
SUBMISSION TO THE INFORMATION COMMISSIONER

–

REQUEST FOR ASSESSMENT OF PROCESSING OPERATIONS BY THE SECRETARY OF STATE FOR THE HOME DEPARTMENT (“HOME OFFICE”)

I. Introduction and Purpose of this Submission

1. Privacy International (“**PI**”) is a non-profit, non-governmental organisation based in London, that works globally at the intersection of modern technologies and rights. Established in 1990, PI undertakes research, litigation and advocacy to build a better future where technologies, laws and policies contain modern safeguards to protect people and their data from exploitation. As such, PI has statutory objectives which are in the public interest and is active in the field of the protection of data subjects’ rights and freedoms. This submission relates to PI’s ongoing work on the protection of migrant communities and of their data. See Annex A for more information on PI’s work in the migration context.
2. Through this submission, PI raises as a matter of concern the policy and practice of the Secretary of State for the Home Department (thereafter “**Home Office**”) in the collection, processing and sharing of location data of migrants released on immigration bail via the imposition of electronic monitoring (“**EM**”) through GPS ankle tags (“**GPS tags**”). We provide the Information Commissioner’s Office (“**ICO**”) with technical evidence and legal analysis in order to assist him in assessing the data controller’s compliance with data protection legislation, in particular the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “**UK GDPR**”) and the Data Protection Act 2018 (the “**DPA 2018**”).
3. We make this submission to challenge the Home Office’s EM policy and practice in a systemic way, rather than by representing individual data subjects. This is in particular because individual complaints would only challenge the imposition of EM on the complainant, whereas PI considers that the entire policy deserves investigation and challenge.
4. GPS tags are ankle tags that monitor the location of an individual using satellite and mobile technology, collecting location data referred to as “trail data” at certain intervals. Trail data is particularly (1) voluminous, (2) sensitive, (3) granular and (4) open to misinterpretation. GPS tags also provide the ability to

track an individual's location in real time, in addition to reviewing their location history.

5. Several private third parties are involved. The company Capita runs the Electronic Monitoring Services (“**EMS**”), contracted by the Ministry of Justice (“**MoJ**”). GPS tags are provided by G4S and communicate location data using Telefonica's mobile network to Airbus, who process and verify the data and present the information to EMS. EMS then process and retain the data, and share it in bulk with the Home Office and other government agencies when a breach of bail conditions is notified, and in other circumstances detailed further in this submission.
6. It is mandatory for Foreign National Offenders to be subject to EM when released on immigration bail. However, anyone subject to immigration control, including asylum seekers in the course of their application or other proceedings, can be subject to GPS tagging. There is no time limit for how long an individual must wear a tag.
7. This form of monitoring is a seismic change in the surveillance and control of migrants in the UK. PI is only aware of a similar practice occurring in the United States.¹ The data-intensive and intrusive nature of this practice merits close consideration by the ICO, particularly in light of recent reports by the National Audit Office (“**NAO**”)² and the Independent Chief of Borders and Immigration (“**ICIBI**”)³ raising concerns about the EM system, and in light of the Home Office's trail record of excessive data processing activities, especially with regards to migrants' data.⁴
8. For the reasons set out below, PI submits that the Home Office's EM policy and practice breaches the UK GDPR and DPA 2018 in a number of ways. In summary:
 - (a) 24/7 GPS monitoring is excessive and goes beyond the aims of the legislation. It falls outside the reasonable expectations of data subjects.
 - (b) The ability to review all trail data in the event of a breach of bail conditions alert is not necessary for nor proportionate to the purpose of data processing.
 - (c) There is no lawful basis to use trail data to assess individuals' Article 8 representations and further submissions.

¹ Danielle Silva, 'GPS tracking of immigrants in ICE raids troubles advocates', NBC News (15 August 2019), <https://www.nbcnews.com/news/us-news/gps-tracking-immigrants-ice-raids-troubles-advocates-n1042846>.

² National Audit Office, 'Electronic monitoring – a progress update' (8 June 2022), <https://www.nao.org.uk/wp-content/uploads/2022/01/Electronic-monitoring-a-progress-update.pdf>.

³ ICIBI, 'An inspection of the global positioning system (GPS) electronic monitoring of foreign national offenders' (March – April 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088880/An_inspection_of_the_global_positioning_system_GPS_electronic_monitoring_of_foreign_national_offenders_March_April_2022.pdf.

⁴ See for example *HM and (1) MA and (2) KH v Secretary of State for the Home Department* [2022] EWHC 695 (Admin), reported on by Diane Taylor, 'Home Office illegally seized phones of 2,000 asylum seekers, court rules' (The Guardian, 25 March 2022), <https://www.theguardian.com/uk-news/2022/mar/25/home-office-illegally-seized-asylum-seekers-phones>.

- (d) No transparency is provided to data subjects as to the nature and extent of data collection and processing.
 - (e) The various uses and re-uses of location data do not comply with the purpose limitation principle.
 - (f) GPS location data can be inaccurate and quality failures can produce inaccurate data, in violation of the accuracy principle.
 - (g) This form of surveillance poses a considerable risk to the fundamental rights and freedoms of tagged individuals.
 - (h) The scheme lacks safeguards.
9. This submission will first provide background on the use of GPS tags by the Home Office, after which it will set out in detail the legal framework and concerns identified.

II. Background – The Use of Satellite Tracking by the Home Office

10. PI was alerted to the Home Office use of electronic monitoring in immigration bail by various migrant rights organisations, who first denounced this practice in March 2021.⁵ While the Home Office had been electronically monitoring people on immigration bail since 2004 under the Asylum and Immigration (Treatment of Claimants) Act 2004 s.36, a new policy was introduced in January 2021 to replace existing radio frequency tags with GPS tags (the previous version 6 of the policy from November 2020 first referenced the transition).⁶ A new “mandatory duty” to impose electronic monitoring on people subject to deportation proceedings was also introduced in legislation that came into force in August 2021.⁷
11. The present submission has been informed by obtaining Data Protection Impact Assessments (“**DPIA**”) from the Home Office through Freedom of Information requests. We obtained two DPIAs, one completed on 22 September 2020 (the “**2020 DPIA**”) and one completed on 19 August 2021 (the “**2021 DPIA**”). Both are exhibited to this submission (Exhibits 1 and 2). PI is aware that an equality impact assessment performed by the Home Office exists,⁸ however we have not had sight of it.
12. In this section we briefly explain how immigration bail works and the legislation that enables it, the introduction of the mandatory electronic monitoring duty, and then summarise who is in practice subject to GPS tracking.

A. Immigration Bail and Electronic Monitoring

13. Immigration bail can be granted to individuals who are detained by the Home Office on immigration matters, either by the Home Office itself or by the First Tier

⁵ Bail for Immigration Detainees (“**BID**”), ‘**BID**’s Briefing on Electronic Monitoring’ (24 March 2021), <https://www.biduk.org/articles/805-bid-s-briefing-on-electronic-monitoring>.

⁶ Home Office, ‘Immigration bail policy Version 7’ (January 2021).

⁷ Immigration Act 2016, Schedule 10, paragraph 2(3).

⁸ Reference is made to such an assessment in the ICIBI’s inspection report (n 3), §1.17.

Tribunal (Immigration and Asylum Chamber) (“FTT”). Immigration bail is usually granted subject to certain conditions, listed in paragraph 2(1) of Schedule 10 of the Immigration Act 2016 (“IA 2016”), such as restrictions on individuals’ occupation, curfews, or conditions on where they can go (called “inclusion or exclusion zones”). Pursuant to paragraph 2(1) of Schedule 10, the Home Office must impose at least one immigration bail condition on those subject to deportation proceedings or under a deportation order. Electronic monitoring is one of the potential immigration bail conditions the Home Office can impose (paragraph 2(1)(e)).

B. The mandatory Electronic Monitoring duty

14. Schedule 10 of the IA 2016, Part 1 paragraphs 2(2) and 2(3) place a mandatory duty on the Secretary of State to electronically monitor those on immigration bail who could be detained because they are liable to deportation, commenced on 31 August 2021 (the “**mandatory EM duty**”). The mandatory EM duty applies to everyone who is liable to be deported, at any point within the deportation process, from the point at which the Home Office considers whether deportation should apply, to those subject to a signed deportation order, even where the order is not enforceable owing to a legal or practical barrier.
15. There are two exemptions to the mandatory EM duty. Schedule 10 provides exemptions for people who are under 18, and for mentally unwell people who are released on to immigration bail following detention under sections 37 and 41 of the Mental Health Act 1983 whilst they remain subject to a supervision order. There are also two more general exceptions: where it would be contrary to a person’s Convention rights and where it would be impractical (paragraph 2(5)).
16. Only the Home Office has the power to decide whether an exemption or an exception applies. The FTT cannot impose an EM condition where the Home Office considers that the condition would be contrary to an individual’s Convention rights or impractical (paragraphs 2(7) and 2(8) of Schedule 10). However, if the Home Office decides an exemption or exception does not apply, the FTT cannot override that decision, nor review it. Thus, so far as the imposition of an EM bail condition on people deemed to fit the deportation criteria is concerned, the FTT has no jurisdiction over whether an exemption applies and no discretion as to whether EM should be imposed where the Home Office has decided that it should be.
17. Schedule 10 makes no reference to the type of technology to be used for the EM condition. The introduction of GPS tags and the proposal to use ‘Non-Fitted Devices’, i.e. smartwatches (as indicated in the 2021 DPIA), are therefore policy decisions.

C. Who is subject to GPS monitoring?

18. From January 2021, those who were subject to EM but on Radio Frequency tagging were transferred to monitoring by GPS, following introduction of Version

7 of the Home Office's Immigration bail policy. The latest version of this policy is version 12, published on 28 June 2022.⁹

19. On 31 August 2021, the mandatory EM duty was commenced, as explained above, and from this date the Home Office began tagging people upon release from detention where they fitted the mandatory EM criteria. The Home Office announced that from 31 January 2022, all those already on immigration bail and subject to either deportation proceedings or a deportation order would be made subject to a review of an individual circumstances, and devices issued to them. However, FOI data obtained by BID indicated that by 20th March 2022 no individuals who were already at liberty in the community had yet been tagged.¹⁰
20. In summary, this means:
 - (a) All those subject to EM prior to January 2021 were transferred to GPS tags from January 2021.
 - (b) All those subject to deportation proceedings or a deportation order were considered for fitting with a GPS tag from 31 August 2021 – unless an exemption was applied.
21. The 2020 DPIA anticipated that following the introduction of the mandatory EM duty, the number of tag wearers would rise from 280 to approximately 4,500. The anticipated rise is yet perhaps a conservative estimate. According to the charity Bail for Immigration Detainees (“**BID**”), data from 2020 shows that *“[a]t the end of March 2020 there were 194 people on immigration bail subject to an electronic monitoring condition. There are 9,987 people facing deportation living in the community – meaning that an additional 9,793 people could become subject to electronic monitoring.”*¹¹ More recent data suggests that 11,358 people currently living in the community are facing deportation.¹²
22. In response to BID's FOI request, the Home Office states that 1,649 people released from immigration detention were made subject to an EM condition between 31 August 2021 and 20 March 2022. It also states that between 31 August 2021 and 27 March 2022, 3 persons who were made subject to an EM condition have subsequently had the tag removed because the Home Office decided that one of the exceptions applies.¹³
23. The reason for the discrepancy between the number of people who are subject to the duty and those who are actually made subject to an EM condition is unclear, but unlikely to be that the Home Office has applied an exemption to

⁹ Home Office, 'Immigration bail policy Version 12' (28 June 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1084425/Immigration_bail.pdf.

¹⁰ BID, FOI response received Wednesday 4 May 2022 reference number 68882 (Exhibit 3).

¹¹ BID (n 5).

¹² Gov.uk, 'Immigration Enforcement data: Q1 2022' (26 May 2022), <https://www.gov.uk/government/publications/immigration-enforcement-data-q1-2022>.

¹³ BID (n 10) (Exhibit 3).

everyone in between. In their FOI request, BID requested numbers on how many people subject to deportation proceedings were released from detention since 31 August 2021 and weren't tagged because the Home Office applied an exception – the Home Office refused to answer as to do so would exceed the appropriate limit of £600 specified in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

24. The discrepancy might be attributable to low device availability: the Immigration bail policy states that *“There will be fewer devices available than the number of individuals subject to the duty.”*¹⁴ A factor that may influence the availability of GPS tags is the absence of a time limit to wearing a tag, such that tagging can last a considerable amount of time while deportation proceedings are ongoing.
25. We note that the Home Office has recently expanded the EM system so that some people arriving on small boats are also being subject to an EM tagging condition: *“From 15 June 2022, a 12-month pilot will operate and will test whether electronic monitoring (EM) is an effective means by which to improve and maintain regular contact with asylum claimants who arrive in the UK via unnecessary and dangerous routes and more effectively progress their claims toward conclusion.”*¹⁵ This marks a significant widening of the policy to include asylum seeker arrivals, who are not subject to formal deportation proceedings.

III. The Technology and the EM System

26. “Traditional” ankle tagging, both in criminal justice and immigration enforcement contexts, uses “Radio Frequency” technology. New devices use GPS technology, although they can be fitted with dual capability: *“If a curfew condition is required, or to extend the life of the GPS device battery, or where limited GPS signal is available, the GPS device (tag) may also use radio frequency technology whilst in a property where a home monitoring unit is installed.”*¹⁶
27. In this section we describe the differences between Radio Frequency and GPS technologies, and explain how these impact the types and amounts of data collected by the devices. We then describe the Home Office’s plans with regards to the roll out of smart watches.
28. We note that the documents we have reviewed do not specify which make and model of devices the Home Office uses. Our analysis is informed by testimonies from tagged individuals and by the expertise of our team of technologists, who have performed real-life testing of two different types of GPS tags, none of which we are aware are the ones that the Home Office actually uses. Their general functioning is most likely similar and any differences would not be of a nature to

¹⁴ Home Office, ‘Immigration bail policy Version 12’ (n 9).

¹⁵ Home Office, ‘Immigration bail conditions: Electronic monitoring (EM) expansion pilot Version 1.0’ (15 June 2022),

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082956/Immigration_bail_conditions_-_Electronic_Monitoring_EM_Expansion_pilot.pdf.

¹⁶ Home Office, ‘Immigration bail policy Version 12’ (n 9).

materially impact our submissions. Findings from this research will be referred to throughout these submissions.

A. Radio Frequency Tags – How they work

29. Radio frequency tags rely on two elements – a base station usually located in the subject’s house, and a tag attached to the individual. The base station polls the tag occasionally over a specific radio band to detect if it is within range. If the tag fails to report (or the signal is below a threshold), it will raise an alert, and a number of alerts over a timeframe will prompt the tagging authority’s control centre to phone the tag wearer on their landline. If this fails, the control centre may ask law enforcement to visit the address and ascertain if the wearer has absconded.
30. As noted in the Consultation on the Future Direction of the Electronic Monitoring Service¹⁷ by the Scottish Government, the information the Radio Frequency tag sends the monitoring unit provides information about a person’s movements within an agreed location. The locational information is essentially binary: it can only indicate whether the tag is present or is not present within the range of the home monitoring unit. The tag only “communicates” with the monitoring unit and it is the monitoring unit that sends the information back to the monitoring company. The two pieces of equipment therefore need to be within range of each other for locational information (such as whether the tag is present) or other information (such as whether the tag has been tampered with) to be registered by the monitoring unit.
31. The home monitoring unit will usually have a signal detecting range that can be set to cover the size of “most domestic dwellings”.¹⁸ This means that the main capability and purpose of a radio frequency tag is to enforce curfew conditions, such as that an individual remain at home from 7pm to 7am.

B. GPS Tags – How they work

32. GPS tags, on the other hand, only consist of the tag attached to the individual and a GPS navigation chip in the tag, that communicates directly with a control centre through a mobile network (either GPRS or 4G). The tag also contains a SIM card (or equivalent) to authenticate it to the network.
33. GPS tags require no base station (although the Home Office can still decide to place a home monitoring unit in the subject’s home if the device has dual radio frequency/GPS capability). The Immigration Bail policy also refers to the issuing of mobile phones, stating that “*Where the person is not issued with a Home Monitoring Unit a mobile phone will be issued to the person to allow contact to and from the EM supplier.*”¹⁹

¹⁷ (September 2013), <https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf>.

¹⁸ Ibid.

¹⁹ Home Office, ‘Immigration bail policy Version 12’ (n 9).

34. GPS (Global Positioning Service) is a space-based navigation satellite system that provides location and time information in all weather, anywhere on or near the earth. Devices equipped with GPS technology work by receiving location signals from at least 4 different satellites equipped with radio transmitters.
35. In the case of GPS tags, location data is communicated through the mobile phone network to a central computer at a monitoring centre, in real time. The monitoring centre may then use a mapping service to plot locations and times.
36. When GPS is unavailable or weak, GPS devices track location using GPS signals backed up by mobile signals.²⁰
37. Whilst GPS tags work by receiving location signals from satellites, they then communicate location data via a mobile phone network to a case management system.²¹ The SIM card or equivalent will authenticate it to the network. In 2014, the Ministry of Justice awarded a contract to Telefonica²² in relation to “network services” (Global System for Mobile Communications) for electronic monitoring. Thus, the SIM card in the tag will communicate using the mobile network. The mobile telephone network is, by design, also a tracking network. To try and maintain a signal whilst moving, as well as to connect to the “best” tower, the SIM card will send constant “pings” to towers in their vicinity, meaning the position can be easily triangulated. In several countries around the world, telecommunications operators are legally compelled to store these records. This means that the communications data generated by the tags is not only being shared with the Electronic Monitoring Service, Home Office, Ministry of Justice, and Law Enforcement, it is also being processed and may be retained by the relevant telecommunications operator.
38. Tags can collect location data at different frequency or intervals. For example, the buddi ST3 Smart Tag 4 indicates that “*Intervals can be defined, or a real-time request made*”.²³ Another device allows setting intervals at 15 minutes, 30 minutes or an hour.²⁴ Which intervals are selected naturally has a significant impact on the amount and granularity of data collected. If only real-time requests are made instead of interval tracking, GPS location is only collected in response to a specific location request.

²⁰ Anthea Hucklesby and Ella Holdsworth, ‘Electronic Monitoring in England and Wales’ (May 2016), Centre for Criminal Justice Studies, University of Leeds,

http://www.antonioacasella.eu/nume/Hucklesby_Holdsworth_2016.pdf.

²¹ Ministry of Justice, ‘Process evaluation of the Global Positioning System (GPS) Electronic Monitoring Pilot’ (2019),

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779199/gps-location-monitoring-pilot-process-evaluation.pdf

²² Ted-tenders electronic daily, ‘United Kingdom-London: Tracing system services’,

<https://ted.europa.eu/udl?uri=TED:NOTICE:284886-2014:TEXT:EN:HTML>.

²³ Manuals+, ‘buddi ST3 Smart Tag 4 ERA Monitoring System Instruction Manual’ (7 January 2022),

<https://manuals.plus/buddi/st3-smart-tag-4-era-monitoring-system-manual#axzz7PgoPr5dw>.

²⁴ Manualslib, Link-2 User manual, <https://www.manualslib.com/manual/587617/Lowrance-Link-2.html?page=54>.

39. GPS tags rely on chargeable batteries. GPS technology is much more battery intensive than radio frequency technology, therefore GPS tags are larger to accommodate for a larger battery and need to be charged more often. The design of the tagging system also contributes to the drain on battery life, as live location tracking is much more draining than interval tracking. The Reform report ‘Cutting crime: the role of tagging in offender management’ dated September 2015 stated that:

“1.6.1 As pressure rises to ensure GPS devices run more and more concurrent capabilities, the battery life reduces significantly. In addition, increasing volumes of data transfer drains the battery life of a device. Continuously tracking offenders to provide real-time intelligence requires much more frequent communications between the electronic anklet and central portal. Interview for this report suggest that this type of tracking can reduce a tag’s battery life to just a few hours...”

40. EMS state in their “tagging handbook” published on the government’s website that GPS tagging devices need to be charged for an hour a day.²⁵ A handbook on GPS tagging from the Ministry of Justice, however, suggests that fully charging a tag usually takes “*at least 2 hours every day*”.²⁶ This poor battery performance and frequent charging needs often have serious implications for the accuracy of breach reporting and the proportionality of GPS tracking – this will be further explored in section IV.D. (Accuracy) below.

C. Intrusiveness of data collected by GPS tags

41. The main type of data collected is “trail data”, a term used to refer to the location history of the individual wearing the tag. Trail data is particularly (1) voluminous, (2) sensitive, (3) granular and (4) open to interpretation.
42. **First**, the volume of data collected through live location tracking is enormous. In the US Supreme Court judgment of *United States v. Jones*,²⁷ law enforcement installed a GPS tracking device to the undercarriage of the Jeep of a suspect and tracked the vehicle’s movements over the next 28 days. Justice Scalia, delivering the opinion of the Court noted the volume of data that this period generated stating:

“By means of signals from multiple satellites, the device established the vehicle’s location within 50 to 100 feet and communicated that location by

²⁵ EMS, ‘Tagging – Everything you need to know about being tagged’, <https://www.gov.uk/government/publications/gps-location-monitoring>.

²⁶ Ministry of Justice, ‘Electronic Monitoring GPS Satellite Tagging handbook’, <https://www.bl.uk/britishlibrary/~media/bl/global/social-welfare/pdfs/non-secure/e//e/electronic-monitoring-global-positioning-system-annex-n-gps-handbook.pdf> – this handbook seems to date back to 2019, as it refers to the Ministry of Justice GPS pilot dated 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814219/processevaluation-gps.pdf).

²⁷ Supreme Court of the United States. *United States v Jones*. 10-1259, 23 January 2012, <https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf>.

cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.” [emphasis added]

43. While a vehicle only moves at certain times a day, and only on certain days, an individual is in nearly constant movement – hence the volume and granularity of data inevitably increases considerably when the tag is attached to a person. The number of pages of data generated by an ankle tag over a 4-week period is therefore likely way above 2,000 pages.
44. It is unclear what intervals the Home Office has set for location data collection. Our technologists tested GPS tags with different intervals, rendered the data in Excel spreadsheets, resulting in varying amounts of data produced:
 - (a) 2 minute intervals led to **1,000 data entries** in an Excel spreadsheet over a 2-day period (note that this specific tag does not ping the network if the tag doesn't move, therefore there can be long periods of time where no data is collected e.g. when the subject is sleeping or working at their desk) – see Figure 1 below.
 - (b) 30 second intervals led to approximately **30,000 entries** over a 2.5-month period (same as above, the tag doesn't ping if it doesn't move, and our technologist did not wear the tag constantly over the 2.5 months) – see Figure 2 below.

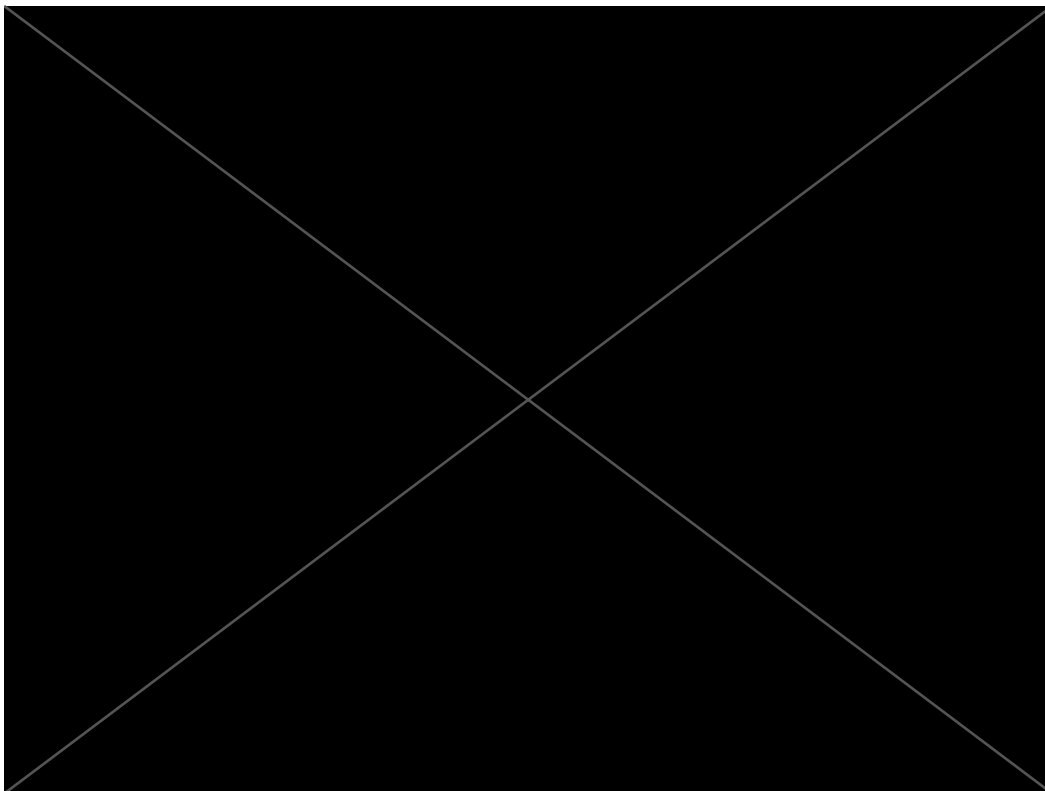


Figure 1 – Excerpt from spreadsheet data for 2-minute interval P monitoring

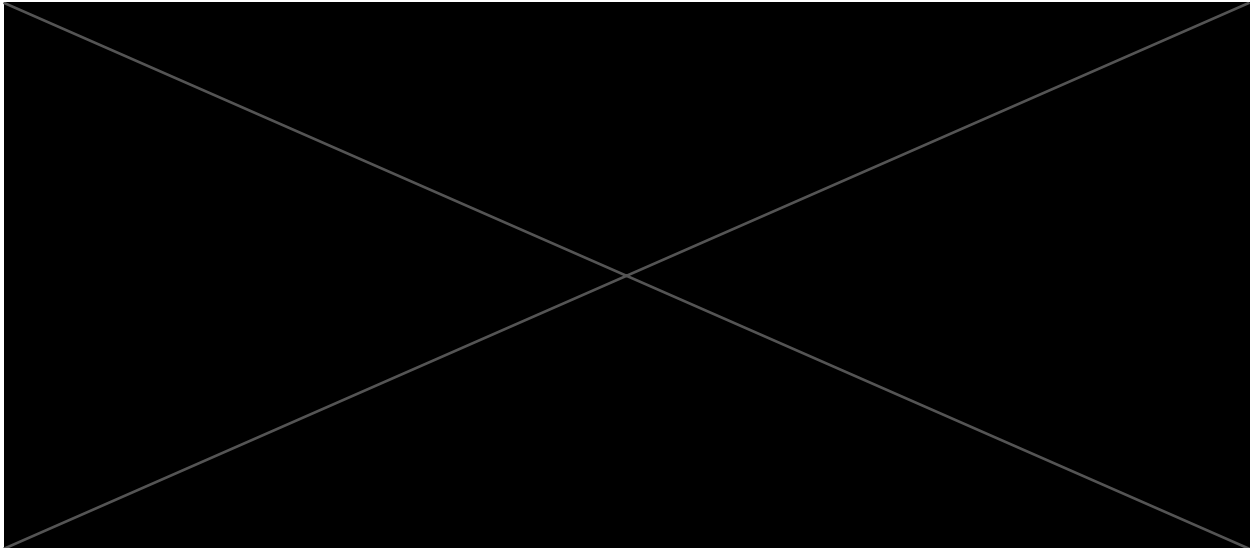


Figure 2 – Excerpt from spreadsheet data for 30-second interval GPS monitoring

45. **Second**, trail data is highly sensitive – it provides deep insight into intimate details of an individual’s life, revealing a comprehensive picture of everyday habits and movements, permanent or temporary places of residence, hobbies and other activities, social relationships, political, religious or philosophical interests, health concerns, consumption patterns, etc. When and how a person moves around can therefore reveal a considerable amount of information about their life and personality.
46. Again in the US Supreme Court case of *United States v. Jones*, Justice Sotomayor’s concurring opinion reaffirms the intrusive nature of GPS monitoring:
- “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations. See, e.g., People v. Weaver, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) (“Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on”).”*
47. The intrusiveness of location data was also affirmed by the Grand Chamber of the Court of Justice of the European Union (“**CJEU**”) in its decision of 6 October 2020 in *La Quadrature du Net and Others v Premier ministre and Others*:
- “That conclusion is all the more justified since traffic and **location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health**, given that such data moreover enjoys special protection under EU law. **Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life,***

permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 27, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 99).²⁸ [emphases added]

48. Trail data can therefore contain special categories data as defined in Article 9(1) UK GDPR. Indeed, the following examples of location data can reveal:
- (a) racial or ethnic origin – trips to certain specialised ethnic shops and community centres
 - (b) political opinions – attendance at certain rallies, protests, meeting centres
 - (c) religious or philosophical beliefs – trips to a church, mosque, synagogue or other religious or philosophical meeting centre
 - (d) trade union membership – attendance at rallies or trade union headquarters
 - (e) data concerning health – trips to specialised surgeries or health centres
 - (f) data concerning a natural person’s sex life or sexual orientation – trips to gay bars or attendance at gay pride
49. **Third**, trail data is particularly granular – the ability to track someone’s movements every minute of the day and night, every single day, provides information not just of a general nature about sensitive aspects of someone’s life, but also provides extremely precise insights into these sensitive aspects. For example, data might indicate that an individual holds certain religious beliefs – such as regular trips to a place of worship. This information is made much more granular and invasive if location data shows that such trips happen every day or multiple times a day, perhaps at late hours of the night – providing an indication as to the intensity of the individual’s beliefs. Knowing the precise timings of someone’s whereabouts provides profound insight into their private and intimate life.
50. Screenshots from the monitoring platform recording one of our technologists’ location data during their research shows the very high number of location points one can obtain from just 16 hours of monitoring:

²⁸ Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791, para 117.

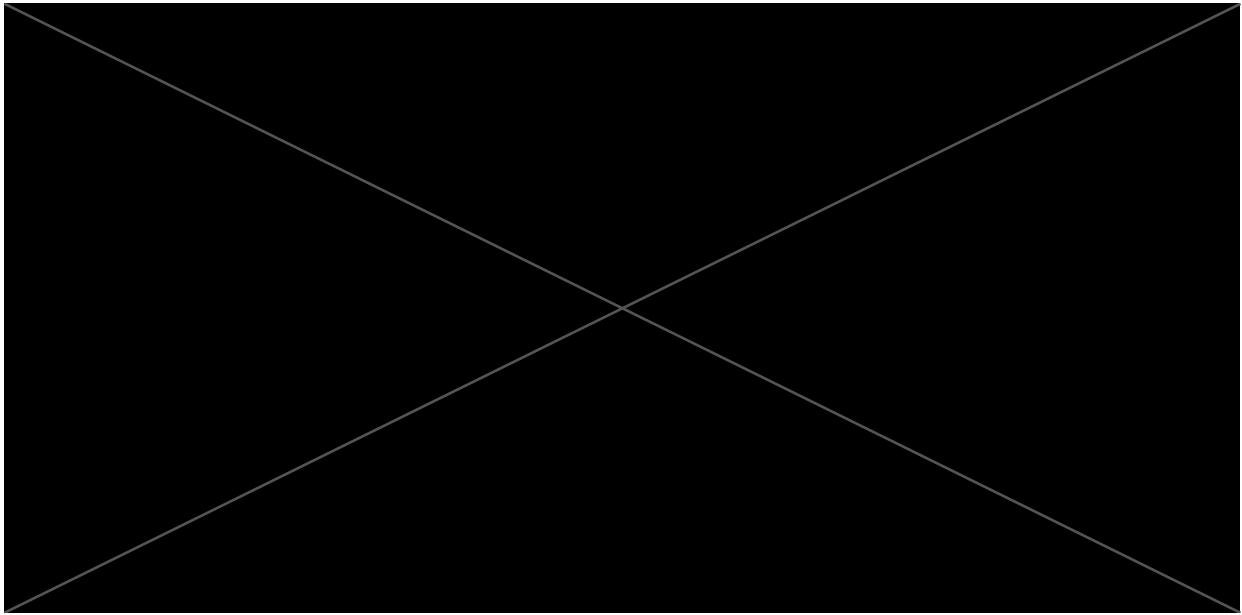


Figure 3 – Screenshot of monitoring platform recording our technologist's GPS location over 16 hours

51. **Finally**, trail data can be interpreted in many different ways to draw conclusions about an individual's lifestyle – that is, the meaning or significance of a particular movement or activity will likely be interpreted in widely divergent ways by different people. In an immigration enforcement context, this can potentially lead to significant decisions being taken on the basis of subjective interpretations of an individual's movements and activities. Combined with issues of accuracy, this can lead the Home Office to make fundamentally wrong assumptions about an individual's movements and activities.
52. An example of location history collected through a GPS tag over a 1-week period is provided at Figure 4 below, and over a 2-day period at Figure 5 below. By clicking on the various pins on the map, one can figure out the precise times at which the tagged individual was in certain locations, how long they remained there, etc. For example, from Figure 5 one can interpret that the individual:

[REDACTED]

53. Any of these observations may come from misinterpretation of the data. For example, [REDACTED]

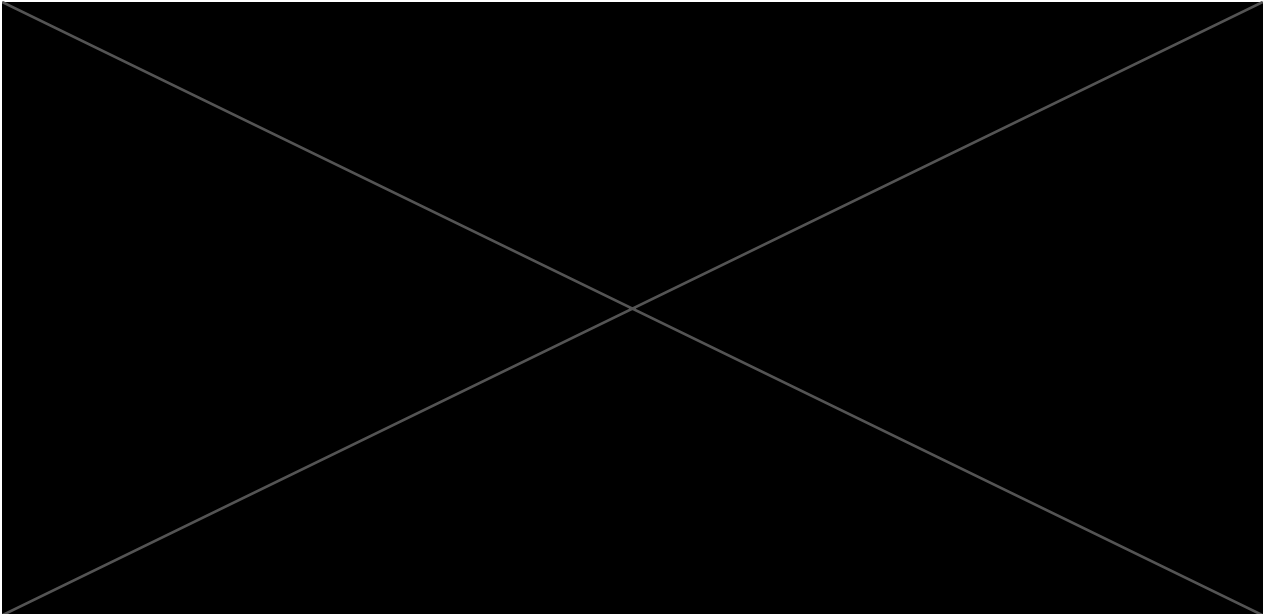


Figure 4 – Screenshot of monitoring platform recording our technologist’s GPS location over a 1-week period

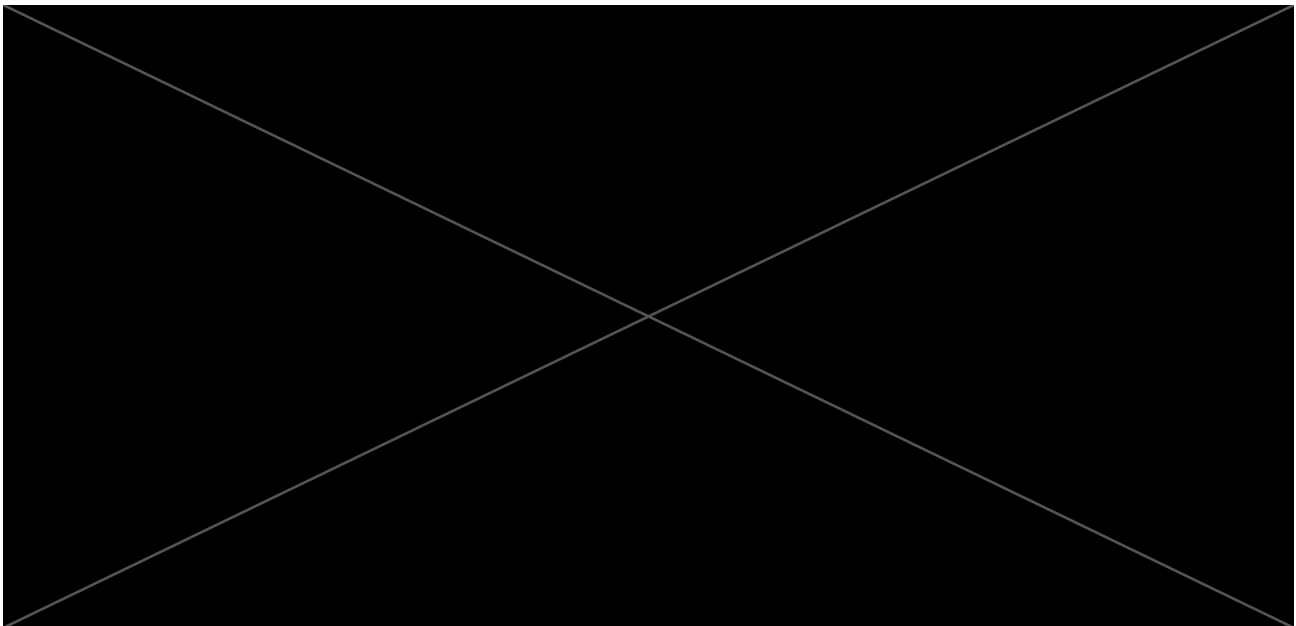


Figure 5 – Screenshot of monitoring platform recording our technologist’s GPS location over a 2-day period, with one pin clicked

D. How the system works – Third parties and Home Office access to data

Third parties

54. Under the current system, the Home Office does not run the tagging service itself. This is outsourced to Electronic Monitoring Services (“EMS”), an entity set up by the Ministry of Justice’s HM Prison and Probation Service (“HMPPS”), who integrates services provided by various companies. According to a report by the

National Audit Office on Electronic Monitoring, prior to 2016, “HMPPS acted as an ‘integrator’ to coordinate work across the four suppliers. It took on this role in 2016 following a dispute with Capita, who previously acted as integrator”.²⁹ Capita still runs the “live service monitoring centre, case management, and fit[s] tags to offenders”.³⁰ Service contracts therefore only exist between the Ministry of Justice and these companies, while the Home Office uses this existing service for its own purposes. On 7 April 2022 we requested (under the FOIA 2000) to see any documents in place between the Ministry of Justice and the Home Office, but the Home Office’s response is still long overdue.³¹

55. To procure the tags, HMPPS designed a single end-to-end service split into four Lots, awarded respectively to:

- (a) the monitoring service – Capita, awarded a contract valued at £229,000,000 in 2017,³² renewed in 2020 for £114,000,000³³;
- (b) the monitoring and mapping software – G4S monitoring technologies, awarded a contract valued between £29,000,000 and £53,000,000³⁴ in 2018 as well as a £22,000,000 contract in May 2022³⁵;
- (c) the monitoring hardware – Airbus Defence and Space Limited, awarded a contract valued at £10,400,000 in 2019³⁶; and
- (d) the network – Telefonica, awarded a contract for £3,200,000 in 2019³⁷, and another that expires in 2024 (as indicated in the NAO report³⁸).³⁹

56. The following figure from the National Audit Office report illustrates the roles and contracting relationships of the various parties:

²⁹ National Audit Office, ‘Electronic monitoring – a progress update’ (8 June 2022), <https://www.nao.org.uk/wp-content/uploads/2022/01/Electronic-monitoring-a-progress-update.pdf>.

³⁰ Ibid.

³¹ WhatDoTheyKnow, Privacy International request to Home Office, ‘Electronic Monitoring of Immigration Offenders using GPS Tags’, https://www.whatdotheyknow.com/request/electronic_monitoring_of_immigra.

³² Gov.uk Contracts Finder, ‘Electronic Monitoring & Field Services and Service and System Integration’ (published 10 January 2017), <https://www.contractsfinder.service.gov.uk/notice/6b7768af-64c7-42c1-9ca2-47999949084f?origin=SearchResults&p=1>.

³³ Capita, ‘Capita extends contract with the Ministry of Justice’ (16 April 2020), <https://www.capita.com/news/capita-extends-moj-contract>.

³⁴ Gov.uk Contracts Finder, ‘Electronic monitoring hardware services’ (published 22 February 2018), <https://www.contractsfinder.service.gov.uk/notice/453fb31d-e00e-43fb-b7d2-413c3216a765?origin=SearchResults&p=1>.

³⁵ Gov.uk Contracts Finder, ‘Electronic Monitoring Service IT & Systems Managed Service’ (published 18 May 2022), <https://www.contractsfinder.service.gov.uk/notice/bc827d59-6481-4eda-a25c-2ebe17150347?origin=SearchResults&p=1>.

³⁶ Gov.uk Contracts Finder, ‘Electronic Monitoring Monitoring and Mapping and Related Services’ (published 1 November 2019), <https://www.contractsfinder.service.gov.uk/notice/e8255365-4e01-422e-a797-6d24e8afc1fa?origin=SearchResults&p=1>.

³⁷ Gov.uk Contracts Finder, ‘Contract Award Notice’ (3 June 2019), <https://www.contractsfinder.service.gov.uk/notice/3d55d1a7-fe54-4e4a-b9b1-d3a0a875d651?origin=SearchResults&p=3>.

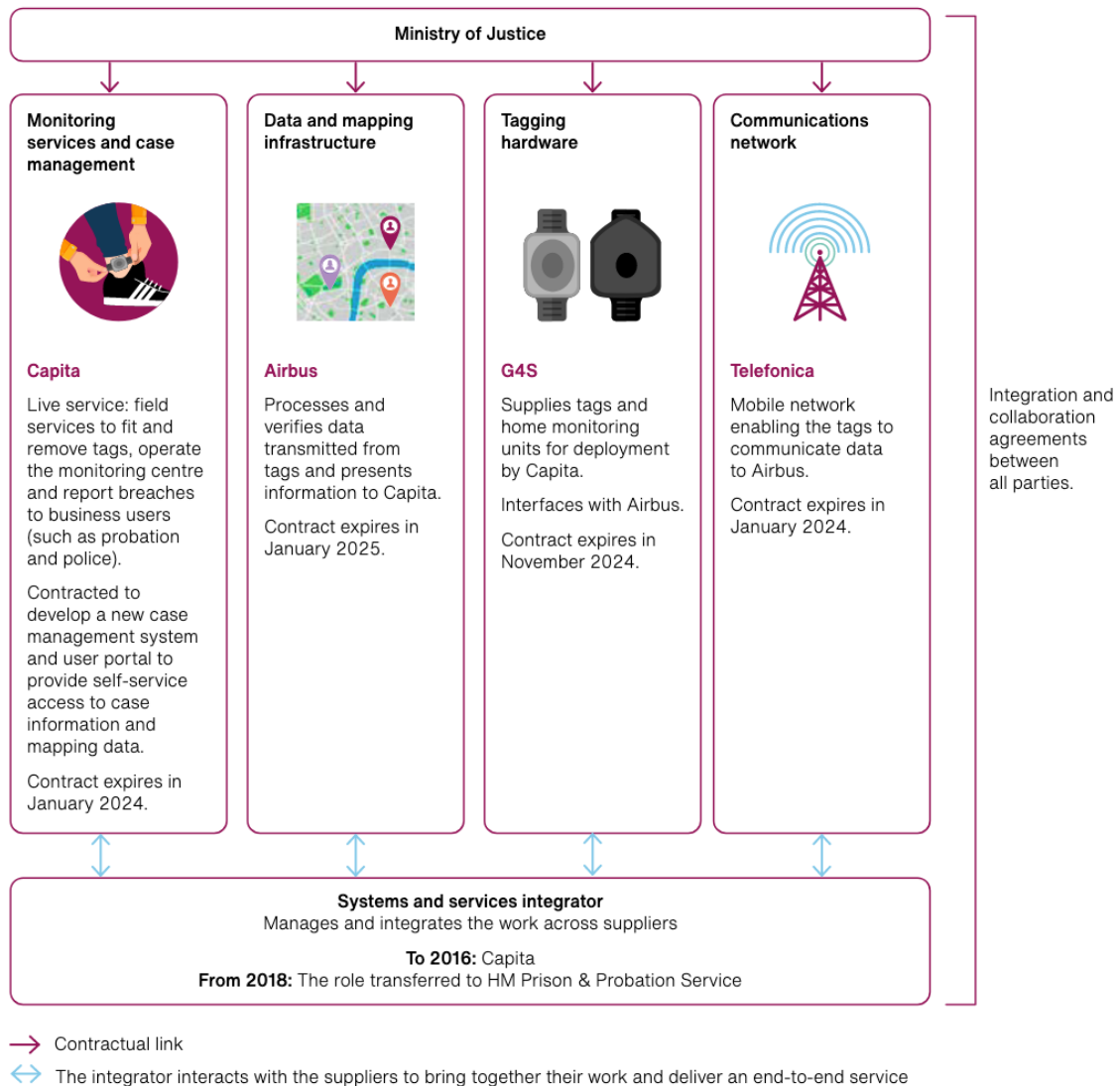
³⁸ National Audit Office (n 2), p.22.

³⁹ The latest contract may be this one for “Provision Mobile Devices, Voice, SMS text and Data Services to Ministry of Justice” expiring in 2024 for £7,950,000, however we do not have confirmation of this: <https://www.contractsfinder.service.gov.uk/notice/7e104c33-9287-4b48-b309-3efff93f4b82?origin=SearchResults&p=2>.

Figure 4

HM Prison & Probation Service's (HMPPS's) 'tower' delivery model for its tagging transformation programme

HMPPS's delivery model involves four main suppliers whose work it brings together in its role as systems and services integrator



Note

1 The Ministry of Justice is the contracting authority. HM Prison & Probation Service managed the tagging transformation programme.

Source: National Audit Office analysis of HM Prison & Probation Service documents

Figure 6 – Parties and contracting relationships involved in the Ministry of Justice’s EM programme (source: National Audit Office)

57. We note that a tendering process for Electronic Monitoring closed in April 2022,⁴⁰ and that in May 2022 a contract for Electronic Monitoring using Non-Fitted Devices was awarded to Buddi Limited.⁴¹ The use of non-fitted devices was

⁴⁰ Gov.uk Contracts Finder, ‘Early Market Engagement for the provision of Electronic Monitoring Future Service in England & Wales’ (16 November 2021), <https://www.contractsfinder.service.gov.uk/notice/cdf01f23-7054-4f81-8215-695fb4a7a8f9?origin=SearchResults&p=1>.

⁴¹ <https://www.contractsfinder.service.gov.uk/notice/60bb8854-257a-4c11-b3e0-efc733a87512?origin=SearchResults&p=1>.

presaged in the 2021 DPIA (paragraph 3) but we are not aware that they have been rolled out yet.

How the Home Office accesses trail data

58. According to the Immigration Bail policy and the DPIAs we have seen, the Home Office does not have direct access to the trail data collected by GPS tags. Instead, trail data is held by EMS (i.e. Capita) and only accessed by the Home Office in certain circumstances:

“trail data will be held by the EM supplier but may be accessed by the Home Office where one or more of the following applies and where proportionate and justified in the circumstances in accordance with data protection law:

- *a breach of immigration bail conditions has occurred, or intelligence suggests a breach has occurred to consider what action should be taken in response to a breach up to and including prosecution*
- *where a breach of immigration bail conditions has occurred, which has resulted in the severing of contact via EM, trail data will be used to try to locate the person*
- *where it may be relevant to a claim by the individual under Article 8 ECHR to be shared with law enforcement agencies where they make a legitimate and specific request for access to that data”⁴²*

59. We therefore understand that the Home Office will obtain access to all trail data every time a breach is notified.

60. What remains unclear from either the Immigration Bail policy or DPIAs, and would deserve further enquiries to understand the extent of Home Office access to trail data, is the following:

- (a) How are breach notification alerts set up? Do Home Office staff set them up themselves on software provided by EMS, or do they provide a list of bail conditions to EMS who set the alerts themselves?
- (b) Are breach alerts notified first to EMS, who then pass on information to the Home Office, or are they notified directly to the Home Office? Or both?
- (c) Are tagged individuals notified of every breach and given an opportunity to provide an explanation or mitigation, before the Home Office accesses trail data?
- (d) Is trail data automatically shared as soon as a breach is notified, or do Home Office staff first review the breach notification, then decide whether access to trail data is necessary, and if so make a request for the data from EMS?

⁴² Home Office, 'Immigration bail policy Version 12' (n 9).

- (e) In what form is data shared with the Home Office – is data (i) view-only through a software, or (ii) can it be downloaded by the Home Office directly from the software, or (iii) is it shared by EMS in a file, or (iv) any other option?
- (f) The information in Figure 6 above indicates that as part of HMPPS’s tagging programme, Capita was “*contracted to develop a new case management system and user portal to provide self-service access to case information and mapping data.*” Does the Home Office use the same system and user portal, hence does it have self-service access to mapping data?
- (g) What exactly constitutes “*intelligence [that] suggests a breach has occurred*”, and how does that differ from a breach alert?
- (h) Is trail data retained by the Home Office once a breach alert has been resolved?

61. Answers to the above questions would be required to assess the degree of necessity and proportionality of Home Office processing of trail data.

Why the Home Office accesses trail data

62. The Immigration Bail policy sets out the reasons for which the Home Office accesses trail data:

- “*a breach of immigration bail conditions has occurred, or intelligence suggests a breach has occurred to consider what action should be taken in response to a breach up to and including prosecution*
- *where a breach of immigration bail conditions has occurred, which has resulted in the severing of contact via EM, trail data will be used to try to locate the person*
- *where it may be relevant to a claim by the individual under Article 8 ECHR to be shared with law enforcement agencies where they make a legitimate and specific request for access to that data*⁴³

63. This is also set out and substantiated in the 2021 DPIA in the following terms:

“• Breach of Immigration Bail Conditions

In the event of a notification of a qualified breach of Immigration Bail conditions from the supplier, authorised Home Office Staff may perform a full review of the bail conditions and ask the individual wearer for any mitigation for the breach. The review consideration may be informed by the mitigation supplied and the review of the full trail monitoring data records where proportionate and justified. If, during the course of the review of the trail data, it becomes apparent that further breaches of immigration bail conditions may have been/ are being committed (e.g. Trail data provides a strong indication that subject is working in breach – showing them at a specific location other than home between 08:00 –

⁴³ Home Office, ‘Immigration bail policy Version 12’ (n 9).

17:00 hours) then that data may be shared within the Home Office e.g. Immigration Intel where proportionate and justified to investigate for further possible immigration breaches, under Part 2.

If, during the course of the review of the trail data, by the HO, there is any other indication that criminal activity is or has taken place then that data may be processed and shared with Law Enforcement agencies under Part 3.

• **Individual Absconds**

If the individual wearer loses contact and effectively 'absconds'. Authorised Home Office staff may access the full trail data in order to try and ascertain the current whereabouts of the individual in order to arrange possible arrest and detention under immigration powers. Data processed under Part 2.

• **EAR Requests**

Where a legitimate and specific request is made for access to specific data by a Law Enforcement Agency. We may process and share under Part 3.

• **Article 8 Representations / Further Submissions**

In the event of the receipt of Article 8 representations or further submissions from the individual, authorised Home Office staff dealing with those submissions may request access to the full trail data to support or rebut the claims. This will hopefully negate the need to request 'substantiating' evidence from third party's which can cause unnecessary delays in considering the claims.

• **Allegations of EM Breaches or Intelligence of Immigration Bail Condition Breaches Received**

In the event of Home Office staff receiving either of the above, Home Office staff may request details of full trail data to cover a specific period relating directly to the allegations or intelligence.

• **Subject Access Requests or Legal Challenge**

In the event of either of above being implemented Home Office staff will comply with legal process and timelines for provision of data. Rights will be assessed on a case by case basis and delivered in conjunction with supplier or other government/public bodies as required."

64. The various trail data processing activities can therefore be summarised as follows:
- (a) In the event of a notification of breach of bail conditions, to perform a review of full trail data to inform a review of bail conditions
 - (b) If the above review reveals further breaches of bail conditions, to share trail data within the Home Office for further investigation
 - (c) If the above review reveals evidence of criminal activity, to share with law enforcement

- (d) If contact is lost with the individual (considered absconding), to locate them and arrange possible arrest and detention under immigration powers
 - (e) In the event of a legitimate request, to share with law enforcement
 - (f) In the event of receipt of Article 8 submissions or further submissions from the individual, to review the full trail data to support or rebut the claims
 - (g) If intelligence or allegations indicate that a breach of bail conditions has occurred, to investigate this breach
 - (h) To respond to subject access requests or legal challenges
65. We will explore the implications of these various purported purposes of processing in the following section.

IV. Legal Framework and Concerns

66. This section sets out PI's concerns in relation to the compliance of the Home Office's use of GPS tags with its obligations under the UK GDPR and DPA 2018. We consider that the Home Office's tagging programme does not comply with the vast majority of the 7 principles of data protection law.
67. It should be clear from the previous sections of these submissions that the Home Office is engaged in the "processing of personal data wholly or partly by automated means" as provided by Article 2(1) UK GDPR. It should also be clear, notably from section III.C. above, that the Home Office processes special categories data as defined by Article 9(1) UK GDPR.

A. First Principle – Lawfulness, fairness and transparency (Art 5(1)(a))

Lawfulness

68. The 2021 DPIA (§§ 2.1 and 3.1) provides that both the general processing (UK GDPR/Part 2 DPA 2018) and law enforcement (Part 3 DPA 2018) regimes apply to processing of data, applying as follows to the different processing activities (as summarised in the previous section):
- (a) In the event of a notification of breach of bail conditions, to perform a review of full trail data to inform a review of bail conditions – **Part 2 DPA 2018**
 - (b) If the above review reveals further breaches of bail conditions, to share trail data within the Home Office for further investigation – **Part 2 DPA 2018** (however the 2020 DPIA had stated that this would fall under Part 3 DPA 2018: "*In a subset of the above cases where the individual breaches their Immigration Bail conditions a Breach Report Review will be created and prosecution for the criminal offence of breach of Immigration Bail will be*

considered by HOIE [“Home Office Immigration Enforcement”], and where the threshold is met a prosecution will be conducted in a timely manner. All such processing will be done by the HO under Part 3 DPA 2018.” It is unclear whether this was a mistake and was corrected in the 2021 DPIA, or whether investigation of potential further breaches by Immigration Enforcement is considered a separate processing activity to prosecution of such breaches.)

- (c) If the above review reveals evidence of criminal activity, to share with law enforcement – **Part 3 DPA 2018**
 - (d) If contact is lost with the individual (considered absconding), to locate them and arrange possible arrest and detention under immigration powers – **Part 2 DPA 2018**
 - (e) In the event of a legitimate request, to share with law enforcement – **Part 3 DPA 2018**
 - (f) In the event of receipt of Article 8 representations or further submissions from the individual, to review the full trail data to support or rebut the claims – **not specified, likely Part 2 DPA 2018**
 - (g) If intelligence or allegations indicate that a breach of bail conditions has occurred, to investigate this breach – **not specified, likely Part 2 DPA 2018**
 - (h) To respond to subject access requests or legal challenges – **not specified, likely Part 2 DPA 2018**
69. The DPIA 2021 provides the following legal bases for processing:
- (a) Processing under Part 2 DPA 2018 (“General processing”): “Performance of a public task” under Article 6(1)(e) UK GDPR (para 3.2.a), with “Explicit statute/power” indicated as the Immigration Act 2016 and The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021 (para 3.3).
 - (b) Processing of special categories data under “General processing”: the Article 9 condition for processing is “Substantial Public Interest” under Article 9(2)(g) (para 3.4.a). We note that this condition requires the processing to be “necessary” for reasons of substantial public interest, and “*on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*”. No detail is provided in the DPIA as to how the processing complies with this latter part of Article 9(2)(g).
 - (c) Processing under Part 3 DPA 2018 (“Law enforcement processing”): “Necessary for a law enforcement purpose” under s.35(2)(b) (para 3.2.b).

(d) Processing of special categories data under “Law enforcement processing”: the DPA Schedule 8 condition is listed as “Substantial public interest (for a statutory purpose)” (para 3.4.b).

70. The power to impose an EM condition is set out in the Immigration Act 2016 Schedule 10, § 2(1) and EM is defined at § 4(1):

“In this Schedule an “electronic monitoring condition” means a condition requiring the person on whom it is imposed (“P”) to co-operate with such arrangements as the Secretary of State may specify for detecting and recording by electronic means one or more of the following—

(a) P’s location at specified times, during specified periods of time or while the arrangements are in place;

(b) P’s presence in a location at specified times, during specified periods of time or while the arrangements are in place;

(c) P’s absence from a location at specified times, during specified periods of time or while the arrangements are in place.”

Lawfulness of 24/7 GPS monitoring

71. **First**, the wording of the legislation makes clear that EM can only enable the detection and recording of a person’s location at, presence in or absence from a location “*at specified times, during specified periods of time or while the arrangements are in place*”. However, EM using GPS tags enables the detection and recording of a person’s live location at all times, in all locations. While GPS tags could potentially be configured to only detect and record location in a specific place or at a specific time, this is not a limitation the Home Office seems to have put in place. PI therefore submits that the legislation does not provide statutory footing for the use of GPS tags in its current form – while the legislation provides powers to impose a form of electronic monitoring, GPS tags enable a type and level of monitoring that go far beyond what the legislation allows.

72. 24-hour GPS monitoring is therefore excessive for enacting the aims of the legislation. For example, for individuals on whom an overnight curfew is imposed, an EM condition is a considerable extension of surveillance and control, no longer justified by the need to verify compliance with other bail conditions.

Lawfulness of review of full trail data upon breach notification

73. **Second**, PI submits that the processing and review of *all* trail data in the event of a breach notification is not *necessary* for the performance of a public task (in the case of general data processing) nor for reasons of substantial public interest (in the case of special categories data processing).

74. As provided by the ICO, if a data controller relies on the public task lawful basis, “[t]he processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.”⁴⁴ A full review of all trail data will rarely ever be necessary nor proportionate for every breach alert. In light of the statistics provided by the ICIBI for reasons for breach notification⁴⁵ – 69.7% of breaches were battery breaches, 12.9% were 15-minute absences – it appears that a full review of all trail data will rarely be necessary nor proportionate for every breach alert, and many less intrusive options are available to the Home Office when dealing with breaches.
75. In addition, the Home Office has not demonstrated how processing special categories data when performing full trail data reviews is necessary for substantial public interest. The condition at Schedule 1, Part 2 § 6 requires the processing to be “*necessary for [...] the exercise of a function conferred on a person by an enactment or rule of law*”, *and* “*necessary for reasons of substantial public interest*”. Contrary to the other substantial public interest conditions in this schedule, processing being necessary for the exercise of a function is not sufficient to demonstrate that it is necessary for reasons of substantial public interest. Neither the DPIAs nor the Immigration Bail policy have provided any justification for the necessity of special categories data processing.

Lawfulness of processing for Article 8 claims

76. **Third**, it is clear from the context of Schedule 10 that the legislation’s purpose in providing this power is to enable the Home Office to monitor compliance with immigration bail conditions and to prevent individuals from absconding. Indeed, the schedule is titled “Immigration Bail”, and deals in its entirety with immigration bail matters.
77. It is therefore concerning and, PI submits, unlawful, that the Home Office has granted itself the right to use trail data in order to assess individuals’ Article 8 representations and further submissions. It is difficult to see how this use fits within immigration bail or even law enforcement purposes. As will be further explored below, the use of trail data by the Home Office to support or rebut individuals’ claims is a concerning abuse of the powers provided by Schedule 10 IA 2016, with potential to violate individuals’ fundamental rights – notably their rights to privacy, freedom of expression and freedom of association.

Lawfulness of the mandatory duty

78. **Finally**, PI considers that the mandatory duty to impose EM on those subject to deportation, established by Schedule 10 §2(3)(a), is contrary to public law principles and does not provide for “suitable and specific” measures to safeguard people’s fundamental rights, as required by the Substantial Public Interest

⁴⁴ ICO, ‘Guide to the General Data Protection Regulation (UK GDPR) – Lawful basis for processing – Public task’, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>.

⁴⁵ ICIBI (n 3), p.16.

condition for processing under Article 9(2)(g). Indeed, the mandatory EM duty has effectively removed judicial discretion and oversight. Despite the serious interference with the right to privacy resulting from real-time collection of location data, there is no attempt to justify that its use is necessary and proportionate on an individual basis. Despite the ability for the Home Office to decline the use of EM if it would be “contrary to an individual’s Convention rights”, there are no further safeguards nor indication of how these decisions are made in practice.

Fairness and reasonable expectations

79. The principle of fairness in Article 5(1)(a) UK GDPR is central to data protection law. PI supports and adopts the ICO’s definition and interpretation of fairness, described on its website as follows: *“In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.”*⁴⁶
80. The adverse effects on tagged individuals of permanent live tracking of their location are evident – constant fear that their movements may trigger a breach alert, anxiety about the tag’s battery charge levels when they go out and away from a mains power supply, uncertainty about the interpretation of their movements for purposes of assessing Article 8 representations, or suffering of social stigma. These adverse effects are entirely disproportionate to the aim pursued, which is to monitor compliance with bail conditions by individuals who are seeking a stable immigration status and rebuilding of their lives in a new country.
81. Core to fairness is that the data processing should be in line with individuals’ reasonable expectations.
82. Reasonable expectation of privacy is also a key principle in jurisprudence of the European Court of Human Rights (the “**ECtHR**”), which is used to assess whether there has been an interference with an individual’s private life under Article 8 of the European Convention on Human Rights (“**ECHR**”). The ECtHR has on several occasions investigated whether individuals “had a reasonable expectation that their privacy would be respected and protected”.⁴⁷
83. PI submits that the Home Office’s processing of trail data generally falls outside of data subjects’ reasonable expectations. Indeed, research and interviews by migrant rights organisations have shown that individuals rarely understand the nature and extent of the Home Office’s processing of their personal data. Testimonies from tagged individuals demonstrate (1) the lack of information provided to them as to how their data will be processed, (2) the uncertainty caused by this lack of transparency, and (3) the anxiety and anger that comes when they realise the extent of processing:

⁴⁶ ICO, ‘Guide to the General Data Protection Regulation (UK GDPR) – Principle (a): Lawfulness, fairness and transparency’, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.

⁴⁷ *Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), para 73.

“I’ve been reading up a little bit here and there about it and the one that I’m most worried about is, if we are making a claim under Article 8 right to family life and life in the UK, and the Home Office can turn around and say that we’ve got GPS evidence that you have not had consistent contact with your child, and therefore you do not meet the criteria for subsistent relationship. Surely that’s an invasion of right to private life?”

And my question also goes the other way – if I wanted to prove that I’ve had a subsistent relationship with my child, could I then stipulate a request for the Home Office to bring that information and show that I’d been to the area or place where he lives and therefore prove that I have had that kind of consistent relationship with my child.”⁴⁸

“there is definitely data, like you will be monitored by them, wherever you go, how far you go, this one and this one. That makes me very sick, it might be I go somewhere out with the family, with the friends, somebody watching, where are you, what are you doing... it makes me so much crazy now”⁴⁹

84. It is also apparent that individuals do not always fully appreciate what compliance with their bail conditions requires. For example:

“Not knowing whether I have a curfew or not. There’s so much vagueness around it all which should not be like that. What does sleep at my premises mean? Can I get home at 4’oclock in the morning and then sleep to 8 or 9 or 10? Or is that taking the piss? Where’s the line?”⁵⁰

85. This means they can be unaware or uncertain about the fact that certain movements or behaviours may trigger a breach notification and thereby provide opportunity for the Home Office to perform a review of their entire trail data.

86. In addition, even if individuals do understand the extent to which their location data is recorded and monitored, they may not fully appreciate the implications – the volume and granularity of GPS location data is difficult to grasp for most people. In the US Supreme Court case of *United States v. Jones*,⁵¹ the Court considered individuals’ reasonable expectations of privacy:

*“I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements. **I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits and so on**” [emphasis added]*

⁴⁸ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

⁴⁹ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

⁵⁰ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

⁵¹ N 27.

Transparency

87. Whether processing falls within data subjects' reasonable expectations and is therefore fair is also directly affected by the level of transparency provided around this processing: *"Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data."*⁵²
88. PI submits that the Home Office does not provide individuals with sufficient information to comply with the principle of transparency.
89. Informed by migrant rights organisations and law firms who support tagged individuals, PI has found that these data subjects are provided with very limited and unclear information about what data will be processed and how. Among the set of questions asked to participants in research by a migrant rights organisation was "were you given any information about how your data would be processed". Not a single person answered yes to indicate that they were told how their data would be processed.
90. Another testimony from this research, in answer to the question "When the tag was attached, were you given much information about how it would operate? Were you given any information about how your data would be processed?", provides:

*"They were absolutely useless. They just gave me the documentation, the leaflets provided by the monitoring service and asked me to sign some paperwork. I think they gave me the basics of, You need to make sure its charged at all times."*⁵³

91. A client of a law firm representing tagged individuals also said:

"I am not aware of what will be done with any data that is being collected through the GPS tag. I have not been given any paperwork to explain this that I can remember or am aware of. One time recently, however, I was told by the Home Office that I had breached my bail conditions. This is because they said they had visited my home on several occasions to check my tag [REDACTED] [REDACTED], and I had not been there. This was confusing because I do not have a bail condition which says I need to be in the house at a certain time imposed, nor do I have a curfew condition. I have not seen the paperwork associated with this breach, I was told about it by one of the officers who I spoke to on the phone following the attempted visits to my house. As far as I know, this breach resulted from the fact that I wasn't present at the house when someone from the Home Office came to check my tag, it was not because they

⁵² ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Principle (a): Lawfulness, fairness and transparency', <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.

⁵³ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

*were tracking me. Obviously, I can never know what the Home Office do with my data though, and sometimes I do feel like they are tracking me.*⁵⁴

92. Research from Dr Monish Bhatia of Birkbeck University also found that tagged individuals who participated in his research “*were not offered an explanation as to why the device was attached to their ankles and why they were placed on curfew (which lasted anywhere between 8 and 12 hours). Individuals were told that breaking the monitoring conditions or tampering with the device could result in arrest and/or a negative decision on their immigration and asylum cases.*”⁵⁵

93. PI has been provided with the various documents given to individuals when they are tagged. We understand that these include (i) the EMS tagging handbook,⁵⁶ (ii) a Bail 201 form (Exhibit 4), and (iii) a Bail 211 form. According to the Immigration Bail policy,⁵⁷ the Bail 211 must be served on individuals, or at least they should be informed of their right to make representations against the imposition of an EM condition. However, individuals frequently do not receive this form, nor the EMS tagging handbook, which provides further information about individuals’ data rights (including how to make a subject access request). As one individual said:

I didn't even know that I was going to get tagged until it happened. I wasn't given a Bail 211 form when I was released. I didn't receive any leaflet or any other information explaining how the tagging works, how my data would be used, or how to ask for the tag to be removed.

94. Even where they are given to individuals, these documents provide little information about what data will be processed, under what conditions, and for what purposes. In addition:

(a) Individuals are certainly not informed of which entities will be processing their data. The only “entity” with which they directly interact is EMS, however they are not informed that this service is run by Capita, nor that a number of other third parties are involved in the processing of their data.

(b) We know from solicitors working with tagged individuals that these manuals are only provided in English – a number of individuals are therefore unable to fully understand their contents.

95. Another testimony also indicates that individuals are never directly informed of the possibility that their location data may be used in assessments of their private and family life for purposes of Article 8 representations and further submissions, and some of them only know of it from rumours or word of mouth:

⁵⁴ Anonymous testimony from a tagged individual, client of a law firm.

⁵⁵ Dr Monish Bhatia, ‘Racial surveillance and the mental health impacts of electronic monitoring on migrants’, *Race & Class* (2021), Vol. 62(3) 18–36, p.25.

⁵⁶ EMS, ‘Tagging – Everything you need to know about being tagged’, <https://www.gov.uk/government/publications/gps-location-monitoring>.

⁵⁷ Home Office, ‘Immigration Bail policy Version 12’ (n 9).

“My biggest thing in all the research I’ve done in this is that it’s an invasion into the right to private life. Article 8 stipulates that if we want to stay that we have to prove we have family and that we are embedded in UK society. Obviously the biggest one is right to family life. So having a child and proving that I am a substantial role model in his life is a huge one. But the Home Office, if they want to, this is what I’ve heard, I don’t know the reality of it but this is the reading I’ve done. If they want to prove that I have no subsistence – this is a word they love to use – relationship with my son; they can pull up the tracking GPS evidence from my tag and say that I have not had consistent interaction in a face to face way with my son and therefore do not have proof to subsistence relationship and therefore have the grounds to deport me from the country.”⁵⁸

96. The lack of clarity provided to individuals around the specifics of their bail conditions also leads to profound uncertainty about what kinds of behaviours will trigger a breach notification and whether this will lead to the Home Office reviewing their trail data:

*“No information and so much confusion on our immigration release as also per licence release. I have to stay at my approved premises which I get, but I am not liable to any kind of curfew. I do not have to be at home at a certain time or I’m not limited to a certain place. So that has no bearing whatsoever but when I received my Home Office immigration thing it says I have to abide and stay at my approved address but there’s no time there. It just says you need to stay there at the approved address. I’ve just check in with immigration today and asked a specific question, Is there a curfew? It says I have to sleep there, but is there a curfew? To which he answers, No, there is no curfew on your conditions. **So that’s just so confusing because obviously the scare there is that I have a GPS tracking device on my leg at all times and obviously if they can prove that I haven’t stayed there at home, is this going to be grounds for breaking my conditions and deporting me? Also there’s no contact number for ease of clarity.***

*At the weekend I went camping with some friends. Obviously I couldn’t stay out. My friend was going to drop me home but he had some problems with his car battery but it was too late because I live in [REDACTED] and things are quite rural. So, I only got back the next morning in complete panic that I had broken my conditions. **So I phoned up the monitoring centre. They said, No we don’t monitor your curfew condition, we only track and trace whether your tag is fully charged or fully functional or not. To which I asked, if the Home office have access to that information. To which they answered, Yes if they wanted to, they have access to that information.** So, in so many ways, I just feel like I’m held over a barrel of fear and intimidation of not really knowing what my rights are.”⁵⁹ [emphasis added]*

⁵⁸ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

⁵⁹ Anonymous testimony from a tagged individual, client of a migrant rights support organisation.

97. By contrast, when an individual is tagged under the criminal justice system, HM Prison & Probation Service’s Code of Practice for EM requires that they are provided with a “Fair Processing Notice”, *“which explains the legal basis for the processing of their personal data and will explain the data subject’s rights. The notice will explain the types of data that may be collected and, where necessary and proportionate to do so, this data may be shared with Criminal Justice Agencies for specific purposes.”*⁶⁰
98. PI therefore submits that the Home Office’s GPS tagging programme suffers from a systemic lack of transparency, with little to no information provided to data subjects about whether and how their data will be processed.

B. Second Principle – Purpose limitation (Art 5(1)(b)) and particular concerns regarding use of trail data for Article 8 claims (and compliance with Article 22 UK GDPR)

99. The 2020 DPIA states that the primary purpose of the processing is to *“track and record the location of individuals in order to support immigration control”* (§4.11, p.11). However, that is not the only anticipated purpose, and PI submits that the Home Office’s expansive use of trail data violates the purpose limitation principle provided by Article 5(1)(b) UK GDPR, which requires that data is “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.” A data controller may only process data for a new purpose if:
- *“the new purpose is compatible with the original purpose;*
 - *you get the individual’s specific consent for the new purpose; or*
 - *you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.”*⁶¹
100. We previously summarised the various **processing purposes** stated in the DPIAs and in the Immigration Bail policy. Here we assess their compliance with the purpose limitation principle:
- (a) **In the event of a notification of breach of bail conditions, to perform a review of full trail data to inform a review of bail conditions** – this purpose may fall within the original stated purpose of *“track[ing] and record[ing] the location of individuals in order to support immigration control”*. However, as submitted above in the *Lawfulness* section, a review of full trail data does not appear necessary to inform a review of bail conditions following a breach. It may therefore already constitute an extension of purpose.

⁶⁰ HM Prison & Probation Service, ‘Code of Practice – Electronic Monitoring Data’ (October 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf, § 21.

⁶¹ ICO, ‘Guide to the General Data Protection Regulation (UK GDPR) – Principle (b): Purpose limitation,’ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.

- (b) **If the above review reveals further breaches of bail conditions, to share trail data within the Home Office for further investigation** – this processing activity is a worrying example of extension of purpose, and violates the principles of necessity and proportionality. Putting aside the fact that a review of full trail data is unnecessary and disproportionate to investigate one breach (see (a)), the fact that indication of further breaches may lead to further investigations is concerning. Indeed, it skirts the established and stated process of breach identification, notification and investigation, leaving individuals unaware of the various circumstances in which a breach may be investigated, and unable to respond to a challenge.

For example, a battery depletion breach investigation may reveal a breach of curfew that occurred weeks ago and for one reason or another did not trigger a breach alert. As this goes back in time and the individual was not provided with the opportunity to explain this breach shortly after, they are left to be challenged about it weeks later, having to reminisce and find a justification for something they may not have realised was a breach at the time.

This was an issue identified in the ICIBI’s inspection report: *“Many of the breaches received were not processed or reviewed and so risks associated with non-compliance would not be considered. One of the other impacts of this was that individuals who had breached their EM bail conditions, for whatever reason, would not have the opportunity to provide mitigation close to the time of the breach.”*⁶²

- (c) **If the above review reveals evidence of criminal activity, to share with law enforcement** – this processing purpose effectively places criminal law investigative powers in the hands of the Home Office. While it is understandable that should the Home Office come across such evidence, they ought to disclose it, it goes to show that they should not have been able to come across this evidence in the first place. The purposes of immigration enforcement, and (for example) the monitoring of compliance with a curfew, do not require surveillance powers that enable detection of this kind of activity. The ability to do so blurs the line between the Home Office and law enforcement, and extends the surveillance control powers of the Home Office beyond what legislation intended.
- (d) **If contact is lost with the individual (considered absconding), to locate them and arrange possible arrest and detention under immigration powers** – this may also be an extension of powers beyond what legislation intended. The IA 2016 provides that electronic monitoring can be used to monitor a person’s location, presence or absence from a location “at specified times, during specified periods of time or while the arrangements are in place”. This wording does not provide means to the Home Office to constantly monitor someone’s whereabouts, and loss of contact cannot automatically be

⁶² ICIBI (n 3), § 5.82.

a breach of bail conditions. A breach can only occur if someone fails to be present at the location and time specified in their bail conditions. The Home Office is thereby extending its monitoring powers beyond the scope of the legislation and beyond the stated purpose of GPS tagging.

- (e) **In the event of a legitimate request, to share with law enforcement** – while a legitimate request from law enforcement must be complied with, the GPS tagging system is producing a considerable volume of highly granular data that should not have been produced in the first place. This is a clear example of a “technological innovation” approved in legislation for one purpose, massively expanding police surveillance powers by virtue of powers in other legislation.
- (f) **In the event of receipt of Article 8 submissions or further submissions from the individual, to review the full trail data to support or rebut the claims** – this is the most worrying, and PI submits, unlawful, extension of purpose. Further analysis of this purpose is at paragraphs 101 to 105 below.
- (g) **If intelligence or allegations indicate that a breach of bail conditions has occurred, to investigate this breach** – as previously noted, it is unclear what “intelligence” or “allegations” are referred to here, and how these differ from breach alert notifications. In any case, as submitted before, review of full trail data is not necessary nor proportionate for investigating an individual breach.
- (h) **To respond to subject access requests or legal challenges** – this is a legitimate purpose. However, organisations working to support tagged individuals have indicated that subject access requests to EMS yielded no trail data. We are therefore concerned that EMS does not fully comply with subject access requests.

101. The most extensive and concerning potential re-use that is contemplated by the Home Office in relation to trail data access is where such data is relevant to “*a claim by the individual under Article 8 ECHR*” and for the purposes of rebutting the merits of the claim. Article 8 representations and further submissions are claims made by individuals that they have a private and family life in the UK, and therefore ought to be granted leave to remain. It is difficult to see how this data use fits within the realm of law enforcement or immigration bail purposes.

102. The 2020 DPIA also states that the trail data will negate the need to request evidence from third parties: “*In the event of the receipt of Article 8 representations or further submissions from the individual, authorised Home Office staff dealing with those submissions may request access to the full trail data to support or rebut the claims. This will hopefully negate the need to request ‘substantiating’ evidence from third party’s [sic] which can cause unnecessary delays in considering the claims.*” [emphasis added]

103. This places a heavy burden on an individual to recall events recorded by their GPS tag, which could go back months or years in the past. It also shows no appreciation for issues relating to inaccuracy of satellite location – even with a level of accuracy to around 10 meters, a difference of 10 meters can indicate presence at one shop or property rather than the next, which can have profound implications for the individual’s case. Concerns are of course compounded when inaccuracies go to hundreds of metres, which commonly occurs (see Section IV.D. Below (Accuracy)). It is also deeply concerning that the Home Office would seek to make life changing decisions on an individual’s future purely based on location data and without evidence from third parties. Prior to the deployment of GPS tagging, the only thing an individual would need to remain conscious of during their bail is to comply with their conditions – they now need to think about how every single one of their movements might impact their future or potential Article 8 representations or further submissions. Making a claim on the basis of one’s human rights should never (and as far as we’re aware, has never) entitled the state to engage in such levels of surveillance and invasion of privacy.

104. As the charity Bail for Immigration Detainees has stated:⁶³

“Article 8 claims can be very broad and involve a lot of personal and private details about an individual’s life. Presently there is no clear limit on the circumstances in which location data might be deemed by the Home Office to be relevant to an Article 8 claim. This could mean that whenever an individual makes an Article 8 claim the Home Office would have the right to access all their ‘trail data’ on the grounds that it ‘may be relevant’.

This provision gives unlimited discretion to the Home Office decision-makers to retrospectively access location data for purposes over and above monitoring compliance with bail conditions. The Home Office is not a neutral third party and they have a vested interest in proceedings which could have negative repercussions on an individual’s substantive case. This can be contrasted with the use of electronic monitoring in the criminal justice system, where electronic monitoring data must only be “processed for specified, explicit and legitimate purposes.”

105. This power, which the Home Office has effectively granted itself with no basis in legislation, implies that life-changing and rights-impacting decisions may be taken on the basis of erroneous, non-representative or misinterpreted data. We do not believe there are sufficient or adequate safeguards in place to address the risk of abuse and the significant power imbalance this creates between the tagged individual and the Home Office.

106. PI also queries whether using trail data for such assessments complies with the prohibition on automated decision-making under Article 22 of the UK GDPR, which provides data subjects with the right “*not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects*

⁶³ BID (n 5).

concerning him or her or similarly significantly affects him or her.” If decisions on Article 8 representations are made without active, critical interpretation of trail data and without providing individuals with an opportunity to make representations as to its accuracy and interpretation, this would constitute automated decision-making with legal effects on the data subject.


107. To summarise, the purposes of processing described are not within the scope of the original or primary purpose of electronic monitoring. According to the purpose limitation principle (Article 5(1)(b) UK GDPR), data collected for certain purposes cannot be further processed in a manner that is incompatible with those purposes. Any use for an incompatible purpose must be supported by a new legal basis, and an updated impact assessment. This does not appear to have been done – the only hint in the DPIA to a consideration for this principle shows that no serious analysis has been performed of the compatibility of purposes, simply stating *“We believe the use of GPS including ‘Trail Data’ is in line with the original intent of Electronic Monitoring referred to within Schedule 10(4) of the Immigration 2016 and that it’s use is compatible with the overall aims of effective immigration control”* (sic).
108. PI also wonders whether location data may be collected by the Home Office to generate actionable intelligence for wider action against migrants or groups of migrants – which has been the practice of immigration authorities in the US in the past.⁶⁴ While we have not seen evidence that this is so, we haven’t either seen safeguards against re-use of data for purposes not listed in the policy. We would recommend that the ICO investigates this potential re-use.

C. Third Principle – Data minimisation (Art 5(1)(c))

109. The principle of data minimisation requires that personal data be *“adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”* (Article 5(1)(c) UK GDPR).
110. As explained above, various models of GPS tags provide technical settings to limit the amount of data collected, for example by setting location data collection only at certain intervals rather than 24/7. However we do not know whether this is a feature of the tags procured by the Ministry of Justice, and have not seen any indication that the Home Office has set particular data collection intervals. This means that the amount of data collected is not limited and tailored to what is necessary to monitor bail compliance and/or minimise the risk of absconding.
111. PI therefore submits that the Home Office collects an amount of data in excess of what is necessary to effect the purposes of the legislation, and is thereby in violation of the data minimisation principle. The standard of necessity for accessing trail data is also lower than what is required by the purpose limitation principle, leading to excessive processing.

⁶⁴ Danielle Silva, ‘GPS tracking of immigrants in ICE raids troubles advocates’, NBC News (15 August 2019), <https://www.nbcnews.com/news/us-news/gps-tracking-immigrants-ice-raids-troubles-advocates-n1042846>.

D. Fourth Principle – Accuracy (Art 5(1)(d))

112. The principle of accuracy requires that personal data be “*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*” (Article 5(1)(d) UK GDPR).
113. GPS location is accurate to about 10 meters in good conditions. Accuracy is affected by a number of factors, such as urban canyons (built up areas where tall buildings can block the satellites and cause the signal to bounce), long distance to the nearest satellite, or restricted view of the open sky so that only a few satellites are visible. As the density of mobile base stations can vary from a hundred meters in town centres to several kilometres in the open countryside, GPS location can be less accurate in rural areas (like many smartphones).⁶⁵ All these factors affecting accuracy of GPS location data can give rise to errors of 100 meters or more.⁶⁶
114. Some of these accuracy issues were considered in *R v Calland*: “*Cell siting evidence can be powerful evidence. But it is not capable of locating a phone with pinpoint accuracy and it has other limitations. Those limitations are familiar to all who conduct and try criminal cases in which such evidence is commonly adduced. The limitations are not however necessarily familiar to the members of a jury.*”⁶⁷
115. In circumstances where GPS location is used to monitor compliance with bail conditions, inaccuracies, even small, can have profound consequences for individuals. Trail data can show individuals attending certain locations when they have actually attended others – for example, inaccuracies of just a few meters can show someone attending an office building every day, when they have actually been attending the coffee shop next door. If the individual’s bail conditions forbids them from working, this can lead to wrongful accusations of breach to be made against them.
116. Research by PI’s technologists has also shown that GPS tags stop functioning when the tag is underground or in certain places with poor satellite visibility, such as when riding London’s underground or attending a concert. For example, 

⁶⁵ Reform, ‘Cutting crime: the role of tagging in offender management’ (September 2015), https://reform.uk/sites/default/files/2018-10/Tagging%20report_AW_8.pdf.

⁶⁶ See PI’s tech primer on GPS tracking for further references regarding accuracy issues, PI, ‘GPS tracking and COVID-19: A tech primer’ (7 May 2020), <https://privacyinternational.org/explainer/3753/gps-tracking-and-covid-19-tech-primer>.

⁶⁷ [2017] EWCA Crim 2308, §30.

117. Similarly, one of our technologists observed that when shopping at his local grocery store, his GPS tag is unreachable due to there being no cell coverage in the store, and therefore a notification is sent to the monitoring device (his phone in this case).
118. In circumstances where loss of contact for more than 15 minutes can trigger a breach alert and be considered absconding (as provided by the list of processing purposes in the 2021 DPIA), thereby triggering a full review of trail data to locate the individual, this can lead to wrongful accusations of breach and inaccurate records.
119. Evidence from migrant rights organisations and law firms representing tagged individuals also shows that many of the tags suffer from poor battery performance, having to be charged multiple times a day and for much longer than recommended in the tagging handbook. This results in GPS tags running out of battery at random times in the day, sometimes when the individual is unable to get to a charging point. The ICIBI has found through its inspection that *“Instances of faults in December were exceptionally high across the whole of the MOJ contract, with 1,195 devices returned, which included “907 SOLO [EM devices]” which “[Capita EMS] had to recall and return due to a charging fault which all had to go back for repair.”*⁶⁸ As battery depletion constitutes a breach of bail conditions, their breach reports can show many breaches that they were not responsible for, thereby painting an inaccurate and negative picture of their compliance.
120. None of the DPIAs or Immigration Bail policy acknowledge these accuracy issues, nor do they provide any guidance or safeguards to mitigate them or guard against abuse. As such no “reasonable step” has been taken to ensure that that inaccurate data is rectified – having regard to the purposes for which they are processed, this is particularly concerning, as the consequences of inaccuracy can be dire for individuals. PI therefore submits that without such safeguards, the Home Office’s processing of location data violates the accuracy principle.

E. Fifth Principle – Storage limitation (Art 5(1)(e))

121. The storage limitation principle requires that personal data be *“kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”* (Article 5(1)(e) UK GDPR).
122. The DPIA 2021 provides that *“All the data contained within the monitoring orders will be retained for 6 years after the Monitoring ceases to be live. All audit trail data will be retained for 6 years after the monitoring order ceases to be live.”* (§ 6.3)

⁶⁸ ICIBI (n 3), § 5.72.

123. PI assumes that the rationale for such a retention period is the limitation period for prosecuting offences of breach of immigration bail conditions, however this is not explicit in either the DPIAs or Immigration Bail policy. However it is difficult to see how this reconciles with the purpose of “live monitoring”. Under the breach alert system, trail data is reviewed as soon as a breach alert occurs – it is unclear why retaining all data for 6 years would be necessary to prosecute individual bail breaches.
124. The gigantic amount of highly granular data generated by live location monitoring is disproportionate to the need to retain data to review individual bail breaches as they occur. A more proportionate approach would entail, for example, retaining data for 3 months and deleting it if no bail breaches have occurred in that period. PI therefore submits that the Home Office’s GPS location data processing violates the storage limitation principle.

F. Sixth Principle – Integrity and confidentiality (security) (Art 5(1)(f))

125. The integrity and confidentiality principle requires that data is “*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*” (Article 5(1)(f) UK GDPR).
126. Article 32(1) of the UK GDPR also provides: “*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*”.
127. Information as to data management systems is scant in the DPIAs. In response to “Where will the data be stored?” (§ 2.9), the DPIA 2021 provides:
- “Immigration Enforcement encrypted data storage and EMS data storage as the existing third-party supplier under the contract awarded by MOJ. The data is stored by EMS on their internal servers and HOIE do not have access to their systems. Immigration Bail Condition Breach data is forwarded to HOIE on a daily basis for us to be able to manage the breaches. It is received in PDF format and data is transferred to the Case Information Database (CID) and dually onto the Atlas system service until CID is de-commissioned in 2021 whereupon the data will be transferred solely onto the Atlas system on the Immigration Bail Condition Breach screens of the individual. The original breach report is stored under normal HOIE storage and retention.”*
128. However we understand from the ICIBI’s inspection report that data assurance concerns were identified:

*“Hub staff had to work with multiple IT systems which provided different data that was not easily retrieved for workflow planning and analysis. Consequently, there was reliance by Hub staff on the use of Microsoft Excel spreadsheets, including by individuals to manage their own caseload. This resulted in limited assurance that data was being managed and shared appropriately.”*⁶⁹

129. PI is therefore concerned that despite assurances in the DPIAs as to security of the data, no serious and systematic consideration has been given to the significant sensitivity of the data being processed, and hence no clear measures have been taken to limit vulnerabilities in data storage or to limit the number of individuals with access to the data and their levels of security clearance. In light of the very sensitive nature of data being processed, a strict assessment of security measures ought to be conducted.

130. Further enquiries should therefore be made as to exactly what types of data are stored in what format, and how access controls are defined and monitored.

G. Seventh Principle – Accountability (Art 5(2))

131. The accountability principle provides that “[t]he controller shall be responsible for, and be able to demonstrate compliance with” the principles in Article 5(1) UK GDPR (Article 5(2) UK GDPR).

132. PI finds that the amount of information and analysis provided in the DPIAs is very limited compared to the considerable risks that this data processing entails. Our analysis of the Home Office’s compliance with the six data protection principles of Article 5(1) has required piecing together information from a wide array of sources, notably from third parties, as information provided by the Home Office in the DPIAs and Immigration Bail policy was insufficient to evaluate compliance. This is concerning and demonstrates disregard for, or at the least ignorance of, the profound impacts of GPS tagging on the privacy of tagged individuals.

V. Impact on fundamental rights and freedoms

133. In this section we provide an overview of the various ways in which GPS tagging impacts individuals’ fundamental rights and freedoms, to demonstrate the need for a strict assessment and application of the various data protection principles.

134. **First**, as already evoked throughout these submissions so far, the monitoring of individuals through GPS tags interferes with their right to privacy under Article 8 ECHR. The ECtHR has previously ruled on the interference of GPS surveillance with the right to private life under Article 8 ECHR. In *Uzun v. Germany*,⁷⁰ it considered that the placing of a GPS device in someone’s car led to “*the applicant’s observation via GPS*”, and that the “*processing and use of the data*

⁶⁹ ICIBI (n 3), §3.1.

⁷⁰ *Uzun v. Germany* App no 35623/05 (ECtHR, 2 September 2010).

*obtained thereby [...] amounted to an interference with his private life as protected by Article 8 § 1.*⁷¹

135. Whether this interference is justified depends on the necessity and proportionality of the measure:

*“In determining whether the applicant's surveillance via GPS as carried out in the present case was “necessary in a democratic society”, the Court reiterates that the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (see *Leander v. Sweden*, 26 March 1987, § 58, Series A no. 116; and *Messina v. Italy (no. 2)*, no. [25498/94](#), § 65, ECHR 2000-X).”*⁷²

136. In assessing necessity and proportionality of GPS surveillance of the vehicle of an associate of the applicant, the Court in *Uzun v. Germany* provided that:

*“in these circumstances, the applicant's surveillance via GPS had led to a quite extensive observation of his conduct by two different State authorities. In particular, the fact that the applicant had been subjected to the same surveillance measures by different authorities had led to a more serious interference with his private life, in that the number of persons to whom information on his conduct had become known had been increased. Against this background, the interference by the applicant's additional surveillance via GPS thus necessitated more compelling reasons if it was to be justified. However, the GPS surveillance was carried out for **a relatively short period of time (some three months)**, and, as with his visual surveillance by State agents, **affected him essentially only at weekends and when he was travelling in S.'s car**. Therefore, he cannot be said to have been subjected to total and comprehensive surveillance. Moreover, the investigation for which the surveillance was put in place concerned **very serious crimes, namely several attempted murders of politicians and civil servants by bomb attacks**. As shown above, the investigation into these offences and notably the prevention of further similar acts by the use of **less intrusive methods of surveillance had previously not proved successful**. Therefore, the Court considers that the applicant's surveillance via GPS, as carried out in the circumstances of the present case, was proportionate to the legitimate aims pursued and thus “necessary in a democratic society” within the meaning of Article 8 § 2.”*⁷³
[emphases added]

137. The UK Supreme Court confirmed, in *Elgizouli v Secretary of State for the Home Department* [2020] UKSC 10, that the test of necessity is a strict one. In *Johnson v SSHD* [2020] EWCA Civ 1032, Dingemans LJ further held that:

“any limitation of the fundamental right to the protection of personal data must be strictly necessary, see [Elgizouli] at paragraph 9. Necessity should be

⁷¹ Ibid, § 52.

⁷² Ibid, § 78.

⁷³ Ibid, § 80.

justified on the basis of objective evidence. The proportionality of the limitation on the fundamental right must also be assessed. If there are less restrictive measures that can be taken, they should be taken.” [at § 40]

138. Applying the different elements of the ECtHR’s necessity and proportionality assessment in *Uzun v. Germany* to the GPS surveillance of migrants by the Home Office, PI submits that it cannot be found necessary nor proportionate:

(a) **Duration of surveillance** – a period of three months was considered “relatively short”. By contrast, the Home Office tagging of migrants can last many months or sometimes years, as deportation proceedings are often protracted in time. Even after proceedings have ended and a deportation order has been signed, enforcement can be delayed by a range of practical or legal reasons – for example if removal is not practically possible or safe. Similarly, if a person is subjected to tagging but not threatened with deportation, they may be tagged indefinitely until they either secure leave to remain or are removed administratively.

(b) **Timing and location of surveillance** – GPS surveillance occurring “essentially at weekends” and only when in someone else’s car meant that the applicant could not “be said to have been subjected to total and comprehensive surveillance”. By contrast, the Home Office collection of location data occurs 24 hours a day, 7 days a week, wherever the individual goes. The surveillance in this case is therefore “total and comprehensive”.

(c) **Justification of surveillance** – the investigation for which surveillance was put in place in this case concerned “very serious crimes, namely several attempted murders of politicians and civil servants by bomb attacks”. While the Home Office “mandatory duty” to consider EM applies to Foreign National Offenders (“**FNOs**”), the offences concerned can range across the range of crime seriousness. As Stephen Shaw’s 2018 review into immigration detention states, “*the twelve month sentence criterion for deportation in the UK Borders Act is not a very good guide to criminality*”⁷⁴. There is no minimum threshold of crime seriousness below which the duty does not apply. In addition, some individuals who have not previously been found guilty of offences can be tagged as well, if the Home Office considers it appropriate and justified. The UK government has also recently announced that asylum seekers subject to deportation to Rwanda for external processing of their applications may be tagged while they await their flight.⁷⁵

(d) **Less intrusive methods** – in this case, “*less intrusive methods of surveillance had previously not proved successful*”. By contrast, the previous

⁷⁴ Assessment of government progress in implementing the report on the welfare in detention of vulnerable persons (July 2018),

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728376/Shaw_report_2018_Final_web_accessible.pdf.

⁷⁵ The Guardian, ‘GPS tagging of migrants appears to contradict Home Office guidance’ (19 June 2022),

<https://www.theguardian.com/uk-news/2022/jun/19/gps-tagging-of-migrants-appears-to-contradict-home-office-guidance>.

methods of monitoring immigration bail conditions cannot be said to have proved unsuccessful and therefore to justify heightened levels of surveillance. Indeed, data obtained through FOIA requests show low and stable levels of absconding under previous practice: in 2020, only 1 percent of people released from immigration detention tried to abscond.⁷⁶ Data obtained by Bail for Immigration Detainees (BID) shows that of the people granted bail from February 2020 to March 2021 (of which there were more than 7,000⁷⁷), just 43 people absconded – less than 0.56 percent.

139. None of the various necessity and proportionality factors relied on by the court in *Uzun v. Germany* apply to this case – the Home Office GPS surveillance of migrants lasts for a long and indefinite amount of time, is total and comprehensive, is not justified by crime seriousness, and less intrusive methods of surveillance have previously proven successful. PI therefore submits that EM by the Home Office would be found by the ECtHR to violate individuals’ Article 8 ECHR right to privacy.
140. PI understands from organisations representing tagged individuals that in individual cases, including where subject access data is available, the Home Office appears to have made no attempt to justify the imposition of EM on the facts of the case, nor explained why less intrusive alternatives are not available. We note that in the ECtHR case of *Ben Faiza v. France*,⁷⁸ a breach of Article 8 was found in relation to surveillance by a GPS device, because the manner in which the power to impose the surveillance was framed was not clear and was overly general.
141. **Second**, GPS surveillance infringes on the rights to freedom of expression (Article 10 ECHR), assembly and association (Article 11 ECHR). By tracking individuals’ every movement, GPS tags can provide the Home Office with precise information about their trips to, for example, trade union headquarters, specialist bookstores, embassies, places of cult, political party meetings, a protest, etc. – all places that can reveal an individual’s political, religious, philosophical, or other opinions.
142. This can chill individuals’ exercise of their rights in multiple ways. Knowledge that the Home Office and/or EMS (or other third parties) may see this information when reviewing trail data in case of breach alerts may lead individuals to restrain any “controversial” or “fringe” activities out of fear of such activities being consciously or unconsciously taken into account when assessing a breach and reviewing their bail conditions.

⁷⁶ Whatdotheyknow, Response to FOIA request from Brian Dikoff to the Home Office (18 January 2021), https://www.whatdotheyknow.com/request/absconding_rate#incoming-1706999.

⁷⁷ Home Office, ‘How many people are detained or returned?’ (18 June 2021), <https://www.gov.uk/government/statistics/immigration-statistics-year-ending-march-2021/how-many-people-are-detained-or-returned>.

⁷⁸ Application no. 31446/12 [2018].

143. The US Supreme Court recognised in *United States v. Jones*⁷⁹ that whatever actual or potential use of location data is made, GPS monitoring chills associative and expressive freedoms:

“Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may “alter the relationship between citizen and government in a way that is inimical to democratic society.”

144. Beyond the government’s processing of location data, GPS tags inhibit individuals’ freedoms of movement and association by physically burdening them with an undetachable object that is rife with social stigma. In the words of individuals who were fitted with tags:

“the tag was very visible – it’s much larger than the previous type of tag I had, and hard to hide. I felt that people were always looking at me, and I felt really embarrassed and again, quite paranoid.”⁸⁰

“Since the imposition of electronic monitoring via GPS on me, I feel that I have lost interest in doing anything. I feel that there is no hope for me in life. This is because I am finding myself spending almost all my time inside my house due to the shame and humiliation I feel as a result of being seen publicly with the tag as well as the limited battery life of the device and the length of time I have to spend charging it.

I find it extremely embarrassing to be around people since the tag was imposed, as I feel like I am still a criminal despite the fact that my sentence has concluded and I have not re-offended. I am constantly aware that everyone stares at me whenever I leave the house. This sense of embarrassment and feeling of being watched all the time is incredibly degrading.

[...] The presence of the tag has also impacted how much I see my girlfriend [REDACTED]. She spends much of her time with her family, including young children. Given the bulkiness of the tag, I don’t find it to be appropriate to be around the children in her family or for them to find out that I am subject to an electronic monitoring condition.”⁸¹

145. The mental toll and social stigma caused by GPS tags thereby lead to individuals refusing to partake in certain social activities and gatherings, thereby considerably limiting their freedoms of movement, expression, assembly and association:

⁷⁹ N 27.

⁸⁰ Anonymous testimony from a tagged individual, client of a law firm.

⁸¹ Anonymous testimony from a tagged individual, client of a law firm.

“The tag makes me isolate. I want to join the community for my future. It’s not comfortable when I go out, if it runs out of battery I will break the law. I stay out home all the time, sometimes I just go to buy food and not go anywhere. I don’t want people to see the tag and it’s not comfortable. But I have no choice. When I’ve been outside I’m not talking to anyone. Tag affects me when I want to join the community, do some sport and learning English or something like that. I like some sport like badminton or running but I’m just waiting for end of the GPS, but I don’t know how long.”⁸²

“Restricted social life to the one I used to have. Affecting me mentally definitely because being in the situation where I am. I used to be very sociable, got a group of friends and that. Now, the majority, when they know that I’m on the tag, they’re avoiding me, for no particular reason. I didn’t think that would be enough, someone who used to be a close friend are now avoiding me. They (friends) don’t want to associate with myself, or even if they do, you feel like there’s something there, it’s not like it used to be you know.”⁸³

146. Dr Monish Bhatia of Birkbeck University researched the psychological effects and mental health impact of electronic monitoring on migrants, drawing on eighteen months of ethnographic fieldwork. He found a number of ways in which EM was harmful for their health and well-being:

- (a) While EM is used for immigration control purposes rather than criminal offence punishment, because EM occurs soon after individuals are *“released from confinement (and completing a prison term), they experienced it as continuation of punishment.”*⁸⁴ This has to be considered in light of an overcriminalisation of migration, whereby *“the British government has created a ‘dragnet’ by moving immigration breaches from the civil domain and into the domain of criminal law.”*⁸⁵ As many such individuals are fleeing persecution and lives marked by trauma, *“subsequent imprisonment and punishment exacerbate their mental distress and/or create new conditions, and this results in (re)traumatisation.”*⁸⁶
- (b) EM is also harmful as it creates *“the suffocating feeling of being constantly watched and perceived as a ‘dangerous’ (non-white) person in public spaces”*.⁸⁷ This is a general and common feeling of those subjected to invasive forms of surveillance, that exacerbates their reticence to exercise their rights and freedoms.
- (c) Some individuals were also restricted from carrying out activities that weren’t prohibited in their bail conditions, because of excessive tagging. One individual enrolled in a college course requested that their monitoring times

⁸² Anonymous testimony from a tagged individual, client of a migrant rights organisation.

⁸³ Anonymous testimony from a tagged individual, client of a migrant rights organisation.

⁸⁴ Bhatia (n 55), p. 25.

⁸⁵ Monish Bhatia, ‘Crimmigration, imprisonment and racist violence: narratives of people seeking asylum in Great Britain’, *Journal of sociology* 56, no. 1 (2020), 36–52.

⁸⁶ Bhatia (n 55), p. 25.

⁸⁷ Bhatia (n 55), p. 30.

be adjusted to allow them to attend their lessons on time, but the Home Office refused – so that the individual has to arrive 45 minutes late every day.

147. This considerable impact on individuals' lives and mental health makes EM entirely disproportionate to its purposes. It extends their criminalisation beyond what the law provides for, instead of treating them as former offenders.
148. Despite this impact on individuals' fundamental rights, neither of the DPIAs provide an assessment of the risks to such rights. The Risks section in the 2020 DPIA only declares that the proposal does involve using new technology which might be perceived as being privacy intrusive, the only detail provided being "*Full movement monitoring to allow for effective control to removal.*" The 2021 DPIA, however, replies "Yes" to the question "*Are there any other known, or anticipated risks associated with the processing of personal data that have been identified by the project/ programme/initiative owner, which have not been captured in this document?*", and provides as detail: "*Disproportionate provision of Offending history and Health issues*". This is not further explicated, and does not cover the various risks to other rights of individuals.
149. This fails to comply with Article 24(1) DPA 2018, which requires that an identification and assessment of risk performed, including consideration of both the likelihood and the severity of any impact on the rights and freedoms of individuals.

VI. Lack of Safeguards

150. The Ministry of Justice has published guidance for the use of Electronic Monitoring in the context of probation: the HM Prisons and Probation Code of Practice for Electronic Monitoring (the "**Code of Practice**").⁸⁸ No equivalent document has been produced for use in the context of immigration bail. We have not fully assessed and reviewed this document in the context of its use in the criminal justice system. However, it is useful to consider when assessing whether there are the necessary sufficient safeguards in place in the immigration bail context to prevent against the misuse or abuse of location data.
151. The Code of Practice is accompanied by a Fair Processing Notice⁸⁹, which does not appear to exist in the immigration context. It states that:
- "*Personal data will be only be [sic] processed where there is a lawful reason to do so.*
 - "*Personal data will be held securely on the relevant electronic monitoring subject's record.*
 - "*At the end of the relevant electronic monitoring subject's requirement, personal data will be securely retained and only processed if there is a lawful reason to do so. Any data captured on one order that is relevant to*

⁸⁸ HM Prisons & Probation Service (n 60).

⁸⁹ Ministry of Justice, Fair Processing Notice for Electronic Monitoring Data, <https://www.gov.uk/government/publications/code-of-practice-electronic-monitoring>.

the management of another may be duplicated and retained against the latter.

- *Where necessary, adequate, relevant and not excessive, personal data may be shared with criminal justice agencies, including the Police, for law enforcement, or safeguarding purposes. Personal data will also be shared with agencies involved in managing compliance with electronic monitoring orders/licences.*
- *Personal data may be shared with government departments where necessary, such as in the case of legal proceedings.”*

152. The FPN also provides contact details of EMS to request exercise of data protection rights.

153. PI is not aware of any equivalent notice being provided in the immigration bail context. The only policy document is the Immigration Bail Guidance. But the Immigration Bail Guidance does not, unlike the Code of Practice, clarify *“expectations, safeguards and broad responsibilities for the collection, retention, processing and sharing of electronic monitoring data where it is personal data.”*⁹⁰ The Code states that it has been drafted in consultation with other government agencies and the Information Commissioner’s Office, whereas the Immigration Bail Guidance is a Home Office-owned document and there is no suggestion that it had input from, in particular, the Information Commissioner’s Office.

154. It is apparent from the Code of Practice that there are clear differences between the use of electronic monitoring in the criminal justice system and in immigration bail. For example:

(a) It is a decision for the criminal courts as to whether to impose an EM condition as part of a Court Order and it is incumbent upon them to consider any statutory safeguards and issues of fairness and proportionality. The probation service cannot do so of its own motion. By contrast, in the immigration context, the First Tier Tribunal’s authority is ousted in cases where electronic monitoring is mandatory and where the Home Office has chosen to include it as a condition of immigration bail. There is therefore no independent judicial scrutiny of the use of electronic monitoring in the immigration context.

(b) In the criminal justice context, EM is restricted to compliance with orders and licences. In the immigration context, trail data is used for purposes beyond monitoring compliance with immigration bail conditions, including to make substantive decisions on individuals’ Article 8 representations and further submissions.

155. In addition, the Code of Practice sets out the following condition for review of data:

⁹⁰ HM Prisons & Probation Service (n 60), p.2.

*“The location monitoring hardware and associated software will capture the subject’s location 24 hours a day in compliance with the order/licence. However, where location monitoring is only imposed to monitor a specific requirement/condition, such as an exclusion zone, active monitoring (i.e. reviewing the data rather than the data simply sitting in the system) of the location information will only take place if there is a lawful reason to do so e.g. following a breach of the requirement/condition and only where it is proportionate and **necessary**. It will not be actively monitored at other times.”*⁹¹ [emphasis added]

156. By contrast, the 2021 DPIA only provides that *“The review consideration may be informed by the mitigation supplied and the review of the full trail monitoring data records where proportionate and **justified**.”* [emphasis added] “Justified” is a much lower standard than “necessary”.

157. In the Council of Europe, Recommendation CM/Rec(2014) 4 of the Committee of Ministers to member states on electronic monitoring⁹² noted in particular that:

- (a) *“electronic monitoring technologies should be used in a well-regulated and proportionate manner in order to reduce their potential negative effects on the private and family life of a person under electronic monitoring and of concerned third parties”*
- (b) *“rules about limits, types and modalities of provision of electronic monitoring technologies need to be defined in order to guide the governments of the members States in their legislation, policies and practice in this area”*
- (c) *“ethical and professional standards need to be developed regarding the effective use of electronic monitoring in order to guide the national authorities, including judges, prosecutors, prison administrators, probation agencies, police and agencies providing equipment or supervising suspects and offenders”.*

158. The “Basic Principles” laid out in this recommendation include:

- (a) the duration of electronic tagging should be regulated by law;
- (b) decisions should be taken by the judiciary or allow for judicial review;
- (c) use should be proportionate in terms of duration and intrusiveness to the seriousness of the offence alleged or committed;
- (d) *“When imposing electronic monitoring and fixing its type, duration and modalities of execution account should be taken of its impact on the rights and interests of families and third parties in the place to which the suspect or offender is confined”;*

⁹¹ HM Prison & Probation Service (n 60), § 17.

⁹² (19 February 2014), <https://pjp-eu.coe.int/documents/41781569/42171329/CMRec+%282014%29+4+on+electronic+monitoring.pdf/c9756d5b-be0e-4c72-b085-745c9199bef4>

- (e) *“handling and shared availability and use of data collected in relation to the imposition and implementation of electronic monitoring by the relevant agencies shall be specifically regulated by law”;*
- (f) *“Staff responsible for the implementation of decisions related to electronic monitoring shall be sufficient in number and adequately and regularly trained to carry out their duties efficiently, professionally and in accordance with the highest ethical standards. Their training shall cover data protection issues.”*

159. None of these principles have been applied by the Home Office to its GPS tagging of migrants. While judicial review of the imposition of EM is an option for tagged individuals, the new mandatory duty creates a very high threshold for such a challenge to succeed – and most people are unable to access the high quality, independent legal advice they would need to bring such a claim.

160. The lack of limitation on the duration of tagging in the legislation is of particular concern. And while the Home Office is required to review the use of EM at 3-month intervals to ensure that its use remains proportionate,⁹³ the ICIBI’s inspection found that:

“EM reviews of those already fitted with a tag, which should be undertaken at 3-monthly intervals, were only being conducted when representations were received in respect of an individual.

5.81 There was a backlog of 818 EM reviews (out of 1,622 active EM cases) which should have had a 3-monthly review (Figure 14). Managers said they were “unable” to do EM reviews due to lack of resources, and that PAPs and JRs were prioritised due to the set reply times. The effect of this was that only those persons with access to legal advice would have the benefit of a such a review.”⁹⁴

161. The ECtHR in *Uzun v. Germany* considered that the GPS surveillance at issue in the case was proportionate because, amongst others: domestic law subjected the authorisation of the surveillance measure to very stringent conditions, the GPS surveillance had only been ordered after other less intrusive means of investigation had proved ineffective, and it had been carried out for a relatively short period of time. Safeguards for strict authorisation conditions, limited duration and consideration of less intrusive means are not features of the Home Office policy and practice of GPS tagging of migrants.

162. This lack of safeguards, combined with the risk of excessive data collection and extension of purpose, is deeply concerning. It shows disregard for the risks to

⁹³ The Home Office Immigration Bail policy states “The use of EM and all supplementary conditions to EM must be reviewed by a decision maker in any case allocated to them: • on a quarterly basis • when they receive any representations on the matter, including requests to vary the condition, from the individual or a person acting on their behalf • whenever information on a breach of the condition is received • when a request is made by another decision maker”.

⁹⁴ ICIBI (n 3), § 5.80-5.81.

individuals and significant power imbalance these create between tagged individuals and the Home Office.

VII. Applications / Remedy

163. For the reasons above, PI requests that the ICO issue an assessment notice under section 146 of the DPA 2018, investigates the Home Office GPS tagging of migrants, under Article 58(1) of the UK GDPR, and considers the compliance of the use of GPS tags by the Home Office with the seven data protection principles.
164. In summary, PI invites the Commissioner to consider in particular:
- (a) The lawfulness, fairness and transparency principle – in light of the lack of legal basis for all of the Home Office’s processing activities, considerable impact on individuals’ rights and freedoms, and lack of transparency towards data subjects;
 - (b) The purpose limitation principle – in light of the excessive re-use of trail data beyond scope of the legislation; and
 - (c) The accuracy principle – in light of frequent location data inaccuracies and tags’ poor battery life, and the significant adverse consequences of these inaccuracies.
165. PI requests that the ICO issue an enforcement notice under section 149 of the DPA 2018, requiring the Home Office to stop all collection and processing operations on personal data of data subjects through GPS tags, under Article 58(2)(f) of the UK GDPR. In the alternative, PI requests that the ICO issue an enforcement notice requiring the Home Office to bring processing operations into compliance with the UK GDPR, under Article 58(2)(d) of the UK GDPR.

Privacy International

17 August 2022

Annex A – Summary of PI’s Expertise in Migration Issues

1. PI has specific expertise in the defence of privacy rights in migrant communities. It has for a few years been investigating, analysing and challenging the exploitation of data and new technologies as it relates to the rights of migrants in the UK and abroad.
2. In July 2019, PI joined migrant organisations in a formal complaint⁹⁵ 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.
3. In February 2021, PI published a report on the UK’s migration surveillance regime.⁹⁶ This report resulted from extensive research and investigations, using procurement, contractual and open-source data, into the use of surveillance systems and tools by HM Government to police the UK’s borders.
4. PI regularly publishes various analyses of threats to the privacy of migrant communities⁹⁷ and primers on technologies used for migration surveillance, including one published on 21 July 2021 on satellite and aerial surveillance.⁹⁸ Of direct relevance to this complaint is a primer we published on 9 February 2022 on electronic monitoring using GPS tags.⁹⁹
5. On 23 May 2022 PI made submissions to the Independent Chief Inspector of Borders and Immigration in relation to the Inspector’s investigation into the Home Office use of satellite tracking.¹⁰⁰
6. PI was granted permission to intervene in the recent case of *R (on the application of HM, MA and KH) v SSHD* [2022] EWHC 695 (Admin) which challenged the Defendant’s policy and practice of seizing mobile phones of migrants who arrived in small boats on the south coast of England for a period of some months in 2020, and of performing mobile phone extraction (“**MPE**”). PI provided a detailed witness statement concerning the use of MPE, explaining the technical functioning of MPE technology and resulting privacy concerns.¹⁰¹ The court

⁹⁵ PI, ‘Privacy International is joining migrant organisations to challenge the UK’s “immigration control” data protection exemption - find out why!’ (10 July 2019), <https://privacyinternational.org/news-analysis/3064/privacy-international-joining-migrant-organisations-challenge-uks-immigration>.

⁹⁶ PI, ‘The UK’s Privatised Migration Surveillance Regime: A Rough Guide for Civil Society’ (February 2021), https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf.

⁹⁷ PI, ‘10 threats to migrants and refugees’ (8 July 2020), <https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees>.

⁹⁸ PI, ‘Satellite and aerial surveillance for migration: a tech primer’ (21 July 2021), <https://privacyinternational.org/explainer/4595/satellite-and-aerial-surveillance-migration-tech-primer>

⁹⁹ PI, ‘Electronic monitoring using GPS tags: a tech primer’ (9 February 2022), <https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer>.

¹⁰⁰ PI, ‘Privacy International’s submissions for the Independent Chief Inspector of Borders and Immigration Inspection of the Satellite Tracking Service Programme’ (23 May 2022), https://privacyinternational.org/sites/default/files/2022-05/Submissions%20to%20ICIBI%20FINAL%2023.05.2022_0.pdf.

¹⁰¹ PI, ‘*R (HM and MA and KH) v Secretary of State for the Home Department* – Case Page’, <https://privacyinternational.org/legal-action/r-hm-and-ma-and-kh-v-secretary-state-home-department>.

found that section 48 of the Immigration Act 2016 did not authorise the Defendant to search individuals and seize their phones, and that the secret and blanket seizure and extraction policy violated Article 8 of the European Convention on Human Rights.