Statement on behalf of Privacy International
Witness: Lucie Audibert (LA)
Statement: First
Exhibit: LA1, LA2 and LA3
Date: 10 November 2022
CO/ /2022

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

BETWEEN

THE QUEEN
(on behalf of [redacted]

Claimant

And

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

WITNESS STATEMENT OF LUCIE AUDIBERT
(PRIVACY INTERNATIONAL)

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

A. INTRODUCTION

1. I make this statement in support of the Claimants' application for judicial review to assist the Court by providing factual information about the Home Office 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 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 on 15 September 2020 after training at Taylor Wessing LLP, where I qualified as an Associate in the IP and Technology Litigation department.

3. Having worked at PI for two years, I am responsible for our work on the use of satellite tracking and GPS tagging by the Home Office. I work hand in hand with our team of technologists who have performed technical research into GPS tags.

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;
    5.2. **Section C** explains how GPS tags technology works, what data they collect and how intrusive this can be, as well as contractual arrangements between various parties in the GPS tagging scheme; and
    5.3. **Section D** looks at reliability concerns including the accuracy and reliability of GPS tags data, battery life issues, and breach notification.

B. PRIVACY INTERNATIONAL

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

7. 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 ("IPT") and on appeal, reference or application to the Supreme Court, 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.

8. PI intervened in *Secretary of State for the Home Department v. Watson* (C-698/15) before the CJEU on 25 February 2016 that was joined with the *Tele2 Sverige* case. This case successfully challenged the UK's data retention regime in respect of communications data (including location data) set out in the Data Retention and Investigatory Powers Act 2016. On 26 November 2018, Privacy International submitted its intervention to the Court of Justice of the European Union on the case of *LQDN, FDN and others v. France*, concerning the retention of personal data under French law.

9. PI also brought a case in the IPT challenging the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets (BPDs) and bulk communications datasets (BCDs) by the UK Security and Intelligence Agencies. The case was referred to the CJEU, which in its judgment of 6 October 2020 ruled that the relevant UK legislation was incompatible with the privacy safeguards required by EU law.[2]

[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] *Privacy International v United Kingdom*, C-623/17.

10. In a 2018 report[3], 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[4] 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,[5] and wrote to the European Commission calling for stricter safeguards and oversight of aid funds.[6]

13. In February 2021, PI published a report on the UK's migration surveillance regime[7]. 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 ("MPE") which can be used to access someone's GPS location history, and the move towards satellite

---

[3] 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.

[4] 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.

[5] 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.

[6] 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 .

[7] 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.

tracking more generally (p32; p.36)) by HM Government to police the UK's borders.

14. PI gave written evidence[8] to the Justice and Home Affairs Committee whose report '*Technology rules? The advent of new technologies in the justice system*'[9] makes reference to PI's submissions.

15. PI regularly publishes various analyses of threats to the privacy of migrant communities[10] and primers on technologies used for migration surveillance including one published on 21 July 2021 on satellite and aerial surveillance[11]. Of direct relevance to this claim is a primer we published on 9 February 2022 on electronic monitoring using GPS tags.[12]

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 tags.[13] We have made oral and written submissions[14] to the Independent Chief Inspector of Borders and Immigration in relation the Inspector's investigation into the Home Office use of satellite tracking.

---

[8] https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/publications/written-evidence/.
[9] (30 March 2022), https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/.
[10] PI, '10 threats to migrants and refugees' (8 July 2020), https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees.
[11] 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.
[12] PI, 'Electronic monitoring using GPS tags: a tech primer' (9 February 2022), https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer.
[13] PI, Letter to Gary Pugh (20 January 2022), https://privacyinternational.org/sites/default/files/2022-01/Letter%20to%20UK%20Forensic%20Science%20Regulator.pdf.
[14] 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.

17. On 17 August 2022, PI filed complaints regarding the Home Office's GPS tagging scheme with the Information Commissioner ("ICO")[15] and Forensic Science Regulator ("FSR").[16] I produce these complaints at **Exhibits LA/1 and LA/2** respectively.

18. 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 MPE. PI provided a detailed witness statement concerning the use of MPE, explaining the technical functioning of MPE technology and resulting privacy concerns. The SSHD 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.

19. It is hoped that PI's expertise will be of assistance in this claim to provide a factual account of this form of surveillance.

C. THE TECHNOLOGY – GPS TAGS FUNCTIONING AND DATA COLLECTION

[15] PI, 'SUBMISSION TO THE INFORMATION COMMISSIONER - REQUEST FOR ASSESSMENT OF PROCESSING OPERATIONS BY THE SECRETARY OF STATE FOR THE HOME DEPARTMENT' (17 August 2022), https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20complaint%20against%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags%20%5Bpublic%20version%5D.pdf.

[16] PI, Letter to Gary Pugh (17 August 2022), https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20Complaint%20to%20FSR%20re%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags.pdf.

20. Prior to January 2021, the Home Office used Radio Frequency tags for electronic monitoring. In January 2021 the Home Office published version 7 of their Immigration Bail policy, which introduced the use of GPS tags.

21. In this section, I will explain the material differences in the way these technologies work. I will first look at how Radio Frequency ('RF') tags work, being the traditional technology used for tagging individuals. I then look at GPS tags (noting that these devices can also include RF technology) and then smart watches. However, I note that I have not had sight of the make and model of the GPS tags used by the Home Office, their technical specifications nor their instruction/technical manuals. This information would be useful in understanding the full capabilities of the tags. My evidence in this statement is based primarily on my review of the latest Immigration bail guidance (Version 13.0) published by the Home Office on 30 August 2022 (the "Bail Guidance")[17], the Immigration bail conditions: Electronic monitoring (EM) expansion pilot guidance (Version 1.0) published by the Home Office on 15 June 2022 (the "Pilot Guidance")[18], 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").

22. The Home Office Bail guidance states that the GPS devices they use have a dual capability to use GPS and radio frequency technology. A curfew is not mandatory as a result of using a GPS device to electronically monitor a person, because location monitoring is 24/7. The Home Office has also stated 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 is installed.*"

[17]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1114687/Immigration_bail_September_2022.pdf
[18]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082956/Immigration_bail_conditions_-_Electronic_Monitoring__EM__Expansion_pilot.pdf

23. The Bail Guidance refers to the issuing of mobile phones and states 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." However, no other information is provided. This is not covered in the Expansion pilot DPIA nor in the 2021 DPIA.

How Radio Frequency tags work

24. The evidence I provide in this section and the next is based on the knowledge I acquired from PI's team of technologists on electronic monitoring technology, as outlined in PI publications.[19] 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. 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.

25. RF tags communicate with the base station (monitoring unit) over a specific radio frequency to detect if it is within range. *"The home monitoring unit sends information to the EMS Monitoring Centre using the mobile phone network,"* according to the Electronic Monitoring Equipment Operational Procedure.

26. As noted in the Consultation on the Future Direction of the Electronic Monitoring Service[20] by the Scottish Government, the data RF tags send to the

[19] In particular PI, 'GPS tracking and COVID-19: A tech primer' (7 May 2020), https://privacyinternational.org/explainer/3753/gps-tracking-and-covid-19-tech-primer; 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; and PI, 'Electronic monitoring using GPS tags: a tech primer' (9 February 2022), https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer.

[20] 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.

monitoring unit provides information about a person's movements within an agreed location. The locational information is essentially binary though: 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, 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.

27. The home monitoring unit 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 remain at home from 7pm to 7am.

28. The Home Office state that they may make operational decisions to use a RF device rather than GPS where "[i]f a curfew condition is required, or to extend the life of the GPS device battery, or where limited GPS signal is available". This will require the installation of a Home Monitoring Unit.

How GPS Tags work

29. 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 tag was minute-by-minute of every day. This information can be accessed directly by control-centre personnel and can be monitored by software.

30. As stated by the Home Office in letters to tagged individuals, "*GPS devices monitor your movements in any location unlike Radio Frequency devices which monitor your movements as you move in and out of range of your home monitoring unit.*"

31. 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 (either GPRS or 4G). The tag also contains a SIM card (or equivalent) to authenticate it to the network.

32. 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 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."

33. 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. 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.

34. The mobile network can also be used to identify location. It will do this by triangulating data using GSM cell-based data. This means that it will work out location using the mobile phone masts which the SIM card communicated with at a certain time.

35. As noted by the Forensic Science Regulator[21], cell site analysis relies on the acquisition of communications data, the processing of this data and the presentation of this data in the form of maps and tables.

36. 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. In 2014, the Ministry of Justice awarded a contract to Telefonica[22] in relation to "network services" (Global System for Mobile Communications) for electronic monitoring. 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, i.e. location is worked out using the mobile phone masts which the SIM card communicated with at a certain time. As noted by the Forensic Science Regulator,[23] 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.

37. Tags can collect GPS location data at different frequency of intervals. For example, the buddi ST3 Smart Tag 4 manual indicates that "*Intervals can be defined, or a real-time request made*".[24] Another device allows setting intervals at 15 minutes, 30 minutes or an hour.[25] Which intervals are selected naturally has a

[21] 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.
[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] 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.
[24] 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.
[25] Manualslib, Link-2 User manual, https://www.manualslib.com/manual/587617/Lowrance-Link-2.html?page=54.

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.

38. According to one company which sells GPS tracking devices to industry, some devices do not use intervals at all and instead use on-demand tracking[26]. This means that they only turn on in response to a specific location request.

39. It is possible for GPS tags to create inclusion and exclusion zones. As noted by Buddi who have a pilot project with The Mayor's Office for Police and Crime, London ("MOPAC"), their tag features inclusion zones (areas on a map to indicate where the device should be located during set times of the day) and exclusion zones (zones that trigger alerts when the device enters the specified zone).[27] The HM Prison & Probation Service leaflet on GPS tags states that a notification will be sent to the monitoring unit if an individual enters an exclusion zone.[28]

40. The GPS tag itself is usually attached to the ankle, using a reinforced band. It has been described in the Scottish Government consultation report as larger and heavier than radio-frequency tags. 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. 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:

[26] https://www.brickhousesecurity.com/gps-trackers/tracking-intervals
[27] Buddi, 'Security', https://buddi.uk/security.
[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/823842/Location_monitoring_-_Victims_Leaflet_Print.pdf

"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..."

41. Per the Ministry of Justice tagging handbook, tag wearers must not do contact sports such as football, hockey or rugby, water sports, or fly without the approval of their responsible officer. [29]

Trail Data

42. 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 every day. 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 enables live tracking of an individual, i.e. the following of their movements on a regular basis. The Expansion Pilot DPIA states that trail data is stored for six years after the tag is removed, and that daily biometric facial image checks (i.e. the images submitted by the individuals when requested to do so) will be retained for 2 years after each production check, and the original "Enrolment Image" (the one against which each check is performed) will be stored for 6 years.

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

[29] Ministry of Justice, 'Electronic Monitoring GPS Satellite Tagging handbook', https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/non-secure/e/l/e/electronic-monitoring-global-positioning-system-annex-n-gps-handbook.pdf.

44. **First**, the volume of data collected through live location tracking is enormous. The Home Office does not disclose in either its Bail Guidance or DPIAs what intervals have been set for location data collection, however I understand from the solicitors representing the Claimants in this claim that 1-minute intervals were set in one of their cases. This means that the tags are set to "ping" the network every minute to record the individual's location at that time, so that the resulting trail data is a record of where the individual has been every minute of the day, 24/7.

45. PI's team of technologists performed technical research into some GPS ankle tags available on the market, wearing them for some periods of time and analysing the resulting data collected. They tested them with different location data collection intervals, rendered the data in Excel spreadsheets (which showed a list of location coordinates along with the hour, minute and second at which it was recorded), 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).
    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).

46. Plotting location data points on a map is also a common feature available to GPS tagging software, accessible through an online platform provided by the tag supplier. Our technologists observed that doing so by filtering by just a 2-day period could produce an unreadable map crowded with location points (in particular when they set 1-minute or 30-second location data collection intervals).

47. Although GPS technology allows for technical measures to limit the amount of data collected to what is necessary to make the tagging effective, this does not appear to be a feature of the tags procured by the Ministry of Justice, either in the immigration or criminal justice context. Indeed, none of the policies or impact assessments I have seen indicate that the tags can be or are set to collect location data only for what is necessary to monitor bail compliance and/or minimise the risk of offending – for example, to collect data only at certain times of the day, when in certain locations, or on demand if there is suspicion of offending or absconding. This is confirmed by the fact that the tags used to monitor the Claimants collect data every minute, 24/7 – as was indicated to me by their solicitors according to the trail data they have obtained. This was also confirmed by the Ministry of Justice's response to a Freedom of Information Request submitted by the Claimants' legal representatives. I produce the response at **Exhibit LA/3**:

1. *Whether or not the GPS tracking devices are capable of being programmed to send a signal at a specific time/ for a specific time period?*
   Outside the scope of the FOIA and on a discretionary basis as above, the GPS Tags cannot be programmed to send out specific signals at specific times / periods. They operate in real-time and monitor continuously.

48. **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. The Home Office's own Expansion Pilot DPIA acknowledges that the nature of the data is sensitive (p.5). When and how a person moves around can therefore reveal a considerable amount of information about their life and personality. By way of example, 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.

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 can also provide 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. **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. 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, etc. However by showing this to different PI staff members, we saw that different people were drawing widely divergent interpretations of the individual's activities.

D. RELIABILITY CONCERNS

Accuracy and reliability of GPS tags data

51. GPS location is accurate to about 5 meters in good conditions.[30] 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).[31] All these factors affecting accuracy of GPS location data can give rise to errors of 100 meters or more.[32] 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.[33]

52. In circumstances where GPS location is used to monitor compliance with bail conditions, inaccuracies, even small, could have profound consequences for

[30] GPS.gov, 'GPS Accuracy', https://www.gps.gov/systems/gps/performance/accuracy/.
[31] 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.
[32] PI, 'GPS tracking and COVID-19: A tech primer' (7 May 2020), https://privacyinternational.org/explainer/3753/gps-tracking-and-covid-19-tech-primer.
[33] 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.

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.

53. 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. Similarly, one of our technologists observed that when shopping at his local grocery store, his GPS tag was unreachable due to there being no mobile phone network coverage in the store, and therefore a notification was sent to the monitoring device (his phone in this case) when he was in the store for more than 15 minutes. In circumstances where loss of contact can trigger a breach alert and be considered absconding (as provided by the list of processing purposes in the Expansion Pilot DPIA), thereby triggering a full review of trail data to locate the individual, this can lead to wrongful accusations of breach and inaccurate records.

Battery life

54. EMS state in the "tagging handbook" published on the government's website[34] that GPS tagging devices need to be charged for an hour a day. A handbook on GPS tagging from the Ministry of Justice, however, suggests that a fully charged tag usually takes "at least 2 hours every day",[35] as does the latest version of the EMS Monitoring handbook I have seen a copy of. According to the Ministry of

[34] EMS, 'Tagging – Everything you need to know about being tagged', https://www.gov.uk/government/publications/gps-location-monitoring.
[35] Ministry of Justice, 'Electronic Monitoring GPS Satellite Tagging handbook', https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/non-secure/e/l/e/electronic-monitoring-global-positioning-system-annex-n-gps-handbook.pdf.

Justice's tagging handbook, when the battery runs low, the tag will vibrate and the power light will flash red on the tag until it is charged.

55. I understand from my work with migrant rights organisations and law firms representing tagged individuals 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. If the battery begins to fail, it will be necessary to charge devices for much longer periods of time and more regularly with, of course, the tag attached to the individual's leg (including at night), thereby limiting their freedom of movement considerably beyond what is intended through the imposition of the electronic monitoring condition. The Independent Chief Inspector of Borders and Immigration 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.*"[36]

56. 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. Any failure to charge the device is treated as a breach of bail conditions, meaning that if the battery is depleted, all data (including trail data) can be shared with the Home Office, and this can result in civil and criminal penalties relating to the breach. An apparent breach may lead to arrest, bail conditions being varied, the requirement to pay

[36] 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.

money under financial conditions, any unresolved application for leave to enter being refused, or detention.

57. I am aware that the individual can be given a portable charger which they can bring with them to charge a device if they are out and about. I have not been able to identify from publicly available documents how much charge a portable charger can give a properly functioning device.

58. If the device is faulty and will not charge properly when connected to the mains, then a portable charger will face the same problems with being unable to effectively charge the device and making the device hold a charge. If a tag will not charge properly when connected to the mains, then it will not charge properly when connected to a portable charger. Thus, a portable charger is not an answer to a faulty device. Walking around with the tag plugged to the portable charger may also be burdensome, thus not solving the restriction on individuals' movements.

59. Battery life in GPS tags is a recognised problem. This has been noted in the recent reports of the HM Inspectorate of Probation[37] and the Ministry of Justice[38], which noted that "*Forty-three per cent of violations were due to tracker shutdowns resulting from loss of the tag's battery power due to insufficient charging – potentially representing the 'burden' of wearers having to charge the battery daily.*"

60. It appears that in some cases, battery depletion may not result from the individual not charging properly, but rather because of frequent location data collection (it appears in this case every 1 minute, which is on the higher end of

[37] 'The use of electronic monitoring as a tool for the Probation Service in reducing reoffending and managing risk (January 2022), https://www.justiceinspectorates.gov.uk/hmiprobation/wp-content/uploads/sites/5/2022/01/Electronic-monitoring-thematic-inspection.pdf.
[38] 'Process evaluation of the Global Positioning System (GPS) Electronic Monitoring Pilot: Quantitative findings' (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814219/process-evaluation-gps.pdf

possible intervals in common GPS tags, which range between 30 seconds to 1 hour, to on-demand location requests), which in turn drains the battery more quickly. The Reform report "Cutting crime: the role of tagging in offender management"[39] noted this very problem:

> *"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"*

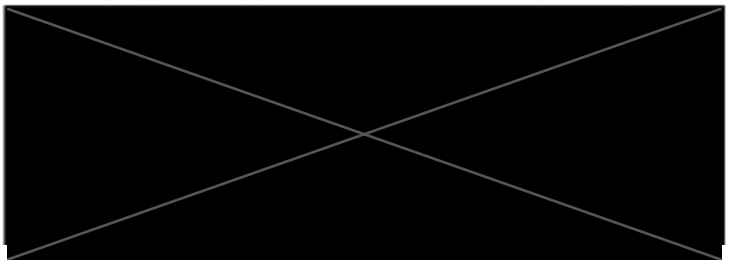
61. Inaccuracies in the recording of breaches of bail conditions, including treating faults in the device as a breach or non-compliance, impact upon broader immigration enforcement and bail compliance reviews. An individual is unlikely to be able to easily make necessarily technical submissions about the quality, longevity and reliability of the battery and charging equipment. Persons on immigration bail can only provide their explanation as to why they have not committed a breach, but are not in a position to make representations on the design of location data collection by the Home office or the quality of the device as causing malfunctions and misreporting of breaches.

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.

[39] Reform, 'Cutting crime: the role of tagging in offender management' (9 September 2015), https://reform.uk/publications/cutting-crime-role-tagging-offender-management/.

Signed by:



Name: Lucie Audibert

Date: 10 November 2022