationships between migrants that have nothing to do with any common trafficker or boat steerer. That is borne out by what happened: this approach generated only 100 leads and resulted in no operational activity. The approach then shifted to identifying associations across *"all the data"*. No leads were generated from this approach, "*which was difficult to work wit*h".[134]

---

[130] First witness statement of David Magrath, para 17 **[CB/2/G/282].**
[131] SMB/07 **[CB/2/G/891].**
[132] ICO Report (June 2020) **[CB/2/G/645]** NOTE [37] : "*The investigation found that the specific hardware and software tools offered by MPE vendors had capabilities designed to minimise intrusion and maximise privacy (eg by allowing focused extraction of specific pieces of data). However, the individual implementations in forces had simplified user interfaces that did not allow use of this privacy-enhancing functionality, and this has led to more data than strictly necessary being routinely extracted and processed*."
[133] DM/40 **[CB/2/G/1278];** Witness Statement of Nicholas Jupp, paras 18-19 **[CB/2/G/912].**
[134] Witness Statement of Graeme Davison **[CB/2/G/1297].**

This suggests that the number of associations thrown up by that analysis was so large that it was impossible to draw useful conclusions – while in the meantime involving dozens of officers reviewing large numbers of innocent associations, a considerable intrusion into individuals' privacy.

(c) Bulk Data Integration

86. **Third**, the privacy implications of MPE are compounded by the fact that, through operations such as Project Sunshine, it is possible to overlay multiple data sources to draw connections and inferences about the meaning and context of certain information on the phone, and thereby about the phone owner. Such additional information might come from:

86.1. **Other mobile phones**: If a mobile phone is seized along with others, or there is some other reason to think that two seized mobile phones might be related, it is possible to analyse their data together to identify common locations or contacts[135] – as explained above.

86.2. **Social media**: The Defendant's disclosure refers to the investigation of social media accounts.[136] 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.

86.3. **Other databases**: as set out above.

[135] Witness statement of Graeme Davison, paragraph 8: "*Project Sunshine combined the call and text logs of the mobile devices into one spreadsheet. The data in the spreadsheet (a set of mobile phone numbers, landline numbers and some email addresses and social media handles) was then put through an analysis and enrichment process.*" **[CB/2/G/1297].**
[136] NJ/003 **[CB/2/G/986].**

86.4. **Physical surveillance**: Data can be supplemented by physical surveillance of migrants. In particular, satellite and aerial (including drone) surveillance are part of the surveillance tools which enable monitoring of migrants as they cross the Channel[137] This information can be fed back to supplement the information extracted by MPE.

86.5. **Communications data**: I note the disclosure refers to requesting data from telecommunications operators.[138] In addition to the example of "*content of text messages*" provided in the investigation management document, this data may include information about visited websites, email or call senders and recipients, map searches, GPS location and information about device connections to Wi-Fi networks.

(d) Third Party Privacy

87. **Fourth**, MPE has the privacy for persons other than the owner of the phone. Contents of communications will necessarily include information relating to wholly innocent individuals with whom the phone owner has communicated; and photos, videos and audio recordings may also include other individuals.

(e) Sharing of Data

88. **Fifth,** it is clear from the disclosure that the data is widely shared, including with Immigration Intelligence, the CFI, the police, NCA or other domestic or overseas law enforcement.[139] There is a "*JDT dissemination list*", and any urgent material may be distributed as the on-duty Chief Immigration Officer/Higher Executive Officer considers appropriate.[140] The JDT also disseminates the monthly analyst report to a wide range of recipients in the UK and overseas.[141] Further, it is intended to establish an automated data

[137] 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* **[CGW1/14/106]**; 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* **[CGW1/15/111]**; UAS Systems, Tekever AR5 [Online]. Available from: *http://uas.tekever.com/ar5/* **[CGW1/6/36]**.
[138] NJ/003 **[CB/2/G/987].**
[139] Second Witness Statement of David Magrath, para 15(d) **[CB/2/G/1126].**
[140] DM/27 **[CB/2/G/1161].**
[141] Witness Statement of Nicholas Jupp **[CB/2/G/1161].**

sharing link between the Clue 3 case management system and other Home Office databases.[142]

(6) <u>Reliability</u>

89. There are a number of interrelated concerns about the reliability of information which is extracted by MPE. These concerns are recognised in the industry generally and frequently expressed by various forensic experts.

90. **Accreditation**: MPE should be conducted (if at all) in accordance with accredited standards, in particular ISO 17025, which specifies the general requirements for the competence, impartiality and consistent operation of laboratories. The First Witness Statement of David Magrath (and exhibits) makes it clear that ISO 17025 accreditation has not yet been achieved, and that some practices may have contravened the standard.[143]

91. **Training**: MPE is complex and technical. It should only be undertaken by properly trained officers in order to ensure that privacy is protected so far as it can be, data is properly interpreted, and information is accessed and used responsibly. The importance of training is recognised by the Defendant.[144] There is a lack of information in the disclosure relating to whether all those involved in seizure and extraction and analysis of data from mobile phone devices have received the appropriate training. A lack of expertise and training, coupled with the vast amount of data that can be obtained, can easily lead investigators to misinterpret evidence[145] or fall victim to confirmation bias[146].

---

[142] NJ/001 **[CB/2/G/928].**
[143] DM/22 **[CB/2/G/673];** DM/28 **[CB/2/G/1270].**
[144] See, for example DM/40 **[CB/2/G/1274].**
[145] House of Commons Justice Committee (20 July 2018) Disclosure of evidence in criminal cases, Eleventh Report of Session 2017-2019 [Online]. Available from: *https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf.*
[145] CPS Disclosure – A Guide to "Reasonable Lines of Enquiry" and Communications Evidence (24 July 2018) (note [37] above) **[CGW1/25/225]**.
[146] See for example The Guardian, *Digital forensics experts prone to bias, study shows* (31 May 2021), in which former Forensics Science Regulator Dr Gillian Tully commented: "*I cannot overemphasise the importance of forensic scientists understanding the potential for unintentional bias, and of ensuring they take measures to minimise risks.*" [Online] available at: https://www.theguardian.com/science/2021/may/31/digital-forensics-experts-prone-to-bias-study-shows **[CGW1/2/9]**; see also CPS Disclosure – A Guide to "Reasonable Lines of Enquiry" and Communications Evidence (24 July 2018) **[CGW1/24/220]**].

92. **Integrity of the data:** As indicated in the Defendant's disclosure,[147] the integrity of intelligence or evidence obtained by MPE cannot be assumed. MPE technologies often cannot be independently tested,[148] and function as a black box, without objective evidence of correct links between inputs and outputs.[149] Extraction technologies may themselves have security vulnerabilities which can be exploited, and which may compromise the reliability of future (or past) extractions. One test in particular, on Cellebrite MPE technology, revealed that apparently innocuous files on phones connected for extraction could be used to modify not just the Cellebrite report being created in that scan, but also all previous and future generated reports from all previously scanned devices and all future scanned devices.[150]

(7) <u>Lack of Oversight</u>

93. In **June 2020** the ICO released a critical report[151] on the use of mobile phone data extraction by police forces in England and Wales, which the Defendant has referred to in evidence. The report called for reforms and safeguards so that data and privacy is protected from unnecessarily intrusive practices. The ICO echoed PI's concerns that, currently, there is no clear legal basis, policy guidance or independent, effective oversight for the police's use of MPE technology.

---

[147] DM/40 **[CB/2/G/1278].**

[148] House of Lords Science and Technology Select Committee (1 May 2019), Forensic science and the criminal justice system: a blueprint for change [Online]. Available from *https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/33302.htm***[CGW1/18/166]**; see also evidence provided to the Select Committee on Forensic Science by Dr Jan Collie (available at: https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html) **[CGW1 / 21 / 189]**.

[149] Marshall, A. M. and Paige, R. (11 October 2018) Requirements in digital forensics method definition: observations from a UK study (Digital Investigation 27(2018) 23-29) [Online]. Available from: https://eprints.whiterose.ac.uk/137032/1/requirements_digital_forensics.pdf **[CGW1/23/198]**; and Sommer, P. (19 November 2018) Supplementary written evidence (FRS0098): Artificial Intelligence and digital forensics [Online]. Available from: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/92608.html **[CGW1/22/195]**.

[150] Marlinspike, M. (21 April 2021) Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective (Signal) [Online]. Available from: *https://signal.org/blog/cellebrite-vulnerabilities/***[CGW1/4/26]**.

[151] ICO Report (June 2020) (note [50]) **[CB/2/G/632].**

94. On **7 October 2020,** the Law Commission laid before Parliament its report on Search Warrants, which included extensive analysis and recommendations in respect of electronic devices. Throughout the course of the project, the Law Commission became "*fortified in the view that there is a need for a wider review of the law governing the acquisition and treatment of electronic material. This stems from concerns about whether law enforcement agencies have the powers necessary to investigate crime, and whether adequate safeguards apply to ensure the use of powers is proportionate*".[152]

95. In that regard, it is notable that there are indications in the disclosure of the use of MPE by the Defendant at locations and times other than those addressed in the Defendant's evidence and which are the subject of the Claimant's claim. DM1 and DM4, for example, include "*Location Codes[153] for ISO 17025[154]*", indicating where in house forensic work was taking place. These locations include Immigration Reporting Centres, potentially indicating the use of mobile phone extraction in these locations from at least July 2017. There is also reference to immigration detention centres in SMB/05/2021 (page 831): "*seize the remainder migrant phones at Yarlswood.*" The disclosure also refers to the use of MPE by HMRC as part of Operation Chariot.[155] PI also understands from a report by the Independent Chief Inspector of Borders and Immigration that MPE technology is used in the context of lorry drops.[156]

---

[152] Law Commission (7 October 2020) Search warrants (Law Com No 396) [Online] para 18.1. Available from: *https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/10/Search-warrants-report-grayscale-web-1.pdf* **[CGW1/11/75]**.

[153] DM/1 includes Location Codes for Basingstoke, Becket House, Bedford, Belfast, Bristol, Cardiff, Croydon, Dover, Durham, East Midlands Airport, Eaton House, Gatwick, Heathrow, Humberside, Leeds, Liverpool, Manchester, Sheffield, Solihull, Stanstead. DM4 further includes Joint Debriefing Team, SACU Croydon, SACU Manchester **[CB/2/G/pages 290-291].**

[154] See DM/1: "ISO 17025 (which specifies the requirements for the competence to carry out tests or calibration) is the recognised standard to which laboratories must operate. The standard is to become mandatory for law enforcement agencies undertaking any type of in-house forensic work." **[CB/2/G/, 291].**

[155] SMB/05 **[CB/2/G/859]**.

[156]See the Independent Chief Inspector of Borders and Immigration Report [Online]. Available at: 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 **[CGW1/10/65].**

G. CONCLUSION

96. MPE is a complex and multifaceted technology. As often happens with new technologies used by authorities, the use of MPE by CFI grew organically with few policies or oversight mechanisms. This was the case until the ICO's 2020 report, at which point attempts were made to reduce the amount of data extracted and provide guidance on compliance with data protection legislation. It is doubtful whether those attempts went far enough.

97. MPE is also a particularly intrusive technology. Its use by the Defendant in the context of the small boat arrivals appears to have been particularly excessive, with recognised disproportionality, lack of proper expertise and training, and no adequate safeguards to protect individuals' privacy. As set out in this witness statement, even after the 30-day download policy applied, and particularly before then, the use of MPE would have extracted a vast amount of personal data, most of which was sensitive and personal but of no relevance to any criminal investigation and yielded no operational results (although it may still have been integrated with existing bulk data sources). Indeed, it seems from the disclosure that the amount of data extracted was overwhelming, to the point that it was actively unhelpful to investigations.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed by: 

Name: Camilla Graham Wood

Date: 1.11.2021