IN THE HIGH COURT OF JUSTICE **CO/4793/2020**
QUEEN'S BENCH DIVISION **CO/577/2021**
ADMINISTRATIVE COURT

B E T W E E N:

THE QUEEN
(on the application of HM (CO/4793/2020) and MA and KH (CO/577/2021))

Claimants

- and -

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

- and-

PRIVACY INTERNATIONAL

Intervener

WRITTEN SUBMISSIONS BY PRIVACY INTERNATIONAL

A. INTRODUCTION

1. These are Privacy International's ("**PI's**") written submissions, filed pursuant to paragraph 7 of the order of Mrs Justice Foster dated 1 December 2021 (the **"Order"**).

2. The purpose of PI's intervention is to assist the Court with the application of the law to the technologically complex facts of this case. PI has filed and served the witness statement of Ms Graham Wood, pursuant to paragraph 8 of the Order. PI's evidence is effectively uncontested by the Secretary of State.[1] Mr Blackwell has consulted a Home Office specialist, Mr Wyatt, who has informed him that *"very broadly speaking, the technical detail in Graham Wood 1 is accurate"*: **Blackwell 4 §29 [CB/63/881]**. It is therefore hoped that it

[1] Subject to clarificatory comments concerning **Graham Wood 1 §75, §77 [CB/64/915-916]** (both of which paragraphs concern Cloud extraction).

will be of use to the Court and the parties in understanding the technical nature of what occurs and the extent of interference with privacy involved.

3. PI also makes the following brief submissions:

   3.1. **First**, mobile phone extraction is a serious interference with the right to privacy, which can be justified only by cogent reasons.

   3.2. **Second**, the ECHR requires that prior independent authorisation be obtained before data from an individual's mobile phone is extracted.

   3.3. **Third,** the Secretary of State has failed to discharge her burden of demonstrating necessity and proportionality.

B. LEGAL FRAMEWORK

(1) Data Protection Act 2018 ("DPA")

4. Part 3 of the DPA governs the processing of personal data for law enforcement purposes. S. 34 sets out the six data protection principles and provides, at s. 34(3):

> *The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.*

5. The first data protection principle (s. 35 DPA) provides:

> *(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.*
>
> *(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either –*
>
> *(a) the data subject has given consent to the processing for that purpose, or*
>
> *(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.*
>
> *(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).*
>
> *(4) The first case is where –*
>
> *(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and*
>
> *(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).*

(5) The second case is where –

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

[…]

(8) In this section, "sensitive processing" means –

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

6. Accordingly, the processing of any personal data for a law enforcement purpose must be *"based on law"* and fair. Further, if, as in this case, the data processed is "*sensitive*" within the meaning of s. 35(8), and no proper consent was obtained, then the processing would only be lawful where *"strictly necessary"* for the law enforcement purpose.

(2) ECHR

7. The Secretary of State admits that MPE amounts to an interference with the right protected by Article 8 ECHR. That Article provides:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

8. An interference with Article 8 will be lawful where it is in accordance with law, and objectively justified as a proportionate means of achieving a legitimate aim. What must be justified is the precise interference at issue, not

the general use of MPE in law enforcement: *S and Marper v UK* (2009) 48 E.H.R.R. 50 §106.

(a) In Accordance with Law

9. The requirement that an interference be in accordance with law is summarised in *R. (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin), [2020] 1 W.L.R. 243 §76:

> *(1) The interference must be authorised by domestic law. This is a necessary condition for compatibility with the Convention but it is not a sufficient condition.*
> *(2) The domestic law must have a certain "quality". In particular it must be accessible.*
> *(3) The quality of law also entails that it must be reasonably foreseeable.*

10. In order for the law to have the *"quality of law"*, and in particular to be reasonably foreseeable, the law must confer discretion *"with sufficient clarity to give the individual adequate protection against arbitrary interference"*: *Weber and Saravia v Germany* (2008) 46 EHRR SE5 §94. There must be *"adequate and effective guarantees against abuse"*: *Weber* §106. The measure must not confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself: *In the matter of an application by Lorraine Gallagher for Judicial Review (Northern Ireland)* [2019] UKSC 3, [2020] A.C. 185 §17.

11. The *"quality of law"* requirement takes on a particular importance in the context of data protection (*S and Marper*, §103, emphasis added):

> *The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, mutatis mutandis, Z., cited above, § 95).* ***The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes****. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention and the preamble thereto and Principle 7 of Recommendation R(87)15 of the*

Committee of Ministers regulating the use of personal data in the police sector). ***The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse*** *(see notably Article 7 of the Data Protection Convention). The above considerations are* ***especially valid as regards the protection of special categories of more sensitive data****[.]*

(b) Necessary in a Democratic Society

12. The correct approach to determining whether an interference can be objectively justified requires (*Bank Mellat v HM Treasury* [2013] UKSC 39, [2014] A.C. 700, §20):

> *[…] an exacting analysis of the factual case advanced in defence of the measure, in order to determine*
> *(i) whether its objective is sufficiently important to justify the limitation of a fundamental right;*
> *(ii) whether it is rationally connected to the objective;*
> *(iii) whether a less intrusive measure could have been used; and*
> *(iv) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.*

13. That justification analysis will necessarily be fact sensitive: *R. (Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6, [2016] 1 W.L.R. 1505 §61.The burden is on the Secretary of State to justify an interference with Article 8 rights: *R (Quila) v Secretary of State for the Home Department* [2011] UKSC 45, [2012] 1 A.C. 621 §44.

C. MPE IN THIS CASE

14. It is common ground between the parties that the MPE practised in this case was unlawful. The Secretary of State accepts that the seizure, retention and extraction policies were not in accordance with the law for the purposes of Article 8, nor did the relevant conduct have a lawful basis for the purpose of the DPA 2018. This concession is made on the basis of the blanket and unpublished nature of these policies: **Detailed Grounds of Resistance §5 [CB/17/399]** (MA and KH Claim, 15 December 2021) (**"DGR"**); **Amended Detailed Grounds of Resistance §9.3-4, §10 [CB/10/183]** (HM Claim, 28 October 2021).

15. PI considers that these concessions are properly made. However, they do not reflect the totality of the unlawfulness of the arrangements.

16. PI makes these written submissions on the additional grounds under which it is alleged that Article 8 ECHR and the DPA 2018 have been breached. In particular, these submissions deal with the following issues:

    16.1. **The proportionality/strict necessity of MPE.** MPE involves a serious interference with privacy. Strong safeguards are therefore required.

    16.2. **The adequacy of the safeguards.** MPE involves such a serious interference with privacy that prior independent authorisation is required under the Convention for its use. In the absence of such a safeguard, MPE is neither necessary nor proportionate, nor does it have an adequate legal basis.

    16.3. **The cogency of the Secretary of State's justification**. PI submits that it is for the Court to determine whether the deployment of MPE in this case is justified; and the Secretary of State has the burden of satisfying the Court of that.

D. THE MPE IN THIS CASE REPESENTED A SERIOUS INTERFERENCE WITH THE RIGHT TO PRIVACY

17. MPE is a particularly serious infringement of the right to privacy, and as such requires cogent justification. In *Liberty* (at §200), the Divisional Court observed, citing the US case of *Riley v California* 573 US 373 (2014) (emphasis added):

> *That said, before we leave Riley, in our view it does provide* ***a helpful reminder of the powerful technology which now exists in (for example) mobile phones and therefore the need for the law to keep up, both in the interests of national security and the protection of the public, and in the interests of the civil liberties of individuals****. As Roberts CJ put it, at p.17:*
>
> > *Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.*
> > *[…]*
> > *The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record.*

> *Second, a cell phone's capacity allows just even one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier."*
> *[…]*
> *An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease … Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.*

(1) Submissions

18. The evidence demonstrates six propositions: MPE involves the extraction and retention of (1) highly sensitive data; (2) much of which will be irrelevant; (3) some will concern uninvolved third parties; (4) of limited reliability (where it is relevant); (5) which is then integrated with bulk datasets; (6) without effective safeguards. Accordingly, the extraction and retention policies involve a serious interference with privacy rights.

19. **First**, the data collected by MPE is highly sensitive. Mr Jupp describes the data obtained as "*communications data*" (**Jupp 1 ¶11**) **[CB/58/827],** sometimes called *metadata*. However, MPE also extracts *content data*, both of communications and other files or applications. MPE will obtain the content of messages and emails, as well as photos, videos or documents on the device, location data and social media data, amongst others: **Graham Wood 1 §48 [CB/64/905]**. This data can reveal information about the most sensitive parts of a person's life: their health and medical information, their personal relationships, family life, sex life or sexual orientation, everyday movements and activities, political and religious beliefs and their finances. Where the information acquired concerns "*a most intimate part of an individual's private life*", "*particularly serious reasons*" are required to justify the interference: *Lustig-Prean v UK* (2001) 31 E.H.R.R. 23 §82. This is especially so in respect of health data (*S and Marper* §72); or that which might reveal ethnic origin (*S and Marper* §76).

20. As Roberts CJ put it in *Riley*, to call a device a mobile phone is "*misleading shorthand… They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*" Therefore, MPE is uniquely intrusive: "*a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form – unless the phone is…*"

21. Further, as Roberts CJ pointed out, the possibility of 'cloud extraction' increases the extent of the interference further: "*The possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in* [an earlier case]".

22. MPE also permits the reconstruction, minute-by-minute, of a person's life: **Graham Wood 1 §45 [CB/64/904]**. The reconstruction of where a person goes and what they do is a serious interference with Article 8: *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France,* (Application nos. 48151/11 and 77769/13, 18 January 2018) §191.

23. Further, as **Graham Wood 1 §§42-55 [CB/64/902-909]** explains, the MPE software which is commercially available (and which the Secretary of State appears to use) allows the reconstruction and ordering of vast amounts of data from various sources and of various kinds automatically into categories, timelines and chronologies.

24. **Second,** most of the information extracted by MPE, including sensitive private information, will be irrelevant to the law enforcement task at hand.

25. There are limits to the extent to which data extraction can realistically be targeted within the process of MPE, as the Defendant's disclosure demonstrates: **Graham Wood 1 §§81-84 [CB/64/916-917]**:

    25.1. There is serious doubt whether the Defendant's kiosks are capable of meaningful selective extraction. On any view, it appears that no such facilities were available at the time MA and KH's phones were seized.

25.2. Prior to the adoption of the 30-day extraction policy, it appears that it would be left to the discretion of the reviewing officer to decide what to look at from the entire contents of the individual's phone.

25.3. Even after the shift to 30-day *"extraction"*, the amount of data being downloaded from each phone was vast: **Graham Wood 1 §83 [CB/64/916-917]**.

26. Much of the information extracted will therefore be sensitive, but irrelevant.

27. These points apply *even after* the Revised Strategy and July Revision (as defined in the DGR) came into effect. It is said that this resulted in *"significantly less data being extracted and reviewed"*: **DGR §23.3 [CB/17/409]**. However, as set out in **Graham Wood 1 §83 [CB/64/916-917]**, for the individual whose phone is subject to a 30-day extraction, the amount of information extracted is still likely to be vast, and of the most sensitive kind.

28. **Third**, it is not only the privacy rights of the individual whose phone is subject to extraction which are implicated by MPE (c.f. *S and Marper* §72): **Graham Wood 1 §87 [CB/64/919]**. Smartphones are likely to contain significant amounts of information about family, friends, and other contacts. MPE involves substantial collateral intrusion into privacy. That information will not be limited to communications data: it will include communications content (emails, texts) and photos, videos and documents stored on the phone, and any information accessible through social media applications.

29. **Fourth**, as **Graham Wood 1 §§89-92 [CB/64/920-921]** explains, there are serious concerns about the reliability of the data extracted by MPE. In particular:

29.1. It is apparent that the officers conducting the extractions were not accredited to ISO 17025, the relevant standard: **Graham Wood 1 §90 [CB/64/920]**.

29.2. The Secretary of State has provided no explanation of the training provided to her officers conducting MPE: **Graham Wood 1 §91 [CB/64/920]**.

29.3. The integrity of MPE data cannot be assumed. **Graham Wood 1 §92 [CB/64/921]** explains that MPE software and hardware can have exploitable security vulnerabilities which compromise the data extracted.

30. **Fifth,** the intrusion is not limited simply to the information extracted from the phone. MPE allows (as the Secretary of State appears to have done in this case) the overlaying of 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: **Graham Wood 1 §86 [CB/64/918-919]**. Such other information might come from other mobile phones, social media, other databases, physical surveillance, and communications data. The fruits of MPE can accordingly be integrated with other data to create an even more intrusive reconstruction of a person's life.

31. **Sixth,** as submitted in Section E below, in the absence of independent authorisation, there is a lack of oversight and effective safeguards.

32. **In conclusion,** the seriousness of the potential interferences requires a particularly cogent justification to be lawful. As submitted in Section F below, the Secretary of State has failed to substantiate the public benefit which is said to flow from these activities.

E. MPE IS IN ACCORDANCE WITH LAW ONLY WHERE PRIOR INDEPENDENT AUTHORISATION IS OBTAINED

33. As set out above, any interference with Article 8 must be in accordance with law. This imports a requirement of "*foreseeability*", and analysis of the safeguards in place. Accordingly, the question of whether the safeguards in place are adequate is relevant both to the question of whether the measure is provided for by law, and the "*closely related*" issue of necessity: *S and Marper* §99. The procedural safeguards required must be assessed in the round, by reference to the totality of safeguards applicable: *National Council of Civil Liberties* §160.

(1) Safeguards required by the ECHR

34. The case law sets out certain minimum safeguards in the case of data *interception* on a targeted basis (*Weber* §95), which comprise of "*the nature of*

the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed". Where the interference with privacy is significant and wide-ranging, the Convention requires a system of prior independent authorisation: *Big Brother Watch and others v UK* (Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021) §425. Particularly important factors are likely to include the extent to which interference is carried out in bulk, where the information obtained includes content as well as communications data or where the information obtained may be particularly sensitive (e.g. journalistic source material was held to be in this category in *Big Brother Watch*).

35. The importance of prior independent authorisation is not only a feature of the Convention case law. The common law has long recognised the importance of judicial warrants to justify serious interference with private property. Those principles are reflected in the Convention case law, and indeed the laws of other countries. Independent authorisation is a requirement designed to secure fair public administration and protects the public interest. As Roberts CJ put it in *Riley*:

> *"We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.*
>
> *Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency."*

36. Thus:

> *"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life,"… Our answer to the question of what police must do before*

searching a cell phone seized incident to an arrest is accordingly simple – get a warrant."

(2) Submissions

37. Here, prior independent authorisation is required. The Convention case law subjects warrantless searches to very strict limits (*Heino v Finland* (Application no. 56720/09, 15 February 2011, §40):

> *Notwithstanding the margin of appreciation which the Court recognises the Contracting States have in this sphere, it must be particularly vigilant where, as in the present case, the authorities are empowered under national law to order and effect searches without a judicial warrant. If individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 8, a legal framework and very strict limits on such powers are called for[.]*

38. This MPE regime does require prior independent authorisation before a search takes place. The extent and degree of intrusion is analogous to the types of case identified in *Big Brother Watch* where such authorisation was held to be required by the Convention.

39. **First**, without prior independent authorisation, it is extremely difficult to guard against arbitrariness. The practical reality of MPE is to give the searching officer *"unfettered discretion to assess the expediency and scope of the search and seizure"* and *"the officer conducting the search [is] competent to assess alone whether or not to conduct the search and to what extent"* (*Heino* §42). Similarly, as in *Särgava v Estonia* (Application no. 698/19, 16 November 2021) (§106, a case of MPE which did involve a warrant) *"the decision of whether to conduct a keyword-based search (or use any other method of sifting) as well as the choice of relevant keywords was left entirely up to the investigative authorities."* Such a power could be consistent with the ECHR only if subject to independent authorisation delimiting its scope. In *Ivashchenko v Russia* (Application no. 61064/10, 13 Februrary 2018, §§81-95), the Court held that the extraction of electronic data from a laptop at the border as part of a customs sampling exercise (that is, where there was no suspicion of breach of customs rules by the particular entrant) lacked the required safeguards to be in accordance with law. In short, this is a law enforcement power where abuse is *"potentially so easy in individual cases"* that independent authorisation is required: *Kennedy v UK* (2011) 52 E.H.R.R. 4 §167.

40. **Second,** such a requirement accords with the approach of the ECHR to house searches:

40.1. In *Funke v France* (1993) 16 E.H.R.R. 297, a house search was conducted without a warrant, under a broad power. The Court held (§57, emphasis added):

> *[T]he customs authorities had very **wide powers**; in particular, they had exclusive competence to assess the expediency, number, length and scale of inspections. Above all, **in the absence of any requirement of a judicial warrant** the restrictions and conditions provided for in law, which were emphasised by the government, appear too lax and full of loopholes for the interferences in the applicant's right to have been strictly proportionate to the legitimate aim pursued.*

40.2. In *Niemietz v Germany* (1993) 16 E.H.R.R. 97, concerning a search of a lawyer's office pursuant to a warrant, part of the basis for the finding that the search was not necessary in a democratic society was that "*the warrant was drawn in broad terms, in that it ordered a search for and seizure of 'documents,' without any limitation*".

40.3. In *Imakayeva v. Russia* (Application No. 7615/02, 9 November 2006), no search warrant was obtained either before or after a house search on an urgent basis, and no details were given to the occupant about what was being sought. The Court held (emphasis added):

> *The Government's reference to the Suppression of Terrorism Act cannot replace an **individual authorisation of a search, delimiting its object and scope**, and drawn up in accordance with the relevant legal provisions either beforehand or afterwards.*

40.4. Accordingly, where wide powers of search are allocated, there will be sufficient safeguards only if the exercise of those powers is constrained by the need for independent authorisation which delimits the object and scope of the search.

F. THE SECRETARY OF STATE HAS FAILED TO JUSTIFY THE INTERFERENCE

41. In *R (Miller) v College of Policing* [2021] EWCA Civ 1926 §104, the Court of Appeal held that whether the proportionality test has been satisfied is ultimately a question for the Court:

> *[T]he court is obliged to consider for itself whether any less intrusive measure could have been used without unacceptably compromising the achievement of the legitimate aim. I accept of course that key parts of the Guidance derived from the views of "sources which should command great respect." […] But this does not obviate the need for the judge to consider the issue for himself.*

42. PI submits that the Secretary of State has not discharged her burden of justification, and so the Court cannot be satisfied that the deployment of MPE through the extraction and retention policies in this case was proportionate.

43. The routine and untargeted use of MPE rarely produced much of value and certainly nothing that could not have been obtained from a lawful approach involving targeted and pre-authorised searches:

    43.1. Under the "*initial Project Sunshine approach*", the identification of associations across all data seems to have led to only 100 leads and no operational activity: **Davison §9 [CB/62/872].**

    43.2. Under the "*second approach*", which saw the team enrich all the data then attempt to establish activity from that position, the amount of data extracted was "*difficult to work with*" and generated no leads at all: **Davison §10 [CB/62/872-873]**.

44. In short, in the absence of proper safeguards which could ensure MPE was used effectively, the Secretary of State's own evidence is that her approach led to large amounts of wasted effort and unnecessary and serious interference with privacy.

G. CONCLUSION

45. For the above reasons, it is respectfully submitted that:

    45.1. MPE represents a serious interference with privacy. Cogent evidence will be required before such an interference can be justified.

    45.2. MPE is only "*in accordance with law*" where it is subject to prior independent authorisation.

45.3. The Secretary of State has failed to discharge her burden of showing that the extraction and retention policies were strictly necessary and proportionate.

BEN JAFFEY QC

TOM LOWENTHAL

Blackstone Chambers

10 January 2021