23 May 2022

Privacy International's submissions for the Independent Chief Inspector of Borders and Immigration Inspection of the Satellite Tracking Service Programme

Table of Contents

Introduction **2**

Background to the introduction of GPS tags **5**

The Technology **7**

Radio Frequency **7**

GPS **7**

Smart Watches **9**

Trail Data **12**

The intrusive nature of trail monitoring and lack of safeguards **13**

Reliability concerns and lack of safeguards **17**

The limitations of electronic monitoring: accuracy and battery life **18**

Accuracy 18

Battery Life 20

Concerns about purposes of trail data processing **24**

Contracting / Third parties **28**

Data analytics and anonymisation **29**

Annex A: Questions **31**

Annex B: The legislation **34**

Introduction

1. Privacy International welcomes the opportunity to provide input to the Independent Chief Inspector of Borders and Immigration (ICIBI) on the Satellite Tracking Service Programme[1] of the Home Office.

2. We highlight key concerns in relation to the Home Office's use and expansion of electronic monitoring using satellite tracking via GPS tags[2] or Non-Fitted Devices,[3] as informed by the Home Office's Immigration Bail policy,[4] and Data Protection Impact Assessments ("DPIAs") obtained through FOIA requests.[5]

3. The seismic change resulting from the introduction of GPS devices cannot be overstated. This enables 24/7 monitoring of an individual's location, as well as live tracking, meaning that you could follow an individual's movements in real time. The data is stored for six years after the tag is removed. All trail data is shared with the Home Office when there is a breach alert on the Electronic Monitoring System (EMS), allowing them to review this material for matters unconnected to the alert in question. This goes beyond the mere monitoring of bail breaches through Electronic Monitoring as provided for in statute.

4. We are concerned there is a systemic failure relating to quality of the tags in terms of battery life which places a far more onerous requirement on individuals to charge for long periods of time with the tag attached to their leg. EMS states in their YouTube video hosted on the HM Prison and Probation Service channel that devices need to be charged for an hour a day[6]. 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"[7].

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1005340/ICIBI_Inspection_Plan_2021-22.pdf

[2] The Home Office Immigration Bail policy states that it uses Global Positioning System ('GPS') devices to electronically monitor individuals. GPS is a system of around 30 satellites that enable location tracking of individuals.

[3] The Data Protection Impact Assessment dated 2021 refers to a smartwatch that an individual shall be expected to carry with them at all times.

[4] Home Office, Immigration Bail policy Version 11, published 31 January 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051204/immigration_bail.pdf.

[5] Two DPIAs were conducted by the Home Office on the transition to use of GPS Tags, one in August 2020 and one in August 2021. We refer to each respectively as the "2020 DPIA" and the "2021 DPIA".

[6] https://www.youtube.com/watch?v=yAsUEcB0yUg dated 5/03/2019

[7] 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 - 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/process-evaluation-gps.pdf).

5. Battery life is an issue which has been noted in the recent reports of the HM Inspectorate of Probation[8] and the Ministry of Justice[9] in relation to GPS tags.

6. Failure to charge is a breach of bail conditions[10], meaning all data can be shared with the Home Office and result in civil and criminal penalties.

7. Further a list of battery breaches leads to assumptions of non-compliance when the reality could be that the problem lies with the quality of the device. Thus, errors and inaccuracies in the recording of breaches of bail conditions, including battery issues, impact upon broader immigration enforcement and bail compliance reviews. This raises concerns about how complicated and difficult it may be for an individual to correct errors in breach notifications that are recorded on their immigration file.

8. Thus, technical implications of the quality of the tags and whether their charging efficiency depreciates, has significant impact on the individual.

9. This intersects with concerns we have been alerted to which related to the poor administration of the electronic monitoring system, confusing and contradictory statements regarding obligations and bail conditions. The HM Inspectorate of Prisons Report details several issues with the service provided by EMS.[11] Practitioners and those supporting individuals are best placed to elaborate on these issues and we encourage the ICIBI to speak to a broad range of individuals.

10. The use of GPS tracking goes beyond the aim of monitoring bail breaches or preventing individuals from absconding. The Home Office plans to use trail data, being the location data collected by the tag and stored by the third-party commercial provider:[12]

    - To consider prosecutions for breach of bail conditions.
    - In decisions on further submissions and Article 8 ECHR claims.
    - To share with law enforcement agencies.

---

[8] https://www.justiceinspectorates.gov.uk/hmiprobation/wp-content/uploads/sites/5/2022/01/Electronic-monitoring-thematic-inspection.pdf

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814219/process-evaluation-gps.pdf

[10] Immigration Bail policy (n 4), "maintaining their EM device and any mobile phone issued to them as outlined in the induction leaflets issued by the supplier to include charging the device daily until fully charged"

[11] https://www.justiceinspectorates.gov.uk/hmiprobation/wp-content/uploads/sites/5/2022/01/Electronic-monitoring-thematic-inspection.pdf
"Current service level agreements with EMS include timeliness for answering of calls, but not the time taken to speak to an individual once the call has been answered electronically. The length of time it took for EMS to answer telephone calls was raised in practitioner focus groups, with some officers reporting waits of up to 45 minutes to get a response. This was echoed by people on probation who also told us they had struggled to get in touch with EMS when required. Although meeting the contracted requirements, the actual experience of waiting to speak to staff fails to meet the needs of busy practitioners and those on probation who are often trying to contact EMS to report issues. As one practitioner indicated: "They always pick up the phone, but they don't follow through and often don't know when things like issuing a new charger is going to happen. When people's liberty is at stake they should be doing better."

[12] Immigration Bail policy (n 4), p.28.

- For data analytics purpose including behaviour mapping and informing immigration policy.

11. The impact on individuals who are subject to this surveillance is little understood or examined. There has been no equality impact assessment. Unlike the use by probation in the criminal justice system where GPS tags are used to work with an individual who is on probation, in the immigration context it is a punitive method of surveillance. We understand that the exemptions to mandatory electronic monitoring are being applied in a highly restrictive manner by the Home Office and the inability to challenge the Home Office imposition of tagging before a judge of the First-tier Tribunal has ousted a fundamental safeguard against unnecessary and disproportionate use.

12. This type of constant surveillance has been reported by the Ministry of Justice to negatively impact tag wearers leading to feelings of increased anxiety[13]. In addition, individuals might not want to spend time with a friend[14] who is wearing a GPS tag. It therefore risks having a strong chilling effect on the exercise of fundamental rights and freedoms. This is in the context of an absence of time limit for tags or safeguards for those wearing tags to ensure they are applied in a manner which is necessary and proportionate.

13. In addition to their intrusive nature, the device limits the way an individual can live their life, not just with the burden of regularly charging the device, but the tag prohibits contact sports such as football, hockey or rugby[15].

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

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

15 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

Background to the introduction of GPS tags

14. From January 2021, those who were subject to EM but on Radio Frequency tagging were moved over to monitoring by GPS[16].

15. From 31 August 2021, by virtue of immigration regulations[17], the provisions in Schedule 10 the Immigration Act 2016, providing for foreign national offenders[18] liable to deportation to be subject to mandatory electronic monitoring as a condition of immigration bail, were commenced.

16. In this context, a foreign national offender is any foreign national who has received a 12-month custodial sentence; or is deemed to be a persistent offender. Power for deportation derives from the UK Borders Act 2007 and applies to non-European Economic Area citizens and EEA citizens. EEA citizens are all EU citizens and those who are citizens of Lichtenstein, Iceland, Norway and Switzerland.

17. This was designed to implement the 2015 Conservative party manifesto commitment to *"introduce satellite tracking for every foreign national offender subject to an outstanding deportation order or deportation proceedings."*[19] The provisions were debated in 2016 during the passage of the Immigration Act 2016[20] and have been debated recently in light of proposed amendments to the Nationality and Borders Bill in November 2021,[21] specifically in relation to the absence of strict limits and safeguards on how long electronic monitoring is used and in what circumstances. These amendments did not pass.

18. Since 31 January 2022 all those already on immigration bail and subject to either deportation proceedings or a Deportation Order, are now subject to a review of individual circumstance and GPS tags are now starting to be issued to those individuals. In addition, the Secretary of State for the Home Department (SSHD) i.e., Home Office, can impose electronic monitoring on those not subject to a deportation order if justified by the circumstances of the case.[22]

---

[16] https://www.biduk.org/articles/805-bid-s-briefing-on-electronic-monitoring
[17] Immigration Act 2016 (commencement and transitional provisions No 1) (England and Wales) Regulations 2021, SI 2021/939 (see paragraphs 2(2) and 2(3)(a) of Schedule 10),
[18] all those in England and Wales subject to either deportation proceedings or a Deportation Order at the point of release from prison or Immigration Removal Centre
[19] https://ucrel.lancs.ac.uk/wmatrix/ukmanifestos2015/localpdf/Conservatives.pdf.
[20] https://hansard.parliament.uk/Lords/2016-03-15/debates/73C9801F-AE95-4E8C-A536-BAE51FFABDDC/ImmigrationBill?highlight=electronic%20monitoring%20immigration#contribution-3EE5F5F7-0688-41F9-9A84-9437DE772086
[21] https://hansard.parliament.uk/Commons/2021-11-04/debates/4d819fad-a167-4619-b084-6ef35bc49ac7/NationalityAndBordersBill(SixteenthSitting)?highlight=electronic%20monitoring%20immigration#contribution-72252173-13DE-46E6-8015-84E474D5C96D
[22] Immigration Bail policy (n 4), p.20.

19. Electronic monitoring must always be considered for those subject to deportation orders. For those who are not subject to deportation orders, electronic monitoring can be imposed by the Secretary of State as a condition of bail, for example where the person presents a high risk of absconding from immigration bail or pose a significant risk of harm to the public or to public health.

20. A bail condition requiring a person to wear a GPS tag can be combined with restrictions on their movements, including curfews and conditions on where they can go (called inclusion or exclusion zones).

21. Given the myriad ways the SSHD seek to use the data, as noted by Stuart C McDonald SNP in November 2021 "the use of tracking goes way beyond the original intention … which was to prevent people from absconding."[23] He noted that the Government's own data suggests that absconding rates are exceptionally low and that a recent FOIA response found that of people granted bail between February 2020 and March 2021 (of which there were more than 7,000), just 43 people absconded – less than 0.56%. Other data suggests that 1% of people released from detention in 2020 absconded[24].

22. The Home Office Data Protection Impact Assessment states that the number of tag wearers will rise significantly from 280 to approximately 4500[25]. Bail for Immigration Detainees (BID) estimates:

> "At 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."[26]

23. There are now more recent figures which show that 11,236 people are facing deportation living in the community[27].

24. A recent Freedom of Information Act request states that currently 1,412 people are being electronically monitored as of 29 March 2022.

[23] https://hansard.parliament.uk/Commons/2021-11-04/debates/4d819fad-a167-4619-b084-6ef35bc49ac7/NationalityAndBordersBill(SixteenthSitting)?highlight=electronic%20monitoring%20immigration#contribution-72252173-13DE-46E6-8015-84E474D5C96D.
[24] FOI data obtained by Brian Dickoff, Response provided Monday 18 January 2021, available here: https://www.whatdotheyknow.com/request/712000/response/1706999/attach/3/61618%20Dikoff.pdf?cookie_passthrough=1
[25] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf
[26] https://www.biduk.org/articles/805-bid-s-briefing-on-electronic-monitoring
[27] https://www.gov.uk/government/publications/immigration-enforcement-data-q4-2021

The Technology

25. The Home Office previously used Radio Frequency tags for electronic monitoring. They have rolled out the use of GPS tags and have proposed the use of smart watches. The Home Office states that the GPS devices they use have dual capability to use GPS and radio frequency technology[28].

Radio Frequency

26. 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. They are typically used to enforce curfew conditions, such as that an individual remain at home from 7pm to 7am.

27. The tag communicates with the base station (monitoring unit) over a specific radio frequency to detect if it is within range.

28. As noted in the Consultation on the Future Direction of the Electronic Monitoring Service[29] 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.

29. The locational information is essentially binary though: in other words, in terms of "location" 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. So, the two pieces of equipment 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.

30. If the tag fails to report (or the signal is below a threshold) then it will raise an alert, and a specified 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.

GPS

31. Whereas radio-frequency tags tell the tagging authority whether the tag wearer is observing a curfew, i.e., that the tag is within the vicinity of the

---

28 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051204/immigration_bail.pdf

29 https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf

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.

32. As explained in the Scottish Government consultation document, 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.

33. GPS tags enable geolocation by receiving signals from at least 4 different satellites and doing some maths to pinpoint location. A GPS navigation chip will calculate and store location data and a SIM card connects the tag to the mobile network[30].

34. The mobile phone network is what is used to communicate the location information to a central computer at a monitoring centre in "real time". The central control then may use a mapping service to plot locations and times.

35. Anyone who has used a GPS-based smartphone app such as Google Maps will have seen something very similar to how GPS tags work; the app will record your location on the Earth's surface.

36. As stated the tag has a SIM card to communicate location data to the EMS. 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.

37. As noted by the Forensic Science Regulator[31], 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.

38. Tags can collect GPS location data at different frequency of intervals. For example, the buddi ST3 Smart Tag 4 indicates the ability to set intervals[32] at either 15 minutes, 30 minutes or an hour[33]. Its specification states: *"GPS Location (Intervals can be defined or a real-time request made)"*.[34] If you collect it at a lower frequency, you collect less location data. The 'Attenti One Piece Tracking Device' states in its manual that in Active Mode, *"The standard 1 Piece call-in interval is once every hour while in compliance"*, while in Passive Mode, *"the standard 1 Piece call-in interval is once every six hours."*

---

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

31 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/918946/135_FSR-C-135_Cell_Site_Analysis_Issue_2.pdf

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

33 https://www.manualslib.com/manual/587617/Lowrance-Link-2.html?page=54

34 https://www.manualslib.com/manual/587617/Lowrance-Link-2.html?page=54

39. 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[35]. This means that they only turn on in response to a specific location request.

40. 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 which are areas on a map to indicate where the device should be located during set times of the day and exclusion zones which are set up customisable zones to trigger alerts when the device enters the specified zone.[36] 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[37].

41. The GPS tag itself is usually attached to the ankle, using a reinforced band. The physical tag consists of the tag attached to the individual. 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. The physical implications of this are that contact sports such as football, hockey or rugby[38] are not allowed according to guidance documents.

Smart Watches

42. The Home Office have not commenced use of smartwatches, but indicated an intention to use them in the 2021 DPIA. The smartwatch will most likely rely on GPS technology to track the location of the wearer, similar to how the GPS tags operate. However, the smartwatches introduce the additional element of biometrics.

43. The Home Office's 2021 DPIA states that:

> "The new Smartwatch device that we will be using for monitoring purposes via inclusion exclusion zones and collection of Biometric Facial Image checks is new technology and is currently still undergoing checks. It will be supported by MOJ and HO DDAT. The Smartwatch devices will not be available until November 2021 and any emerging risk will be included and assessed within this DPIA."

44. Biometric Facial Image checks will be used to ensure that the individual subject to bail monitoring is the individual who is wearing the watch, i.e., to check that they have not taken it off or someone else is wearing it. This

[35] https://www.brickhousesecurity.com/gps-trackers/tracking-intervals
[36] https://buddi.uk/security
[37] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/823842/Location_monitoring_-_Victims_Leaflet_Print.pdf
[38] 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

is the alternative to having a tag fitted to the ankle with a tamper resistant tag that cannot be removed.

45. On 3 May 2021 the Ministry of Justice awarded a contract to Ingenium Biometric Laboratories Limited for 'Assurance testing for the use of biometric-enabled wearable/non-fitted devices as an alternative to electronic tags.' [39] The requirement is for 'biometrics assurances services; test and evaluation of biometric products; biometric assurance plan and strategy'. The services include:

> "Evaluation of biometric functionality of a smartwatch including both performance evaluation (false match rate, false non-match rate/FMR and FNMR) and presentation attack detection (PAD) performance (imposter attack presentation match rate/IAPMR). The specific use case and the likely threats to the system make PAD of particular importance to the evaluation of the system."
>
> "…the solution will need to operate consistently across the user base and not show any bias against any of the demographics comprising the population, in terms of age, gender or ethnicity."

46. The contract highlights some of the risks associated with biometrics devices, being false matches and bias in age, gender or ethnicity.

47. According to the Home Office's DPIA, the intention is that for those individuals who are given a non-fitted device – smartwatch – to carry or wear, they will have to complete random monitoring checks throughout the day by virtue of taking photograph of themselves using the smartwatch which will be cross checked against a system held Biometric Facial image template.

48. Biometric images being held on the supplier's database raise concerns, particularly in the present context where there are inadequate safeguards against the misuse and abuse of GPS location data, and where there is little detail on the system that the Home Office intends to use or is procuring in order to implement the use of smart watches. There is risk associated with opaque systems including how they actually work and why and how they can fail.

49. Biometrics is the "measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals."[40] There are two parts to the use of any biometric system. Firstly, biometric technologies capture and store characteristics in a database to identify an individual. Secondly, the information in this database is cross-referenced to verify or authenticate an individual's identity – image

[39] https://www.contractsfinder.service.gov.uk/notice/9652eb0c-f000-4a7d-b0c1-261faae5e92c?origin=SearchResults&p=1
[40] "Privacy International (2013) Biometrics: Friend or Foe of Privacy?" https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf: page 5

verification via monitoring checks.

50. The Home Office's proposed use involves a 1-1 match of the individual against the stored template to answer the question, "is this x?". Biometrics can also be used to identify an individual – this is a 1-to-many match, to answer the question "Who is this?".[41]

51. The use of biometrics presents a unique set of concerns. In 2018, the United Nations High Commissioner for Human Rights issued a Report on the right to privacy in the digital age[42], which highlights significant human rights concerns with the creation of mass databases of biometric data:

> "Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused.
>
> For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-base projects without having adequate legal and procedural safeguards in place."[43]

52. When adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance.

53. The varying accuracy and failure rates of the technology can lead to misidentification. As the UK's National Cyber Security Centre puts it,

> "However, no two captures of biometric data will produce truly 'identical' results. So, a biometric system must make an estimation as to whether two biometric samples come from the same individual."[44]

54. Thus, a biometric system is not making a definitive decision on whether an individual is who he or she claims to be, but rather a probabilistic one. This means that some are going to be excluded from what they are entitled to,

---

[41] Privacy International (2013) Biometrics: Friend or Foe of Privacy? https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf
[42] "United Nations High Commissioner for Human Rights (2018) The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29"
[43] United Nations High Commissioner for Human Rights (2018) The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29
[44] National Cyber Security Centre, Biometric Recognition and Authentication Systems. Available from: https://www.ncsc.gov.uk/collection/biometrics?curPage=/collection/biometrics

or falsely accepted as somebody they are not, as a result. In the present context, the reliance on biometric identification for regular check-ins may lead to false breach alerts – for example if the technology misidentifies the individual. As explained, this is an issue of particular concern for individuals of colour, women, or individuals who do not "fit" the majority of traditional human representations (e.g. individuals with disabilities).

55. Moreover, biometric data can identify a person for their entire lifetime. Unlike a password, an individual's biometrics cannot be changed. This makes the creation of a biometric database problematic, as they have to anticipate risks far into the future – whether that be a future data breach or the development of technology meaning that biometrics can be used for more purposes and could reveal more information and intelligence about individuals than is currently possible.

56. The use of a centralised database for biometrics compounds concerns. In considering the fundamental rights implications of storing biometric data in identity documents and residents cards, the European Union Agency for Fundamental Rights ("FRA") found:

> "The establishment of a central national database would also increase the risk of abuse for using the data for other purposes than those originally intended. Due to its scale and the sensitive nature of the data which would be stored, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights."[45]

Trail Data

57. Trail data refers to the complete location history of the person who is wearing the tag (or a smart watch), i.e. a log of where the person has been minute-by-minute every day.

58. GPS monitoring provides deep insight into and reveals intimate details of an individual's life. It is highly intrusive, reveals sensitive information, and the longer the tag is in place, the greater the volume of location data collected and thus the ability to have insight into an individual's patterns of behaviour.

59. The data collected may also include the time and length of time that devices are charged, revealing patterns of behaviour.

[45] European Union Agency for Fundamental Rights (2018) Fundamental rights implications of storing biometric data in identity documents and residence cards: page 14. Available from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf

60. 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. The tags used by both the criminal justice and immigration context do not appear to have the ability to limit the amount of data collected so that the data gathered and retained is only what is necessary to monitor bail compliance and/or minimise the risk of offending.

The intrusive nature of trail monitoring and lack of safeguards

61. The use of GPS tags is a significant change in the surveillance of migrants. The Home Office have not adopted a method of collecting location data by intervals, but instead is doing this 24/7. GPS tags thus enable constant monitoring of an indivduals' location and the colletion and storage of this data for passive review and analysis.

62. GPS location data provides deep insight into and reveals intimate details of an individual's life. It reveals everyday habits, 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. It also reveals sensitive information such as potential medical concerns if they visit a particular medical clinic, religion if they visit a place of worship, political beliefs if they attend a protest, rally or political party headquarters, sexual orientation if they visit certain places or advice centres, and other intimate details of their privacy and family life (if they attend schools or nurseries, playgrounds, other residences, etc).

63. Live location data is part of a category of data described using the term "communications data" or "metadata". The UK Communications Data Code of Practice[46] defines location data as a subset of communications data being "'events data" and requires a higher level of authorisation to access this data than other types of communication data, due to it being more intrusive (see paras 2.34-2.35).

> "2.18 The term 'communications data' includes the 'who', 'when', 'where' and 'how' of a communication…
>
> 2.20 It can include … the location of the device from which the communication was made."

64. Location data is "no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the

[46] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

persons concerned the feeling that their private lives are the subject of constant surveillance."[47]

65. In the US Supreme Court Judgment of United States v Jones, 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 cellular phone to a Government computer. **It relayed more than 2,000 pages of data over the 4-week period.**"[48]

66. The volume and granularity of data is likely to considerably increase when the tag is attached to a person, instead of a vehicle which is only used a few times a day on certain days. The privacy intrusion is therefore multiplied in the present case.

67. The US Supreme Court discussed the intrusive nature of GPS monitoring and how it chills associational and expressive freedoms. For individuals themselves, it's unclear whether they understand the volume of information generated as a result of 24/7 monitoring and that the data can be aggregated, such that the government will be able to ascertain, more or less, their political and religious beliefs, sexual habits, etc.

> "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…("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"). The Government can store such records and efficiently mine them for information years into the future. … And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices…"[49]
>
> "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

[47] Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (C-623/17), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)
[48] https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf
[49] https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf

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." [50]

"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…"**[51]

"I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse …"[52]
(Emphasis added)

68. In the Council of Europe, Recommendation CM/Rec(2014) 4 of the Committee of Ministers to member states on electronic monitoring[53] noted that:

"…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" and that there should be "rules about limits, types and modalities of provision of monitoring technologies … in order to guide the governments of the members Sates in their legislation policies and practice in this area".

"…that 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".

69. The "Basic Principles' laid out in this recommendation included that the duration of electronic tagging should be regulated and that decisions should be taken by the judiciary or allow for judicial review; that use should be proportionate in terms of duration and intrusiveness to the seriousness of the offence alleged or committed; and that "handling and shared availability and use of data collected in relation to the imposition and

[50] https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf
[51] https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf
[52] https://supreme.justia.com/cases/federal/us/565/10-1259/case.pdf
[53] https://pjp-eu.coe.int/documents/41781569/42171329/CMRec+%282014%29+4+on+electronic+monitoring.pdf/c9756d5b-be0e-4c72-b085-745c9199bef4

implementation of electronic monitoring by the relevant agencies shall be specifically regulated by law."

70. 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[54]. The tag will have a SIM card or equivalent to authenticate it to the network. In 2014 the Ministry of Justice awarded a contract to Telefonica[55] in relation to 'network services' (Global System for Mobile Communications) for electronic monitoring. As noted, the device can triangulate location using GSM cell-based data being the mobile phone masts.

71. 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.

72. 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.

73. On 26 November 2018, Privacy International submitted its legal briefing to the Court of Justice of the European Union (CJEU) on the case of LQDN, FDN and others v. France, concerning the retention of personal data under French law[56]. In the case before the CJEU, Privacy International included arguments that EU law must be interpreted as precluding national rules governing the real-time collection of traffic data and the location of specific individuals, without submitting this collection to the prior authorization of a Court or an independent authority. On 15 January 2020 the CJEU Advocate General issued his opinion[57]. On 6 October 2020 the CJEU issued its judgment on joint cases against France and Belgium.

74. In this decision of the Grand Chamber of the CJEU in Joined Cases C-511/18, C-512/18 and C-520/18, the intrusive nature of location data was considered:

> "117. 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**

---

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

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

56 https://privacyinternational.org/legal-action/lqdn-fdn-and-others-v-france

57 https://privacyinternational.org/sites/default/files/2020-09/FDN%20ao%20v%20France%20AG%20Opinion%202020%20EN.pdf

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). […]

187. It must be emphasised that the interference constituted by the real-time collection of data that allows terminal equipment to be located appears particularly serious, since that data provides the competent national authorities with a means of accurately and permanently tracking the movements of users of mobile telephones. To the extent that that data must therefore be considered to be particularly sensitive, **real-time access by the competent authorities to such data must be distinguished from non-real-time access to that data, the first being more intrusive in that it allows for monitoring of those users that is virtually total** (see, by analogy, with regard to Article 8 of the ECHR, ECtHR, 8 February 2018, *Ben Faiza v. France* CE:ECHR:2018:0208JUD003144612, § 74). The seriousness of that interference is further aggravated where the real-time collection also extends to the traffic data of the persons concerned. "[58] (Emphasis added)

Reliability concerns and lack of safeguards

75. The Home Office electronic monitoring scheme appears to involve the general and indiscriminate retention of location data with no provision for judicial or independent oversight at the point it is imposed.

76. By contrast, the HM Prisons & Probation Code[59] states that "It is a decision for the Courts whether to impose an electronic monitoring requirement as

58 https://curia.europa.eu/juris/document/document.jsf;jsessionid=F345ED3904E34B16E35E805F67CFAD09?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=729419

59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf

part of a Court Order and it incumbent upon them to consider any statutory safeguards and issues of fairness and proportionality."

77. The HM Prisons & Probation Code goes on to note that when imposing licence conditions which include electronic monitoring these should be "preventative as opposed to punitative and must be proportionate, reasonable and necessary." The Code of Practice for HM Prisons & Probation involved consultation with the Information Commissioner's Office.

78. Despite the serious interference with the right to privacy resulting from real-time collection of location data, there is no attempt by the Home Office to justify its use on an individual and mandatory basis in relation to serious aims commensurate with the gravity of the interference. The scheme does not provide appropriate safeguards to ensure data handling is limited to what is strictly necessary. A clear example of this is the sharing of all trail data with the Home Office upon any breach of bail conditions, which appears to be far beyond what is strictly necessary and proportionate for the requirements of addressing an alleged breach of bail conditions.

79. In relation to the lack of limits on the scope and volume of the data collected, there is no consideration of the frequency of intervals at which GPS locations are monitored. For example, the buddi ST3 Smart Tag 4 indicates the ability to set intervals[60] at either 15 minutes, 30 minutes or an hour[61]: "GPS Location (Intervals can be defined or a real-time request made)." It does not appear that the Home Office has considered using this functionality.

80. In addition to the intrusive nature of such bulk data collection, there is an inherent risk in relation to abuse and unlawful access[62].

The limitations of electronic monitoring: accuracy and battery life

Accuracy

81. Global Positioning System (GPS) is a space-based global navigation satellite system that provides location and time information in all weather, anywhere on or near the earth. GPS monitoring uses a network of 30 US maintained NAVSTAR satellites to calculate the physical position of the GPS tag. Although other networks of satellites do exist (Glonass, Galileo, Compass) they are not yet ready for use[63].

[60] https://manuals.plus/buddi/st3-smart-tag-4-era-monitoring-system-manual#axzz7PgoPr5dw
[61] https://www.manualslib.com/manual/587617/Lowrance-Link-2.html?page=54
[62] Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (C-623/17), Judgment, Grand Chamber, Court of Justice of the European Union (6 October 2020)

[63] https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf

82. GPS location may be accurate to a few meters in good conditions. A high quality position fix requires an open view of the sky. There can be errors in urban canyons, close to buildings and other locations where only a few satellites are visible.

83. Drift relates to issues concerning the strength of a GPS signal. This can vary depending on the distance to the nearest satellite. When the signal is particularly weak this can cause drift being the movement in the accuracy of the signal which means that an individual may be recorded some distance from their true location[64].

84. The impact of tall buildings relates to the phenomenon often referred to as 'urban canyons' where a GPS signal can be disrupted in built up areas where very tall buildings can block the satellites and cause the signal to bounce. Similarly, much like many smart phones, GPS tags may be less accurate in very rural areas. Whilst the GSM mobile phone network can be used as a back-up when GPS signal is unobtainable, the level of accuracy provided by the substitute system is much lower[65].

85. If the signal from one or more satellites bounces off a tall building, this can give rise to an error of 100m of more. Larger errors can also arise where the view of the sky is restricted so that only a few satellites are visible.

86. The devices can use the mobile network where GPS signal is unobtainable, to triangulate location using GSM cell-based data. i.e., if satellites can't be used to pin-point a location the fall-back system is to triangulate using proximity to the nearest mobile phone mast.[66] As noted by the Scottish Government in their 2013 consultation, it is important to note that although the mobile signal can pick people up in buildings and other locations where sometimes GPS cannot, the accuracy of the triangulation using this method may not be as reliable as with GPS.

87. The accuracy of cell tower data depends on the density of mobile base stations. The density of mobile base stations can vary from a hundred meters in town centres to several kilometers in the open countryside.

88. The UK Forensic Science Regulator in the Codes of Practice and Conduct, Digital Forensics – Cell Site Analysis 2020 notes that a risk analysis in relation to mapping should consider[67]:

    i. "Misrepresentation of a cell site in the wrong location, for example, labelled with an incorrect time of usage and/or cell identification; and

[64] https://reform.uk/sites/default/files/2018-10/Tagging report_AW_8.pdf
[65] https://reform.uk/sites/default/files/2018-10/Tagging%20report_AW_8.pdf
[66] https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf
[67] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/918946/135_FSR-C-135_Cell_Site_Analysis_Issue_2.pdf

ii. Inappropriate sector representation."

89. Some of these difficulties relating to cell site analysis were considered in *R v Calland* [2017] EWCA Crim 2308:

> "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."

90. The Scottish Government consultation in 2013 highlighted a number of problems with GPS tags:

- "GPS usually works in most domestic homes, but may not work inside all buildings;
- GPS usually works whilst travelling in cars, however, may not work on trains;
- GPS drift (movement in accuracy of signal) might occur when static for long periods of time and near waters;
- GPS accuracy is affected by nearby tall buildings and does not work underground."

"There are no absolutes about accuracy or performance of any GPS device. However, we can reliably say what the likely accuracy of any one "fix" is within a particular range. (A fix is where the GPS system locates the tag in a particular place at a particular time). Depending on the strength of signals to the nearest satellites a fix might be accurate to 2-5 meters, 5-10 meters, 10-20 meters etc. "No absolutes about accuracy" does not mean the data can't be used it just means that whoever is using it needs to understand the difference between fixes that are accurate to 2 meters as compared to entries that are accurate to 20 meters. Additional assurance can be gathered from multiple fixes. So, if an offender has generated 20 fixes or data points at regular intervals on a map within 5 minutes, whilst any one point may be subject to drift, nineteen others showing an offender proceeding in a certain direction gives you a great deal more certainty about the result showing his or her movements."[68]

Battery Life

91. EMS state in their YouTube video hosted on the HM Prison and Probation Service channel that GPS tagging devices need to be charged for an hour a day.[69] This is also stated in the "tagging handbook" published on the

[68] https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf
[69] https://www.youtube.com/watch?v=yAsUEcB0yUg dated 5/03/2019

government's website[70]. 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".[71]

92. Battery life in GPS tags is a recognised problem. This has been noted in the recent reports of the HM Inspectorate of Probation[72] and the Ministry of Justice[73].

93. The Ministry of Justice evaluation[74] of GPS tags in 2019 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"

94. The design of the tagging system contributes to the drain on the battery due to the use of live location tracking. The Reform report 'Cutting crime: the role of tagging in offender management' dated September 2015 states 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…"

95. The ICO has commented that:

> "While advances to battery technology have increased in recent years, GPS can be very draining on batteries and battery life depends on the frequency with which the system provides updates on locations (every 10 seconds, every 30 seconds, every minute etc)."[75]

---

[70] https://www.gov.uk/government/publications/gps-location-monitoring

[71] 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 - 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/process-evaluation-gps.pdf).

[72] https://www.justiceinspectorates.gov.uk/hmiprobation/wp-content/uploads/sites/5/2022/01/Electronic-monitoring-thematic-inspection.pdf

[73] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814219/process-evaluation-gps.pdf

[74] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814219/process-evaluation-gps.pdf

[75] https://ico.org.uk/media/about-the-ico/consultation-responses/2013/2153/development-of-electronic-monitoring-service.pdf

96. Failure to charge is a breach of bail conditions[76], 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, but it can also be used for unrelated matters.

97. When the battery runs low, the tag will vibrate and the power light will flash red on the tag until it is charged[77]. This can of course happen at any time of the day or night, thereby waking people up in the middle of the night. It may also occur in public spaces, thereby exposing the fact that the individual is wearing a tag.

98. 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, thereby limiting their freedom of movement considerably beyond what is intended through the imposition of the electronic monitoring condition. This is a particular concern if the battery degrades to the point that multiple charges need to occur within a single day.

99. The individual can be given a portable charger which they can bring with them to charge a device if they are out and about. However 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. Thus, a portable charger is not an answer to a faulty device.

Absence of code of practice

100. The Home Office has published guidance for the use of Electronic Monitoring in the context of probation but not in the context of immigration bail. The difference of approach taken by the Home Office in the context of criminal justice and in relation to immigration is important to note and relevant to considering whether there are the necessary and sufficient safeguards in place in the immigration bail context to prevent against the misuse or abuse of the location data gathered and retained from electronic monitoring.

101. The Code of Practice for Electronic Monitoring[78] for the purposes of probation, in the criminal justice context, is accompanied by a Fair Processing Notice[79], which does not appear to exist in the immigration context. This states that:

---

[76] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051204/immigration_bail.pdf "maintaining their EM device and any mobile phone issued to them as outlined in the induction leaflets issued by the supplier to include charging the device daily until fully charged"

[77] 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

[78] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf

[79] https://www.gov.uk/government/publications/code-of-practice-electronic-monitoring

- "Personal data will be only be 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 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."

(emphasis added)

102. There is no equivalent code in the immigration context. The only policy document is the Immigration Bail Guidance. 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."* 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.

103. HM Prison & Probation Service's 'Information for victims' leaflet on location monitoring states that "If the offender has been given a tag by the Parole Board, the tag will be regularly reviewed by the Offender Manager. It will be assumed that the tag will be removed after six months unless it is decided that it is necessary and proportionate to continue monitoring."[80]

104. It is a decision for the criminal courts as to whether to impose an electronic monitoring requirement as part of a Court Order and it is incumbent upon them to consider any statutory safeguards and issues of fairness and proportionality. Probation cannot do so of its own motion.

105. 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.

80 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/823842/Location_monitoring_-_Victims_Leaflet_Print.pdf

There is therefore no independent judicial scrutiny of the use of electronic monitoring in the immigration context.

106. In the criminal justice context, the use of electronic monitoring is restricted to enforcing compliance with orders and licences. In the immigration context, trail data is used for additional reasons beyond monitoring compliance with immigration bail conditions, including, according to the Immigration Bail Guidance (page 28), substantive immigration applications for leave to remain made by an individual under Article 8 ECHR (see section below for concerns in this regard).

109. The Electronic Monitoring Code of Practice[81] states that EM data must only be "processed for specified, explicit and legitimate purposes." The Home Office's Immigration Bail Policy identifies four purposes for which GPS data may be accesses, not all of which concern an individuals' compliance with immigration bail. In light of the volume and granularity of data collected, much of the data collected will be irrelevant to those purposes but will nevertheless be collected in bulk, potentially over a period of years.

Concerns about purposes of trail data processing

107. The Home Office has set out several uses for trail data. Here we examine the different circumstances in which the Home Office seek to access and use the data, and then set out a list of questions that need to be raised in relation to these in Annex A. The detail can be found in the Home Office Immigration Bail policy (Version 11) 'Implementation' section:

"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

Anonymised data may be used to understand the impact of EM and the behaviours of those on EM to continuously improve the service and to inform immigration policy in accordance with data protection law."

81 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf

(Emphasis added)

108. Taking each of the circumstances in which trail data can be accessed in turn, we note the lack of clarity firstly around how the Home Office will be able to directly access the data, i.e., whether this will be via a login to the Electronic Monitoring System or being sent the data by email, for example. These raise questions around access controls and security.

109. Secondly, it is unclear how breach notification works on a practical and technical level, in terms of how the alerts are set up, and whether data is automatically shared by the Electronic Monitoring Service with the Home Office. This has implications for the necessity and proportionality of data sharing.

110. It is also unclear what is meant by 'intelligence suggesting a breach has occurred', and what sources can form the basis of this intelligence if it is other than the tag itself.

111. The arguably unnecessary and disproportionate interference relating to the volume of data that is shared with the Home Office upon each individual breach of bail conditions should therefore be scrutinised. The Data Protection Impact Assessment[82] states that:

> "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."[83]

112. This means the Home Office has access to the whole trail data as soon as a breach is notified. They do not specify if they delete the data they have been transferred after a breach alert or after finding that it was, for example, an error.

113. Further elaboration is provided in the Data Protection Impact Assessment which indicates the Home Office intention to use this opportunity to trawl the data to find other breaches, without adequate safeguards in place to ensure this is necessary and proportionate:

> "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.

[82] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf
[83] [p.9]

> 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 – 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."

114. Third, turning to the ability to access trail data where relevant to 'a claim by the individual under Article 8 ECHR', this is the most extensive potential re-use that is contemplated by the Home Office. This relates to Article 8 representations and to further submissions[84]. Further submissions[85] are a method by which individuals can submit new evidence to support their asylum claim.

115. The DPIA 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 which can cause unnecessary delays in considering the claims.**"[86]

116. This puts an enormous burden on an individual to recall events recorded by the GPS tag, which could be years in the past. It shows no appreciation for issues relating to 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. Previously the only thing an individual would need to remain conscious of during their bail is to comply with their conditions, now they will need to think about how every single one of their movements might impact their Article 8 representations or further submissions.

117. There do not appear to be any safeguards in place to address the imbalance this creates between the tagged individual and the SSHD. For example, there are no arrangements for prior independent authorisation for access to such intrusive data.

118. As BID have stated:

> "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

[84] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf
[85] https://www.gov.uk/government/publications/further-submissions
[86] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf

> 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"."[87]

119. In light of the standards of evidence, those subject to immigration bail will be much more vulnerable to data being used against them. In criminal cases, the burden falls on the Crown to prove an allegation to the criminal standard (beyond reasonable doubt) whereas in immigration cases, the Appellant/Applicant carries the burden to the civil standard (on the balance of probabilities). When an allegation is made against an Appellant/Applicant in immigration proceedings, the decision maker need only decide whether it is more likely than not that it is proved. This risks findings of fact being made on a very tenuous and unsafe basis to the disadvantage of Appellants/Applicants.

120. Fourth, the Home Office refer to sharing data with law enforcement agencies. However, the intention goes beyond what is set out in the Immigration Bail guidance. Where there is an alert of breach of bail conditions, which could include depletion of battery, all trail data goes to the Home Office. The Home Office then trawl that data for 'any other indication that criminal activity has taken place' and share that with Law Enforcement agencies[88].

> "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 the data may be processed and shared with Law Enforcement agencies under Part 3."

121. There is also to be more regular data sharing. The Home Office permits the sharing with law enforcement agencies. The DPIA states that "The MOJ operate and maintain the police dashboard. It will display all details of every IE tag wearer in the UK and will be updated weekly by MOJ, after receipt of data from a third-party supplier 'EMS'. … The sharing of this data to police colleagues is not new. It is just that the data can now be centralised, collated, and analysed easier."[89]

---

[87] [Code of Practice: Electronic Monitoring, Electronic Monitoring Directorate, October 2020 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf].
[88] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf
[89] https://privacyinternational.org/sites/default/files/2022-02/67021%20Wood%20Annex%20B.pdf

122. The ability to centralise, collate and analyse data is a significant and substantial new capability given insufficient attention in the DPIA. It is disingenuous to indicate that it is not new.

Contracting / Third parties

123. The Ministry of Justice are the contract owners and Electronic Monitoring Services are the service suppliers. Criminal Casework manage their FNOs through tagging and EMS provide data direct to CC to respond to any Immigration Bail Condition breaches.

124. To procure the tags, the Ministry of Justice designed a single end-to-end service split into four Lots:

- the monitoring service;
- the monitoring and mapping software;
- the monitoring hardware; and
- the network

125. These were awarded respectively to:

- Capita, who were awarded a contract valued at £229,000,000 in 2014[90];
- G4S monitoring technologies who were awarded a contract valued between £29,000,000 and £53,000,000[91];
- Airbus Defence and Space Limited, awarded a contract valued at £10,400,000[92]; and
- Telefonica who were awarded a contract for £3,200,000[93].

126. It has been argued by Reform[94] that doing this divides accountability and creates compatibility challenges. The horizontal model also means that none of the providers will face any competition for the duration of their contracts (six years for the monitoring service provider and three years for the other three providers). The one-off tender for a single supplier of each service element cements the market position of those providers and hinders entrants[95].

[90] https://www.contractsfinder.service.gov.uk/notice/6b7768af-64c7-42c1-9ca2-47999949084f?origin=SearchResults&p=1
[91] https://www.contractsfinder.service.gov.uk/notice/453fb31d-e00e-43fb-b7d2-413c3216a765?origin=SearchResults&p=1
[92] https://www.contractsfinder.service.gov.uk/notice/e8255365-4e01-422e-a797-6d24e8afc1fa?origin=SearchResults&p=1
[93] https://ted.europa.eu/udl?uri=TED:NOTICE:284886-2014:TEXT:EN:HTML
[94] https://reform.uk/sites/default/files/2018-10/Tagging%20report_AW_8.pdf
[95] https://reform.uk/sites/default/files/2018-10/Tagging%20report_AW_8.pdf

127. It is unclear whether Electronic Monitoring remains split into four lots. Capita were recently awarded an extension of their contract[96] however this states that: "This notice announces the award of three (3) of the originally advertised four (4) contracts for the provision of the next generation of electronic monitoring (EM) services and supplies in England and Wales, being Lots 1, 2 and 4.

> I. Monitoring service including the processing centre, related hardware and software, and field operatives (Lot 1);
> II. Monitoring and mapping software applications (Lot 2);
> III. Monitoring hardware (anklets etc.) and firmware and software; and
> IV. Network (Global System for Mobile Communications (GSM)) (Lot 4)."

128. We note there is a tendering process that closed in April 2022 for Electronic Monitoring[97].

Data analytics and anonymisation

129. There appears to be a degree of automated processing and data analytics that takes place in relation to electronic monitoring. However, this is not explicit or there is insufficient detail.

130. Trail monitoring implementation refers to the use of anonymous data.

> "anonymised data may be used to understand the impact of EM and the behaviours of those on EM to continuously improve the service and to inform immigration policy, in accordance with data protection law".

131. Anonymisation is the process of rendering data into a form which does not identify individuals and where identification is not likely to take place. We do not accept that it is possible to truly anonymise trail data given that it is collected 24/7 and would include an individual's home address amongst other identifying data.

132. The data gathered as a result of both GPS and the mobile network data is highly personalised in nature. In the 2014 paper On the anonymizability of mobile traffic datasets[98], the authors concluded that:

> "[...] mobile traffic fingerprints tend to have a non-negligible number of elements that are much more difficult to anonymize than the average sample. These elements, which determine a characteristic dispersion and long-tail behavior in the distribution of fingerprint sample distances, are mainly due to a significant diversity along the temporal dimension. In other words, mobile users may have similar spatial

[96] https://www.capita.com/news/capita-extends-moj-contract
[97] https://www.contractsfinder.service.gov.uk/notice/cdf01f23-7054-4f81-8215-695fb4a7a8f9?origin=SearchResults&p=1
[98] https://arxiv.org/abs/1501.00100

fingerprints, **but their temporal patterns typically contain a non-negligible number of dissimilar points**.

It is the presence of these hard-to-anonymize elements in the fingerprint that makes spatiotemporal aggregation scarcely effective in attaining anonymity. Indeed, in order to anonymize a user, one needs to aggregate over space and time, until all his long-tail samples are hidden within the fingerprints of other subscribers. As a result, even significant reductions of granularity (and consequent information losses) may not be sufficient to ensure non-uniqueness in mobile traffic datasets.

As a concluding remark, we recall that such uniqueness does not implies[sic] direct identifiability of mobile users, which is much harder to achieve and requires, in any case, cross-correlation with non-anonymized datasets. Instead, uniqueness is a first step towards re-identification. Understanding its nature can help developing mobile traffic datasets that are even more privacy-preserving, and thus more easily accessible."

(Emphasis added)

Annex A: Questions

The ability to retain and access trail data is significant and requires much greater clarity on a number of issues:

Access

1. How does the Home Office gain access the trail data? For example, if a breach occurs, is trail data sent to them or are they given access to the trail data on the Electronic Monitoring supplier's systems via direct login? Respectively, what security and access control measures are in place?

In relation to a breach of immigration bail conditions:

2. How is the data processed and analysed by the Electronic Monitoring Service ('EMS') i.e., the private provider, for the purpose of breach identification and notification? How does the system function i.e., alerts set up, automated monitoring for breaches, alert triggered, and data sent to the Home Office?

3. Do the notifications involve automated decision-making? E.g., if low battery is detected and noted on the system, is this a wholly or partly automated process? E.g., if an individual enters an exclusion zone, is this wholly or partly an automated process?

4. Does any human review take place before the alert is sent to the Home Office together with trail data?

5. How are the alerts formulated that would then flag a breach of bail conditions in the GPS tag location data and the EMS system? Are they subjective i.e. individualised for each person or objective i.e. there are standard alerts that apply to all individuals on immigration bail e.g. if the GPS tag stops sending location logs or runs out of battery there will always be a breach of bail notification? Or both?

6. What data is provided to EMS to enable them to monitor for and flag breaches? Does the Home Office provide the bail conditions to EMS, who then sets up the notifications in their systems? Or does the Home Office set up the notifications themselves, avoiding EMS having to know about individuals' bail conditions? Is additional information shared beyond bail conditions regarding an individual?

7. Are individuals subject to GPS tags provided with a list of the flags/alerts that the Home Office sets up with the EMS supplier which will result in the individual being flagged to the Home Office or a breach being suspected?

8. What procedure is in place for the establishment, review and oversight of an automated system, if this is what is used? E.g., flagging false positives?

In relation to a breach of immigration bail based on intelligence:

9. How does the Home Office 'suspect' that a breach of immigration bail has occurred based on 'intelligence', if they don't have access to the data or any alert system until a breach is suspected?

10. What can form the basis of 'intelligence' that can suggest a breach has occurred? What is meant by 'intelligence' suggesting a breach has occurred. Does this process constitute 'profiling' (see Article 4 GDPR)?

Sharing with Law Enforcement

11. The DPIA states that:

    "Data detailing the number of 'tagged' cases will be presented on a report known as the Police Dashboard. It will only show high level data Name Nationality DOB Address. It will not show any trail data or breach data. This data can be accessed by MOJ, IE and Police via permissions operated by MOJ.

    The sharing of this data to police colleagues is not new. IE currently share these details with police on a Police Risk Notification Form in all cases where an FNO is released from detention into the community. It is just that it will also be presented to police in this new format. This will provide a clearer picture for data analysis for IE MOJ and Police, given that the number of tag wearers is expected to rise from 280 to 4500."

    It appears that whereas in the past high-level data would only be shared with the police in cases where an FNO is released from detention into the community, now details of *all* IE tag wearers will be shared through the Police Dashboard. Is this correct?

12. Is there a data sharing agreement between the HO and the police? Or some other MoU or policy allowing and governing the data sharing?

Removal of the tag

13. When are the tags removed? How long can someone remain subject to a deportation order? How does the Home Office check it remains reasonable and proportionate?

Immigration and asylum decisions

14. The Policy states that "where it may be relevant to a claim by the individual under Article 8 ECHR" trail data will held by the EM supplier may be accessed by the Home Office. Are individuals informed that trail data could be used in immigration decisions? If so, through what means?

15. Do individuals have the right to request access to their trail data in order to provide evidence in support of their Article 8 ECHR claims?

16. Is the Home Office required to contact the individual to inform them that they have accessed their data when it is being used in relation to an Article 8 claim?

Accuracy issues

17. What processes are in place to account for accuracy issues in the case of suspected bail breaches and when trail data is used to substantiate Article 8 representations and further submissions?

18. What assessment has been carried out to consider how an individual could challenge the accuracy of this location, especially when accuracy of just 10 meters can have profound consequences on what location an individual was in (e.g., at a school or visiting a friend next door to a school? At a place of work or at a café every day to read and do admin?)? This requires technical expertise – have provisions been made (such as training staff) to enable the Home Office to consider accuracy issues?

Data analytics

19. We note that the DPIA refers to suspicion of working, based on being at a location other than home between 08.00-17.00, as a breach of bail conditions. Does the EMS system analyse the data for patterns and/or indicators that an individual may be working?

Annex B: The legislation

1. Immigration bail can be granted by the SSHD or by the First Tier Tribunal (FTT). Schedule 10 of the Immigration Act 2016 (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, subject to deportation proceedings or are under a deportation order. These duties were commenced on 31 August 2021.

2. A bail condition requiring a person to be subject to electronic monitoring can be combined with restrictions on their movements, including curfews and conditions on where they can go (called inclusion or exclusion zones) (paragraph 2(1) Schedule 10 IA 2016). Pursuant to paragraph 2(1) of Schedule 10, the SSHD must impose at least one immigration bail condition on those not subject to deportation proceedings or under a deportation order. These conditions are set out at paragraphs 2(1)(a)-(f) of Schedule 10, and Electronic Monitoring ("EM") is one of the potential immigration bail conditions the SSHD can impose (as per paragraph 2(1)(e)).

3. The mandatory duty under Schedule 10, paragraph 2 Immigration Act 2016 to impose an electronic monitoring bail condition applies to everyone who is liable to be deported, at any point within the deportation process, from the point at which the Secretary of State for the Home Department ("SSHD") 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.

4. Paragraph 4(1) of Schedule 10 sets out the power to impose an electronic monitoring condition. Its purpose is to require a person 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 person's location at specified times, during specified periods of time or while the arrangements are in place.
    - A person's presence in a location at specified times, during specified periods of time or while the arrangements are in place.
    - A person's absence from a location at specified times, during specified periods of time or while the arrangements are in place.

5. The arrangements may include: (Paragraph 4(2) Schedule 10):

    - A requirement for a person to wear a device.
    - A requirement for a person to make specified use of a device.
    - A requirement for a person to communicate in a specified manner and at specified times or during specified periods.
    - The exercise of functions by persons other than the Secretary of State.

6. Schedule 10 provides exemptions for people who are under 18, or 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.

7. Immigration bail can be granted by the Secretary of State or by the First-tier Tribunal. The decision to impose electronic monitoring (EM) is mandatory requirement in certain circumstances as noted above. The decision as to whether an exemption applies is a decision for the Secretary of State. The Tribunal has no jurisdiction over whether an exemption applies and no discretion as to whether or not EM should be imposed where it is a mandatory requirement or where the SSHD has made a decision that it should be.

8. If bail is granted by the SSHD, then the SSHD will not impose EM if the SSHD considers imposing such a condition would be impractical/contrary to the individual's convention rights (para 5(a) and (b) of Schedule 10). In cases where immigration bail is granted by the First-Tier Tribunal, the Tribunal cannot impose such a condition where the SSHD considers that the condition would be contrary to an individual's convention rights/impractical (paragraph 2(7) and 2(8) of Schedule 10).

9. Schedule 10 makes no reference to the technology used in the EM condition. The introduction of GPS monitoring was a policy decision.