Statement on behalf of Privacy International
Witness: Jonah Mendelsohn (JM)
Statement: First
Exhibit: 1
Date: 18 August 2023
JR-2022-LDS-000055

IN THE UPPER TRIBUNAL
IMMIGRATION AND ASYLUM CHAMBER

IN THE MATTER OF CLAIM FOR JUDICIAL REVIEW

BETWEEN: -

THE KING
On the application of
MARK ANTHONY NELSON

Applicant

-and-

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

FIRST WITNESS STATEMENT OF JONAH MENDELSOHN
(PRIVACY INTERNATIONAL)

I, Jonah Mendelsohn, Solicitor of Privacy International, 62 Britton Street, London, EC1M 5UY, SAY AS FOLLOWS:

A. INTRODUCTION

1. I make this statement in support of the Applicant's application for judicial review to assist the Tribunal by providing factual information about the Respondent's use of "Satellite Tracking Services (STS) GPS Electronic Monitoring". This system is run by Electronic Monitoring Services ("EMS"), managed by private company Capita, under contract with the Ministry of Justice. The Satellite Tracking Services use the Global Positioning System ("GPS")

technology to determine location and then electronically monitor individuals. GPS technology is a system of around 30 satellites that provide accurate positioning information worldwide.

2. I am a solicitor and legal officer at Privacy International ("PI"). I was admitted as a solicitor in August 2022 after training at Duncan Lewis Solicitors, where I qualified as a Solicitor in the Public Law Team.

3. Since joining PI, I have assisted in coordinating our work on the use of satellite tracking and GPS tagging by the Respondent. I work hand in hand with our team of technologists who have performed technical research into GPS tags that PI were able to purchase on the open market. This included testing them in real conditions by wearing the tags over periods of time and thereby acting as both the tagged individual and the controlling authority we were able to review the data generated by the devices.

4. I am authorised to make this statement on behalf of PI. Where I rely on sources other than my own knowledge, I identify them below. Where the facts and matters to which I refer in this statement are within my own knowledge I confirm that they are true. Where they are based on information obtained from other sources (which sources I shall endeavour to identify), I confirm that they are true to the best of my knowledge and belief.

5. This statement addresses the following topics:

    5.1. **Section B** provides information about PI and our work in this field, including in relation to our work on the Respondent's deployment of GPS monitoring;
    5.2. **Section C** explains how GPS tags technology works, what data they collect and how intrusive this can be; and
    5.3. **Section D** looks at reliability concerns including the accuracy and reliability of the data generated by the tags, including the role of GPS

and phone signals in the accuracy of the devices used by the Respondent. This section also addresses a number of assertions made by the Respondent in this claim (in both her witness evidence and pleadings) in relation to the operation of the Applicant's GPS tag.

6. Both sections C and D rely on the technological research carried out by our technologists who *inter alia*, through their expertise in disciplines such as Computer Science and/or Electronic Engineering, analyse devices and applications, and their generation and uses of data in order to uncover how data is exploited by governments and corporations.

B. PRIVACY INTERNATIONAL

7. PI is a London-based charity (Charity Number: 1147471) that seeks to protect the qualified right to privacy.

8. PI has acted as claimant and intervener in many cases involving the right to privacy in the courts of the United Kingdom (in particular The Investigatory Powers Tribunal and on appeal, reference or application to the Supreme Court, Court of Justice of the European Union ("CJEU") and European Court of Human Rights),[1] Colombia, Kenya, France, Germany, South Korea, the United States and the European Union, as well as at the European Court of Human Rights.[2]

9. Privacy International intervened in *Secretary of State for the Home Department v Watson* (C-698/15) before the European Court of Justice on 25 February 2016 that was joined with the Tele2 case. This case successfully challenged the UK's data

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

[2] PI, 'Legal Action', https://privacyinternational.org/legal-action/

retention regime in respect of communications data (including traffic and location data) set out in the Data Retention and Investigatory Powers Act 2016.[3] Subsequently, Privacy International brought another case before the CJEU that resulted in a finding that UK legislation was incompatible with EU law.[4] Privacy International was also a party to the *LQDN, FDN and others v France* case before the CJEU concerning the retention of personal data under French law which resulted in a similar finding of incompatibility against France.[5]

10. In a 2018 report,[6] PI together with the International Committee of the Red Cross examined risks related to metadata, being the data that describes and gives information about other data and can include location data.

11. PI has specific expertise in the context of privacy rights in migrant communities. In July 2019, PI joined migrant organisations in a formal complaint[7] 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.

12. In November 2020, PI obtained documents from EU agencies evidencing the outsourcing of border surveillance and controls by the EU to neighbouring countries,[8] and wrote to the European Commission calling for stricter safeguards and oversight of aid funds.[9]

---

[3] PI, 'Tele2/Watson', https://privacyinternational.org/taxonomy/term/410
[4] PI, 'CJEU Bulk challenge', https://privacyinternational.org/legal-action/cjeu-bulk-challenge
[5] https://privacyinternational.org/legal-action/lqdn-fdn-and-others-v-france
[6] PI and ICRC, 'The Humanitarian Metadata Problem: "Doing No Harm" In The Digital Era' (October 2018), https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf
[7] 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
[8] PI, 'Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls' (November 2020), https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border
[9] PI, 'Surveillance Disclosures Show Urgent Need for Reforms toEU Aid Programmes' (November 2020), https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes

13. In February 2021, PI published a report on the UK's migration surveillance regime[10]. This report resulted from extensive research and investigations, using procurement, contractual and open-source data, into the use of surveillance systems and tools (including mobile phone extraction which is utilised in part to track location data via GPS and the move towards satellite tracking more generally (p32; p36)) by HM Government to police the UK's borders.

14. PI gave written evidence[11] to the Justice and Home Affairs Committee whose report '*Technology rules? The advent of new technologies in the justice system*'[12] refers to PI's submissions.

15. PI regularly publishes various analyses of threats to the privacy of migrant communities[13] and primers on technologies used for migration surveillance, including one published on 21 July 2021 on satellite and aerial surveillance.[14] Of direct relevance to this claim is a primer we published on 9 February 2022 on electronic monitoring ("EM") using GPS tags.[15]

16. On 20 January 2022, PI wrote to the Forensic Science Regulator raising concerns about the quality of digital evidence with relevance to Immigration Officers and broader use by the Home Office. This included raising concerns about GPS

[10] PI, 'The UK's Privatised Migration Surveillance Regime: A RoughGuide for Civil Society' (February 2021), https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf
[11] https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/publications/written-evidence
[12] (30 March 2022), https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law
[13] PI, '10 threats to migrants and refugees' (8 July 2020), https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees
[14] 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.
[15] PI, 'Electronic monitoring using GPS tags: a tech primer' (9 February 2022), https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer

tags.[16] We have made oral and written submissions[17] to the Independent Chief Inspector of Borders and Immigration in relation the Inspector's investigation into the Home Office's use of satellite tracking.

17. On 17 August 2022, PI filed complaints regarding the Home Office's GPS tagging scheme with the Information Commissioner ("ICO") and Forensic Science Regulator ("FSR").

18. Both complaints raised concerns in relation to quality and accuracy issues in the GPS ankle tags used by the Respondent in her tracking programme. Many of the issues raised in this claim were covered in those submissions, in particular problems with the functioning of the batteries and chargers with which the devices are equipped as well as the accuracy of the locational data they collect.

19. In respect of the complaint to the ICO, we received confirmation in November 2022 that our complaint was being investigated and that enquiries would be put to the Respondent. We were informed on 11 May 2023 that the ICO's enquires with the Respondent were still ongoing.

20. We have similarly followed up the complaint to the FSR and we were informed that enquiries had been made to the Respondent's Immigration Enforcement ("IE") department. The FSR informed us that its enquiries would be limited to the use of GPS tags in criminal investigations and prosecutions due to the nature of its mandate. The FSR subsequently explained that the Respondent replied to its enquiries by stating that any criminal investigation carried out by the IE would comply with internal guidance pursuant to the Data Protection Act 2018 including in relation to sensitive processing.

---

[16] PI, 'Letter to Gary Pugh' (20 January 2022), https://privacyinternational.org/sites/default/files/2022-01/Letter%20to%20UK%20Forensic%20Science%20Regulator.pdf

[17] PI, '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

21. PI was also 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 Respondent'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. The Home Office in that case, having consulted a specialist, accepted that our evidence was "*accurate*". The court 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 ("ECHR").

22. It is hoped that PI's expertise will be of assistance in this claim both to provide details as to the technical nature of this form of surveillance and the extent of the interference with privacy occasioned by it.

C. THE TECHNOLOGY - GPS TAGS FUNCTIONING AND DATA COLLECTION

23. Prior to January 2021, the Respondent used Radio Frequency ("RF") tags for her EM programme, which required the installation of a base station within the individual's house and were mainly used to enforce curfew conditions.

24. Through a change to her Immigration Bail policy, she introduced the use of GPS technology via ankle tags. More recently, in November 2022, the Respondent began to deploy non-fitted GPS trackers ("NFDs") equipped with fingerprint scanning technology in conjunction with the ankle tags.

25. In this section, I will explain the way GPS tagging technology works, relying on the research, which as mentioned above, was carried out by our technologists

including on two models of GPS tracker, which PI purchased on the open market, namely Megastek Technologies – MT60X (the "MT60X") and the ThinkRace - TR40 (the "TR40").[18]

26. While we have not seen what model of GPS tracker is supplied to the Defendant by G4S, we obtained alternative products that we believe are likely to have similar specifications, as all models of GPS trackers we have reviewed, based on their online marketing materials, offer similar functions and capabilities, including in relation to the tracking intervals.[19]

27. In this statement, I rely on my review of the latest Immigration Bail guidance (Version 16.0) published by the Home Office on 8 August 2023 (the "Bail Guidance")[20], the Immigration bail conditions: Electronic monitoring (EM) expansion pilot guidance (Version 2.0) published by the Home Office on 23 June 2023 (the "Pilot Guidance"),[21] the Data Protection Impact Assessment performed on 8 June 2022 (the "Expansion Pilot DPIA") and the Data Protection Impact Assessment performed on 19 August 2021 (the "2021 DPIA").

28. The Respondent has stated via a previous version of her Bail Guidance that the GPS devices have a dual capability to use GPS and radio frequency technology.[22] The previous version of the Bail Guidance also states that a curfew is not mandatory as a result of using a GPS device to electronically monitor a person,

---

[18] PI, 'Life under 24/7 GPS surveillance - A GPS ankle tag experiment' (5 May 2023), https://privacyinternational.org/long-read/5064/life-under-247-gps-surveillance-gps-ankle-tag-experiment

[19] PI, 'Life under 24/7 GPS surveillance - A GPS ankle tag experiment' (5 May 2023), https://privacyinternational.org/long-read/5064/life-under-247-gps-surveillance-gps-ankle-tag-experiment

[20] Immigration Bail Policy, version 16.0 (8 August 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1177994/Immigration_bail.pdf

[21] Immigration bail conditions: Electronic monitoring (EM) expansion pilot, version 2.0 (23 June 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1165035/Immigration_bail_conditions_-_Electronic_Monitoring__EM__Expansion_pilot.pdf

[22] Immigration Bail Policy, version 13.0 (1 November 2022), https://webarchive.nationalarchives.gov.uk/ukgwa/20221109120403/https://www.gov.uk/government/publications/offender-management/immigration-bail-accessible-version

because location monitoring is 24/7. The Respondent further stated in this version (13.0) of the Bail Guidance that: *"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* ("HMU") *is installed."*

29. I note that the current version of the Bail Guidance omits the above reference to the GPS devices having a dual RF-GPS capability. It is unclear to me whether this is because the Respondent has procured new GPS devices with altered capabilities, even as the supplier (G4S) remains the same.

30. Nevertheless, the current Bail Guidance suggests that HMUs (and by extension GPS tags with dual capabilities) may continue to be installed in the properties of individuals subject to EM conditions[23]. The current version of the Bail Guidance states that in the alternative of an HMU, "*a mobile phone will be issued to the person to allow contact to and from the EM supplier*." No other information is provided about the accompanying mobile phones, including what categories of personal data they collect and process. This is similarly not covered in the Expansion pilot DPIA nor in the 2021 DPIA.

How Radio Frequency tags work

31. Traditional radio frequency tags rely on two different elements, a base station usually located in the individual's house and connected to the network and a tag attached to the individual (the HMU). 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.

[23] Immigration Bail Policy, version 16.0 (8 August 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1177994/Immigration_bail.pdf

32. The tag therefore only "communicates" with the monitoring unit, which in turn 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.

33. The HMU will usually have a signal detecting range that can be set to cover the size of "most domestic dwellings". This means that the main capability and purpose of a radio frequency tag is to enforce curfew conditions, such as that an individual remains at home from 7pm to 7am.

How GPS technology underpinning the tags works

34. Whereas RF tags tell the tagging authority whether the tag wearer is observing a curfew, i.e., that the tag is within the vicinity of the monitoring box, GPS tags provide the authority with a *complete* location history, that is a log of where the tracked individual was at all times. The locational data (the "Trail data") can be accessed directly by control-centre personnel and can be monitored by software.

35. GPS tags 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. The tag also contains a SIM card (or equivalent) to authenticate it to the network.

36. GPS 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. 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. When GPS is unavailable or weak, GPS devices track location using GPS signals backed up by mobile signals.

37. The mobile network will do this by triangulating data using Global System for Mobile Communications ("GSM") cell-based data. GSM is a protocol that enables communication on a cellular network. It is equivalent to a "2G" cellular network. However, the device can also communicate with other generations of cellular network, such as 4G. This means that a tag can work out location using the mobile phone masts with which the SIM card communicated with at a certain time.

38. As noted by the Forensic Science Regulator,[24] cell site analysis relies on the acquisition of communications data, the processing of those data and the presentation of those data in the form of maps and tables.

39. 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. The SIM card or equivalent will authenticate the tag to the network.

40. 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 other words location is worked out using the mobile phone masts which the SIM card communicated with at a certain time.

41. In the UK, like in several countries around the world, telecommunications operators are legally compelled to store communications records. This means that the communications data generated by the tags is not only being shared with

[24] Forensic Science Regulator, 'Codes of Practice and Conduct - Appendix: Digital Forensics – Cell Site Analysis' (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/918946/135_FSR-C-135_Cell_Site_Analysis_Issue_2.pdf

the EMS, the Home Office, the Ministry of Justice, and Law Enforcement, it is also being processed and may be retained by the relevant telecommunications operator.

42. As per the Applicant's trail data, which was provided to me by his legal representatives, his GPS tag is set to record his locational data at tracking intervals of every minute or less. As addressed below, the deployment of 24/7 GPS monitoring (as confirmed in the Bail Guidance and the DPIAs) at intervals of every minute enables the controller to collect sensitive categories of personal data and build up an all-encompassing profile of the subject and those around them.

The physical design of GPS ankle tags

43. The GPS tag itself is attached to the ankle, using a reinforced band. It has been described in the Scottish Government consultation report as larger and heavier than RF tags.[25] This is the result of it having to accommodate a larger battery, as GPS technology is much more battery intensive than radio frequency technology and needs to be charged more often.

44. The Respondent's design of the tagging system contributes extensively to the drain on battery life as 24/7 live location at very frequent intervals is highly draining for the battery life of GPS devices. The Reform report '*Cutting crime: the role of tagging in offender management*' dated September 2015 stated that:[26]

> *"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*

[25] 'Development of Electronic Monitoring in Scotland A Consultation on the Future Direction of the Electronic Monitoring Service' (September 2013), https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf
[26] Reform, 'Cutting crime: the role of tagging in offender management' (September 2015), https://www.bl.uk/collection-items/cutting-crime-the-role-of-tagging-in-offender-management

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..."

Trail Data

45. Trail data refers to the complete location history of the person who is wearing the tag, i.e. a log of where the person has been minute-by-minute of every day. As such, the use of GPS tracking is a significant change in the surveillance of migrants, enabling the constant monitoring of an individual's location which is then stored for passive review and potential further analysis. It also permits live tracking of an individual, i.e., the following of their movements on a regular basis. The DPIAs state that trail data is stored for a minimum of six years after the tag is removed.

46. Trail data is particularly (1) voluminous, (2) sensitive, (3) granular and (4) open to interpretation.

47. **First**, the volume of data collected through live location tracking on a 24/7 basis at 1-minute intervals is enormous.

48. The GPS tags worn by PI's technologists were tested with different location and data collection intervals. The locational data was then collected in Excel spreadsheets in an identical fashion to the Applicant's trail data (i.e. the spreadsheets displayed a list of location coordinates along with the hour, minute and second at which it was recorded). This resulted in various 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, for example when the subject is sleeping or working at their desk).

b. 30 second intervals led to approximately 30,000 entries over a 2.5-month period (same as above, the tag does not ping if it doesn't move, and our technologist did not even wear the tag constantly over the 2.5 months).

49. **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 and familial relationships, political, religious or philosophical interests, health concerns, consumption patterns, etc. The Respondent's own Expansion Pilot DPIA acknowledges that the nature of the data is sensitive (p5). When and how a person moves around can therefore reveal a considerable amount of information about their life and personality, including data that would be considered 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; and
f. data concerning a natural person's sex life or sexual orientation – trips to gay bars or attendance at gay pride.

50. **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 belief – 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.

51. The granularity, sensitivity, and all-encompassing nature of the data that is collected through GPS monitoring is underlined by a number of points made by Stephen Murry ("SM") at §10 of his witness statement (dated 7 August 2023) filed on behalf of the Respondent. SM notes that trail data could be used in place of other potentially corroborative evidence in the consideration of human rights claims under Article 8 ECHR so as to avoid delays in the determination of applications. He suggests by way of an example that trail data could be used to confirm the closeness of a relationship between an applicant and the children of a new partner. SM proffers a scenario in which the hypothetical applicant claimed that one of the children had chronic health conditions and that they regularly sleep at the hospital with the child to enable the partner to look after the other children. SM goes on to suggest that trail data could confirm these hospital visits without the need to contact hospital staff. This is of particular relevance to the Applicant in this case (who has a number of children) as it demonstrates that the Respondent, through an EM condition, could collect and process personal data relating to a child.

52. In the scenario proposed by SM, the Respondent is very likely to receive sensitive data pertaining to the child's medical condition such as medical records. If the Respondent has access to such medical records alongside a tag wearer's trail data, they will be able to build up a granular profile not only of the Applicant's movements and personal information, but also those of the child. This combining of datasets, known as the "mosaic-effect", enables the entity that holds the data to reveal new, previously undisclosed, information about a data

subject[27] (often without their knowledge or consent).

53. The same phenomenon is likely to occur if the Respondent was seeking to corroborate a claim that an applicant brings the child in question to school every day or that they take the child with them to attend religious worship together. Not only would the Respondent have highly granular access to the child's movements at specific times of the day, but she would also be processing sensitive, special categories data relating to the children, including for example in relation to health or religious beliefs. It is unclear to me whether the Respondent has proper safeguards in place, including a DPIA that assesses the risks to children of this form of processing, to adequately police this possibility.

54. **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 Respondent to make fundamentally wrong assumptions about an individual's movements and activities. Research by our technologists showed that by clicking the various pins of the map recording their location data, one could figure out the precise times at which the tagged individual was in certain locations, how long they remained there, and so on. However, by showing this to different PI staff members, we saw that different people were drawing widely divergent interpretations of the individual's activities.

The Respondent's access to the trail data

55. The Bail Guidance (Version 16.0) explains that the trail data is held by EM Hub, but that the Home Office may access this data for a number of purposes, where

[27] Jill Capotosto, 'The mosaic effect: the revelation risks of combining humanitarian and social protection data' (9 February 2021) https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/

"*proportionate and justified in the circumstances in accordance with data protection law*", including:

a. In the event an individual has breached their bail conditions (by for example absconding);
b. In order to investigate alleged breaches of EM conditions and immigration bail conditions more broadly;
c. When reviewing submissions made on the basis of Article 8 ECHR; or
d. To respond to External Agency Requests and Subject Access Requests.

56. Each of the purposes listed above at §55(a); (b) and (c) all permit the Respondent to view an individual's *entire* trail data rather than targeted and specific locational data relating, for example, to the time at which a breach of immigration bail took place.[28] The Bail Guidance also states that where trail data is reviewed for one purpose a distinct review of the entire data-set can be carried out for a different purpose in the event that: "*it becomes apparent that further breaches of immigration bail conditions may have been/ are being committed (for example, trail data provides a strong indication that the person is working in breach showing them at a specific location other than home between 08:00 – 17:00 hours)*". The Guidance explains that in such a scenario the data could be shared within different Home Office departments to investigate further possible immigration breaches and to Law Enforcement agencies where there is an "*indication that criminal activity has taken place*".

57. This is concerning, given the risk that inaccurate trail data could lead to further processing and sharing of large volumes of trail data in ways that are likely to be completely unforeseeable to the tag wearer.

D. RELIABILITY CONCERNS

[28] Immigration Bail Guidance, version 16.0 (8 August 2023), pp 54-55, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1177994/Immigration_bail.pdf

Accuracy and reliability of GPS tags data

58. 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).[29] All these factors affecting accuracy of GPS location data can give rise to errors of 100 meters or more.[30] In addition, while GPS usually works in most domestic homes, it may not work inside all buildings, and while it usually works whilst travelling in cars, it may not work on trains. Drift (movement in the accuracy of signal) might also occur when static for certain periods of time, and near waters.[31]

59. As above, the ankle tags deployed by the Respondent collect locational data via satellite or mobile phone signals (if there is weak or no satellite signal). This is confirmed by the response to the subject access request the Applicant submitted to EMS/the Respondent, which refers to this mode of tracking as Location Based Services ("LBS"). In the disclosure received by the Applicant, the Respondent notes that: "*LBS is a tracking system that uses mobile phone signal. The tracking is done using GSM cell towers of local mobile phone service providers. Tracking through LBS is less precise when compared to GPS because the device estimates its position in the area of the cell tower.*"[32]

---

[29] 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
[30] PI, 'GPS tracking and COVID-19: A tech primer' (7 May 2020), https://privacyinternational.org/explainer/3753/gps-tracking-and-covid-19-tech-primer.
[31] Scottish Government, 'A Consultation on the Future Direction of the Electronic Monitoring Service' (September 2013), https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf
[32] Exhibit 08 to EMS Witness Statement dated 13 June 2023 as contained in the response to the Respondent's Subject Access Request dated 12 July 2023.

60. As per the Applicant's trail data, his GPS tag was collecting trail data through LBS at numerous intervals. This is consistent with the poor GPS signal in the area in which the Applicant resides, which is set out in the parties' pleadings and evidence.

61. I have seen a draft of the Applicant's fourth witness statement, in which he and his legal representatives reviewed a sample of his trail data. §X of the Applicant's fourth witness statement highlights how 22 entries are inaccurate. This includes a number of entries in which the Applicant was placed [redacted], including on a path, as well as in a cemetery. The Applicant states at §X of his fourth witness statement that he would have no reason to be at these locations.

62. In our research, as both the wearers and the controllers of the GPS devices and accompanying locational data, our technologists were able to check the data recorded by the device against the actual location of the wearer. This revealed a number of instances where the location points recorded were similarly inaccurate, including where the wearer was marked in a different place than their actual location. For example, in exhibit JM1, showing a portion of the MT60X's trail data visualisation platform, each pin shows where the wearer was at 30 seconds intervals. We know from our technologist that they were at the time [redacted]. The fourth data point (from right to left on the trail) appears off road, in the middle of a church. We know from our technologist that he did not [redacted] or enter the church at any point.

63. The location data was also sometimes inaccurate when the wearer was at home and not moving. In one such example, our technologist was at home; however, the tag recorded that he was located in the next street for a period of 6 hours. I have checked the screenshots that record this error but have not exhibited them because they reveal our technologist's address.

64. In circumstances where GPS location is used to monitor compliance with bail conditions and to consider representations or submissions in relation to immigration claims made under Article 8 ECHR, inaccuracies, even small, could 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 forbid them from working, this can lead to wrongful accusations of breach to be made against them.

65. As in the example of the trail data erroneously indicating that our technologist was not at his home, incorrect locational data could lead to an inference over a period of time that an individual is not complying with a residence condition. Similarly, in the case of the example in SM's statement dated 7 August 2023, if the hypothetical applicant was consistently placed in a park near the hospital (or even further away given the locational entries that erroneously placed the Applicant in this case by a river in the countryside) – this could be used as evidence to dismiss an individual's immigration application made on human rights grounds.

66. The risk of such adverse and misleading inferences being drawn is particularly stark in circumstances where the Respondent is able to access a wearer's entire trail data and carry out multiple reviews for differing purposes.

67. The issue of the accuracy of trail data and therefore the compliance of the EM program with Article 5(1)(d) of the UK GDPR (the "Accuracy Principle") is a live one in PI's pending complaint before the ICO.

The failure of the Applicant's GPS tag to collect trail data

68. Having reviewed the Applicant's trail data, I am able to see that his previous GPS tag did not consistently collect trail data for a period of approximately 5.5 months with it not collecting *any* trail data over five distinct periods, the

longest of which was 6 weeks. At §23 of the Respondent's Amended SGD, she suggests that: "*the issue with the GPS signal might have been caused by the tag not being charged correctly… there is a correlation between signal issues and battery drainage, as the tag has to work harder in order to obtain a signal and therefore the battery depletes more quickly*".

69. As explained above, GPS tags receive location signals from satellites, and they do not send any return signals: the devices are passive. Therefore, the device would not consume more energy such that the battery would deplete more quickly if it did not receive any GPS signals or if the signal was poor. However, as stated above, when GPS is unavailable or weak, GPS devices will collect trail data using mobile signals (LBS). In these circumstances, the device is in effect having a 'two-way conversation' with telephone masts. As such, where the device is relying solely on mobile signals the drain on the battery is likely to be extensive.

70. It is therefore unclear to me what the Respondent means when she states that the signal difficulties were caused by the device not being charged correctly. The extent to which the Applicant charged his device has no impact on GPS signal and/or mobile signal and or vice versa. However, if as appears to be the case, the device was reliant on mobile signals any resultant drain on the battery is outside of the Applicant's control and would take place even if he was charging his tag.

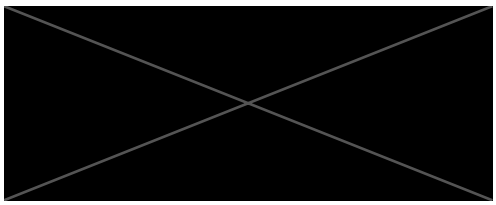
71. If the periods where the device was wholly out of contact are attributable to signal issues, there would have to have been intervals where there was no signal at all. This is possible given that the Respondent states that the signal was extremely poor in the area in which the Applicant resides.

72. In the Amended SGD the Respondent discloses that works are being carried out on a nearby telephone mast. She correctly states that this could potentially have impacted "*the ability of the tag to transmit the data*". As above, the device

can continue to collect locational data through the pings between the mobile phone masts and the SIM card contained in the device. This takes place by way of triangulation between the device and local telephone masts. Thus, the impact of the nearby mast underdoing work is dependent on whether there are other local masts that could have enabled the device to continue to transmit the trail data. The date of when the construction works started would also be material to determining the role of the telephone mast in the periods in which the tag was out of contact.

Statement of Truth

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

Signed by: 

Name: Jonah Mendelsohn

Date: 18 August 2023