THE ASSOCIATION OF BRITISH INVESTIGATORS
POLICY & GOOD PRACTICE GUIDE
USE & DEPLOYMENT OF GLOBAL POSITIONING SYSTEM (GPS) ELECTRONIC TRACKING DEVICES

CONTENTS

PART A - POLICY

USE & DEPLOYMENT OF GLOBAL POSITIONING SYSTEM (GPS) ELECTRONIC TRACKING DEVICES (tracking devices)

1. LAWFUL

Professional investigators must ensure their surveillance activities adhere to legal standards. This means their actions should be Justified, Accountable, Proportionate (and reasonable), Appropriate, and Necessary. This framework is often summarized by the acronym JAPAN.

2. DPIA

It's crucial for professional investigators and / or clients (depending on their respective UK GDPR roles & responsibilities) to conduct a data protection impact assessment prior to initiating any investigation that poses a high risk of harm to the individual. This is especially important when considering deploying tracking devices. For detailed guidance on conducting a data protection impact assessment and access to an optional template, refer to the ABI UK GDPR Code of Conduct for Investigative & Litigation Support Services.

ABI UK GDPR Code of Conduct for Investigative & Litigation Support Services

3. CONFIDENTIALITY

3.1. A tracking device is a covert surveillance aid, and its use / deployment should be treated with respect and strict confidentiality.

3.2. No reference to the use or deployment of a tracking device needs to or indeed should be made outside the confidentiality of the client and surveillance deploying operatives.

3.3. Under no circumstances must tracking device data records or software access (log-in details to access the mapping programme) be provided to the client or anyone outside the surveillance team.

3.4. Details of the data gathered with the aid of a tracking device should in the interests of both transparency and compliance, be recorded and retained by the professional investigator after every surveillance deployment.

4. PRIVATE LAND

A tracking device must never be deployed on private property without the owner's consent. Deployment of such a device is only permissible when the subject vehicle is in an area that the public can legitimately access, regardless of whether access requires payment.

5. PHYSICAL SURVEILLANCE AID

5.1. A tracking device should generally be used as a supplementary tool to physical surveillance, except in extraordinary situations involving evidence gathering.

5.2. Any information obtained from a tracking device serves as covert support for physical surveillance and should be treated as "intelligence only." Such information should not be presented or treated as standalone "evidence" in any investigation.

6. DATA LOGS

The data logs produced by a tracking device should not form the sole basis of any evidential statement, or report.

7. PUBLICATION OF USE / DEPLOYMENT

7.1. Tracking devices are used covertly, so professional investigators should not publicly disclose their use or availability, except in the context of selling related hardware or software, and always in compliance with this policy.

7.2. To avoid any misunderstandings, requests for deploying or retrieving tracking devices must be kept within the surveillance team and not discussed in any group forums.

7.3. Since tracking devices serve as covert tools to assist physical surveillance, any mention of their availability, use, or deployment should clearly align with this policy.

PART B - GOOD PRACTICE GUIDE

USE & DEPLOYMENT OF GLOBAL POSITIONING SYSTEM (GPS) ELECTRONIC TRACKING DEVICES (tracking devices)

8. INTRODUCTION

8.1. Formed in 1913, The Association of British Investigators (ABI) has been upholding professional standards for over a century. The ABI campaigns tirelessly for the wider accountability of professional investigators in the UK and promotes excellence, integrity and professionalism within the sector. The ABI has become the kite mark for the investigation industry.

8.2. The use of tracking devices on vehicles by professional investigators is a topic of frequent discussion, and there are numerous misconceptions surrounding it.

8.3. In January 2012 the Information Commissioner's Office (ICO) written evidence to the Parliamentary Home Affairs Select Committee stated that the 'ICO would support any industry initiatives aimed at promoting informational best practice amongst investigators' (see summary of ICO evidence). This policy and guide, one of several published by the ABI, follows that invitation.

Written evidence submitted by the Information Commissioner's Office [P 108]

8.4. The ICO views the use of tracking devices as a form of surveillance that likely involves processing personal data under the UK GDPR and the Data Protection Act 2018. The ABI acknowledges this perspective. However, there is currently no specific government-sponsored regulation providing guidance for professional investigators on the use and deployment of tracking devices.

8.5. In any investigation involving the processing of personal data, it is crucial for the controller to establish a lawful basis for initiating the investigation. To achieve this, where there is a high risk of harm to the individual, a professional investigator, as controller or to assist the controller or as a matter of good practice, conducts and documents a data protection impact assessment, as outlined earlier in paragraph 2 above. Typically, professional investigators depend on the client's legitimate interest as the lawful basis for processing personal data, provided that this interest outweighs the data subject's rights and freedoms under the UK GDPR.

9. PURPOSE

9.1. The ABI holds that this policy and guide will provide professionally minded and responsible investigators in the private sector with a clear comprehension of how and when tracking devices can be used, especially in scenarios where the vehicle owner's consent is not present.

9.2. This guidance aims to ensure that tracking device usage adheres to legal and ethical standards, balancing investigative needs with individual rights and privacy concerns.

10. GPS ELECTRONIC TRACKING DEVICES

10.1. A tracking device is typically attached to a moving vehicle or carried by a person to monitor their location. It utilises the Global Positioning System (GPS) to accurately determine and track its precise location. This functionality allows the operator, often a surveillance operative, to identify the likely geographic address or locality of the device, and by extension, the vehicle or person under surveillance. The technology is designed to provide detailed location data within a relatively small area, enabling effective monitoring while adhering to ethical and legal standards.

10.2. The recorded location data can be stored within the tracking device, or it may be transmitted to a central location database. This allows the device's location to be displayed against a map backdrop either in real time or when analysing the data later, using tracking device software (recorded history of device locality/movement).

10.3. Tracking devices are tools designed to gather information about the movements of an object or person. These devices are often compared to traditional surveillance methods, such as one person physically following another, as they serve a similar purpose. By utilising technology, tracking devices extend this capability, offering a discreet and efficient way to monitor movement. Similarly, just as a camera captures visual information, a tracking device captures and records location data, enhancing the ability to gather intelligence without the need for physical presence. This technological approach provides a modern complement to human surveillance efforts, ensuring continuous and accurate monitoring.

10.4. Data collected from tracking devices should be treated as supplementary rather than standalone evidence when introduced into legal or investigative contexts. Tracking device data primarily indicates the location or movement of an object or person, such as a vehicle, at specific times. However, for it to serve as credible evidence, it must be corroborated by additional evidence, such as physical surveillance, witness testimony, or other verifiable information. This corroboration ensures the accuracy and reliability of the conclusions drawn from the tracking data and helps establish a more comprehensive and legally sound evidential chain. The combination of tracking data with corroborating evidence strengthens its legitimacy and utility in investigative and legal processes.

11. THE REGULATION OF INVESTIGATORY POWERS ACT 2000

11.1. The Regulation of Investigatory Powers Act 2000 (RIPA) only applies to public bodies and is intended to provide safeguards in the way evidence to support a prosecution is obtained.

11.2. RIPA does apply to investigators in the private sector that are working for a public body that is covered by the legislation (e.g. local authorities, the Environment Agency etc.) and the directed surveillance [1] being conducted requires RIPA authority. Since 2012 local authorities require judicial authority for directed surveillance (local authorities cannot authorise intrusive surveillance [2] under RIPA).

11.3. When deploying and using tracking devices, the ABI recommends adhering to the principles of RIPA (Regulation of Investigatory Powers Act) as a standard of good practice within the private sector. This implies that tracking devices should be used in a manner consistent with the legal and ethical guidelines typically required for surveillance operations. Generally, this means using the device as a covert tool to support physical surveillance efforts.

11.4. Exceptions to this guideline may occur in specific, exceptional circumstances where gathering evidence necessitates a different approach. However, as a rule, tracking devices should serve to complement and aid traditional surveillance methods rather than replace them. This practice ensures that any data collected is handled responsibly and with respect for privacy and legal standards.

11.5. RIPA compliance is emphasised to align with the principles of lawful surveillance and demonstrate that efforts were made to gather evidence in a manner consistent with legal standards. By adhering to the spirit of the RIPA, those in the private

[1] Directed surveillance is covert, but not intrusive surveillance; it is conducted for the purposes of a specific investigation or operation; it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation)
[2] Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device.

sector can better ensure that the evidence they collect will be admissible in court.

11.6. This compliance helps minimise the risk of evidence being excluded under Section 78 of the Police and Criminal Evidence Act 1984 (PACE), which allows courts to exclude evidence if its admission would have an adverse effect on the fairness of the proceedings. Moreover, it supports adherence to Article 8 of the Human Rights Act 1998 (HRA), which protects the right to respect for private and family life. Ensuring that surveillance activities align with these legal frameworks reduces the likelihood of evidence being challenged on the grounds of privacy violations or unfairness during any subsequent litigation.

11.7. Every effort must be made to adhere to the provisions of the RIPA throughout all stages of the proposed operation, including during any directed surveillance activities.

11.8. Currently, there is no legislation that specifically prohibits a professional investigator from using a tracking device on a vehicle without the owner's or user's consent. However, this is permissible only if the physical surveillance that the tracking device aids is lawful, ensuring that the JAPAN principles (Justified, Authorised, Proportionate, Accountable, and Necessary) are applied. Additionally, the processing of any personal data captured in its use must be in compliance with the GDPR. Typically, investigators rely on the client's legitimate interest to justify that it outweighs the rights of the data subject. At a minimum, it is recommended as a best practice for the investigator to conduct a documented DPIA, which should include the lawful basis on which the client depends to carry out the investigation.

11.9. Reference is made at Section 26 (4) RIPA - which states:

> *For the purposes of this Part, surveillance is not intrusive to the extent that — It is carried out by means only of a*

surveillance device designed or adapted principally for the purpose of providing information about the location of a vehicle.

11.10. It follows therefore that surveillance using a tracking device is considered directed surveillance under RIPA.

12. THE DATA PROTECTION ACT 2018

12.1. The Data Protection Act 2018 (DPA) came into force on 25th May 2018 and replaced the Data Protection Act 1998, which came into force on 1st March 2000. DPA made it an offence to unlawfully obtain or disclose personal data (s.170, previously s.55 of the 1998 Act).

12.2. The DPA applies to personal data held in all formats, whether electronic, paper, audio, visual or digital records.

12.3. Processing, under the terms of the DPA, covers all conceivable manipulations of personal data including collection, use, storage, disclosure, deletion and amendment. Mere possession of such data amounts to processing.

12.4. The DPA sets out what may or may not be done with personal data [3].

12.5. Any organisation, which determines the purpose and the means by which personal data is processed, must be registered with the ICO and have a DPA notification number.

12.6. According to the ICO, information gathered from a tracking device can identify the person within a vehicle or their activities, thus qualifying as personal data under the DPA.

[3] **Personal data refers to information relating to a living individual who can be identified either (a) directly from that data, or (b) indirectly from that data combined with other information that is in the possession of, or likely to come into the possession of, the data controller. This includes any opinions expressed about the individual and any intentions articulated by the controller or another party concerning the individual. It is important to understand that when identifying an individual relies on both the data already held and other supplementary information (which may not necessarily be data), the data in question is still considered "personal data."**

12.7. Although using a tracking device may involve processing personal data by recording an individual's movements, the ABI maintains that such use, as outlined in this policy and guide, is not considered unlawful.

12.8. If a tracking device is used solely to assist with physical surveillance, any personal data collected would be equivalent to the information that would have been obtained through conventional methods. The following example illustrates this using a straightforward scenario:

> *Example scenario: In preparation for matrimonial proceedings, a professional investigator is engaged to verify the client's suspicion that their spouse (the 'data subject') is engaging in adultery, and to investigate whether the subject might possess undisclosed assets.*
>
> *The professional investigator determines they are the controller and that they may rely on legitimate interest as the lawful basis for the processing of personal data to confirm or refute the suspicion.*
>
> *The investigator tracks the data subject and observes the subject entering a bank, then later meeting with a third party in a car park. The third party joins the subject in their vehicle, and they are observed engaging in inappropriate behaviour, which the investigator documents with photographic or video evidence. The third party then departs, and the investigator follows them to a residence, subsequently researching public or shared registers to identify the third party.*

12.9. The physical surveillance conducted by the investigator likely uncovered the location of a bank account held by the subject, which may or may not have been previously known to the client. Additionally, the surveillance revealed evidence of the

subject engaging in a clandestine or improper relationship, with the inappropriate behaviour being documented through photographic or video means.

12.10. If only a tracking device had been used without accompanying physical surveillance, these specific details, such as the location of the bank and the nature of the personal interaction, may not have been revealed. The log from the physical surveillance would include notes on the third party's vehicle and residential address. Further investigation using public or shared registers would enable the identification of the third party involved.

12.11. In the scenario described the investigator's actions of conducting physical surveillance and gathering data about the subject's activities, such as bank account details and relationships, were carried out within legal boundaries. As long as the data collected is used appropriately and for its intended purpose, it should not breach the data protection laws or any other relevant regulations. The data should be handled with care, ensuring that it is processed lawfully, transparently, and only for legitimate purposes.

12.12. The use of a tracking device to complement physical surveillance primarily records the location and movements of the subject's vehicle. This data collection method does not inherently breach legal standards, given it is part of a broader, legally conducted investigative process.

12.13. Nevertheless, it is crucial that any data collected using the tracking device is used responsibly and in accordance with applicable legal frameworks, ensuring privacy and data protection rights are respected.

12.14. Whilst it could be argued that the above physical surveillance could have been conducted without the aid of a tracking device, it is fair to counter argue that without the device the prospects of losing the data subject are increased and it also

diminishes the risk of committing moving road traffic offences.

13. TRESPASS

13.1. Civil trespass to land occurs when an individual enters or remains on another's property without permission, or when someone places or projects an object onto that property. This type of trespass is actionable per se, which means it can be subject to legal action without the requirement to demonstrate actual damage. Examples of trespass to land include walking onto property without consent, staying on the property after permission has been revoked, or throwing objects onto the property. A civil trespass, however, is not a crime.

13.2. It may be a civil trespass to deploy a tracking device onto a vehicle not belonging to you or your client but in a 2007 restricted report given by the Office of Surveillance Commissioners (OSC), the OSC's Chief Surveillance Commissioner, Sir Christopher Rose, stated 'putting an arm into a wheel arch or under the frame of a vehicle is straining the concept of trespass'.

2009 DT article referencing OSC report

13.3. The judiciary refers to this concept of trespass as 'de minimis,' meaning the law does not concern itself with trifles, and would not entertain a complaint for such minor intrusions. For example, an act that is technically an infringement can be considered de minimis if it is so minor that it falls outside the purpose of the law, thus allowing for the claim to be dismissed.

13.4. This could be further strengthened if the professional investigator can verify the legality of the surveillance and demonstrate integrity.

13.5. However, as recommended above, professional investigators should comply with RIPA. Entering private property to deploy a tracking device would go beyond directed surveillance, violating the acceptable boundaries of RIPA and human rights regulations. Such practices are unacceptable and contrary to this policy.

13.6. Surveillance conducted from a common area is not considered intrusive due to the definition of residential premises. According to RIPA (Part II), surveillance is not deemed intrusive if it is carried out using a device primarily designed or adapted to provide information about a vehicle's location. If the device is supported by physical surveillance, it will merely offer the location of the vehicle, corroborated by both physical surveillance and the direct evidence of the investigator(s). Documentation of a vehicle's presence at a specific location on private land, at a specified date and time, can be provided by the investigator(s) and substantiated through their choice of media.

14. HARASSMENT & STALKING

14.1. The public may occasionally misinterpret various forms of surveillance as stalking.

14.2. Stalking refers to a specific type of harassment, characterised by a sustained pattern of continuous and repeated contact with, or efforts to contact, a specific victim. Recent legislation has criminalised this kind of harassment.

14.3. Examples of behaviour commonly linked to stalking include: direct communication; physically following the victim; reaching out indirectly through friends, colleagues, family, or technology; and other invasions of the victim's privacy. Such actions restrict the victim's freedom, causing them to feel the need to be perpetually cautious.

14.4. In numerous instances, individual actions may seem harmless when viewed in isolation. However, when these actions are repeated as part of a pattern of behaviour, they can cause significant alarm, harassment, or distress to the victim.

14.5. If the individual being observed becomes aware of the surveillance, it could potentially be considered harassment under the Protection from Harassment Act 1997.

14.6. Similarly, if an individual becomes aware of a tracking device being used on them, this might also constitute harassment under the Protection from Harassment Act 1997. This would apply if those using the device engage in a course of conduct that:

- Involves actions that could be considered harassment of another person, and
- The individuals using the device either know or ought to know that their actions could be perceived as harassment by the person being tracked.

14.7. Surveillance should only be carried out following the guidelines set by legislation designed to regulate covert activities by public bodies, including the police and government agencies, such as those outlined in RIPA.

14.8. Therefore, using a tracking device without considering the need for in-person surveillance may be interpreted as harassment, stalking, or even voyeurism in certain situations.

15. HUMAN RIGHTS ACT 1998 (HRA)

15.1. For professional clients, the main concern with using a tracking device often revolves around reputation. While their use is legal, there is a common perception that it might be viewed as distasteful, underhanded, or unethical.

15.2. Public authorities only need to consider RIPA authorisation when covert surveillance is likely to violate Article 8 of the HRA and a criminal prosecution is being considered.

15.3. Police are permitted to attach a tracking device to the outside of a vehicle without a warrant. However, if they wish to install a tracking device inside the vehicle, a warrant is required. Intrusive surveillance refers to secret monitoring within residential areas or private vehicles, where individuals have a higher expectation of privacy compared to public spaces. This type of surveillance is deemed intrusive when it involves a person or a surveillance device being present inside the premises or vehicle. Notably, placing a tracking device on the exterior of a vehicle is not considered intrusive surveillance, as it falls outside the definition of such activities.

16. JONES v WARWICK

16.1. Anyone has the potential to infringe upon another person's human rights. A pertinent case illustrating this is "Jean F Jones v University of Warwick (2003)." In this case, although the video footage was allowed as evidence because it served to disprove the claim, the court determined that the deception used by the investigators constituted a breach of the claimant's human rights.

16.2. According to Section 6 of the Human Rights Act (HRA), only public authorities are forbidden from acting in ways that are incompatible with the Act. While courts are considered public authorities, insurance companies and professional investigators are not, unless they are acting on behalf of a public authority. However, the court will take the HRA into account when evaluating the evidence.

16.3. In the referenced case, professional investigators working for an insurer obtained valuable video footage of the claimant by deceitfully entering the claimant's home under false pretences. The court criticised the investigators' tactics, particularly their trespassing, but it did not, and could not, determine that the investigators had violated the HRA. The issue before the court concerned whether the evidence obtained in this manner could be admitted in subsequent proceedings, and the court rejected the claim regarding inadmissibility. This case holds significant implications when examining the human rights considerations related to the use of tracking devices, warranting closer analysis.