Association of British Investigators
Upholding Professional Values

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

CONTENTS

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

1. INTRODUCTION & COPYRIGHT

1.1. Formed in 1913, The Association of British Investigators (ABI) has been upholding professional standards for over a century. The ABI campaigns tirelessly for regulation for investigation in the private sector and promotes excellence, integrity and professionalism within its membership. The ABI has become the kite mark for the investigation industry.

1.2. The utilisation of GPS Electronic Tracking Devices on vehicles by private sector investigators is often discussed and there are many misunderstandings. In 2006 the Information Commissioner's Office (ICO) produced two reports entitled 'What Price Privacy?' and 'What Price Privacy Now?' The reports documented the apparent unlawful trade in personal information, in which private investigators were allegedly found to play a significant role.

1.3. The reports contained a recommendation that the ABI should extend its National Occupational Standard for Investigation to include explicit reference to Section 55 [1] offences, and undertake other specific measures aimed at raising standards among private investigators. This was duly done.

1.4. In January 2012 the ICO's 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' [2].

1.5. The ABI concedes the ICO point that their deployment as a surveillance tool may constitute processing personal data within the meaning of the Data Protection Act 1998 (DPA).

1.6. There is no specific government-sponsored regulation to assist private sector investigators with regards to the use and deployment of GPS Electronic Tracking Devices.

1.7. In its commitment to the promotion of good practice in the investigation sector, the ABI publishes this Guide on the use and deployment of GPS Electronic Tracking Devices utilising their own considerable knowledge and experience in this field.

[1] Section 55 of The Data Protection Act 1998; Unlawful obtaining etc. of personal data.
[2] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/writev/1800/m08.htm

2. PURPOSE & DISCLAIMER

2.1. The ABI believes that this policy will give professionally minded and responsible investigators in the private sector a clear understanding of the use and deployment of GPS Electronic Tracking Devices.

2.2. The policy is specifically aimed at ABI members who are bound by the ABI Code of Ethics and accountable to abide by ABI policy guidelines. This is demonstrated by the ABI's robust and independently adjudicated discipline process, that could see substantiated evidence of an ABI member breaching any of this policy's guidelines face expulsion from the ABI.

2.3. The ABI 'Use & Deployment of GPS Electronic Tracking Devices Guide & Policy' is made available to ABI members and the Policies listed at the end of this Guide apply with immediate effect from the date of this document.

2.4. The Policy set out in chapter 9 is binding on the membership of the ABI, however, the contents of this Guide are intended as helpful but not legal advice and the ABI does not warrant or make any representations regarding the correctness, accuracy or reliability of the comments and observations in this publication. Readers of the Guide should obtain their own independent legal advice on any matter referred to in the Guide and be satisfied as to the legal position should they consider using or deploying a GPS Electronic Tracking Device.

3. GPS ELECTRONIC TRACKING DEVICES

3.1. A GPS Electronic Tracking Device is normally carried by a moving vehicle or person. The device relies on the Global Positioning System to determine and track its precise location within a relatively small area sufficient to enable the operator (surveillance operative) to determine the likely geographic address (locality) of the device and the vehicle under surveillance.

3.2. The recorded location data can be stored within the GPS Electronic 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 GPS Electronic Tracking Device software (recorded history of device locality/movement).

3.3. GPS Electronic Tracking Devices provide intelligence on the movement of an object and particularly on a living person. They are not too dissimilar to one person actually following another person ('subject') and are an extension of that capability, as is using a camera to capture what you see.

3.4. Any data or information collected by the use of a GPS Electronic Tracking Device should never be considered in isolation as 'evidence' and introduced into the evidential chain without corroborated evidence. The data merely supports the location of a vehicle, the details of which would be corroborated by physical surveillance.

3.5. A GPS Electronic Tracking Device is a covert aid to physical surveillance and any reference to their use and deployment should be qualified to be compliant with this Policy.

4. THE REGULATION OF INVESTIGATORY POWERS ACT 2000

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

4.2. RIPA does apply to private investigators 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 [3] being conducted requires RIPA authority. Since 2012 local authorities require judicial authority for directed surveillance (local authorities cannot authorise intrusive surveillance [4] under RIPA).

4.3. In the deployment and use of a GPS Electronic Tracking Device the ABI encourages RIPA compliance in the private sector and in particular by its members. Save in exceptional evidence gathering circumstances, this will be achieved by only utilising the device as a covert aid to physical surveillance.

4.4. RIPA compliance would demonstrate, that every attempt was made, to deliver evidence within 'the spirit of the Act' in order to minimise the possibility of such evidence later being ruled as inadmissible under such legislation as Section 78 of the Police and Criminal Evidence Act 1984 (PACE) or Article 8 of the Human Rights Act 1998 (HRA) – 'Right to Respect for Private and Family Life', during any subsequent resulting litigation.

4.5. When deploying a GPS Electronic Tracking Device no authority or activity in respect of intrusive surveillance should ever be sought or attempted in the private sector.

4.6. Every effort should be made to comply within the provisions of RIPA during all aspects of the proposed operation including any periods of directed surveillance.

4.7. There is no current legislation that prevents the use, by an investigator in the private sector, of a GPS Electronic Tracking Device (for example on a vehicle), without the consent of the owner or user of that vehicle, providing that the surveillance is lawful, reasonable and proportionate and the processing of such personal data captured in its use complies with the DPA.

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

4.8.1. For the purposes of this Part, surveillance is not intrusive to the extent that —

4.8.1.1. 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.

4.8.2. It follows therefore that surveillance using a GPS Tracking Device must be directed surveillance under RIPA.

---

[3] 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)

[4] 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.

5. THE DATA PROTECTION ACT 1998

5.1. The Data Protection Act 1998 (DPA) came into force on 1st March 2000 and made it an offence to unlawfully obtain or disclose personal data (s.55).

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

5.3. Processing, under the terms of the DPA, covers all conceivable manipulations of personal data including collection, use, storage, disclosure and amendment.

5.4. Mere possession of such data amounts to processing.

5.5. The DPA sets out what may or may not be done with personal data [5].

5.6. Any business, which determines the manner and the purpose personal data is processed, must be registered as a Data Controller with specific purposes, with the ICO and have a DPA notification number.

5.7. As stated above, the ICO expresses the view that data obtained from a GPS Electronic Tracking Device identifies the individual (within the vehicle) or his activities and it is therefore personal data within the meaning of the DPA. However, some private sector investigators have expressed the view that attaching such a device to a vehicle is no more than that and therefore not processing personal data. The ABI, to avoid further contention, concedes the ICO view.

5.8. However, even though the use of a GPS Electronic Tracking Device may be processing personal data where it records the movements of an individual, the ABI does not consider their use is necessarily unlawful and therefore in breach of the DPA.

5.9. If the GPS Electronic Tracking Device had been deployed purely as an aid to surveillance, then any personal data that had been gathered would be no different from that which would have been gathered without it. The following example is given using the simplest of scenarios: –

5.9.1. In contemplation of matrimonial proceedings, an investigator is tasked to verify the client's suspicion that the spouse (the 'subject') is committing adultery and to further explore whether the subject may be possessed of assets the client may not be aware of.

5.9.2. It is decided that conventional surveillance is lawful, reasonable and proportionate to confirm or deny the suspicion.

5.9.3. The investigator follows the subject and notes the subject calls into a bank and later meets with a female in a car park who gets into the subject's vehicle and where they are observed engaged in inappropriate behaviour, which the investigator records electronically.

[5] Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data". https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

The female then leaves and the investigator follows her to an address, which the investigator researches from public, or consented registers and identifies the female.

5.10. The conventional surveillance probably identified the location of where the subject holds a bank account (either known or unknown to his wife) and revealed that the subject appears to be having a clandestine (improper) relationship, which has been recorded. If the GPS Electronic Tracking Device had been deployed without the physical surveillance it would not have identified the above. The surveillance log would note the female's vehicle and home address and subsequent research identified her.

5.11. In the circumstances described above the investigator had not done anything unlawful and the data gathered, if used correctly and for the purpose for which it was obtained, would not breach the DPA or other regulation.

5.12. Adding a GPS Electronic Tracking Device (as a tool to assist the surveillance) does not alter anything other than recording the data (locality movements of the vehicle).

5.13. Whilst it could be argued that the above surveillance could have been conducted without the aid of a GPS Electronic Tracking Device, it is fair to counter argue that without the device the prospects of losing the subject are increased and it also diminishes the risk of committing moving road traffic offences.

5.14. On 12th April 2016, the ICO published a report [6] in which it stated "We have also had reports about the use of surveillance and tracking devices by PIs, and of PIs failing to give individuals access to information held about them. These are actions which may be in breach of the Data Protection Act."

5.15. In response the ABI made a detailed statement, which included the following:

The ABI too has for some time been concerned about the possible irresponsible use of tracking and surveillance devices and has consulted the ICO, industry and legal experts. However, the ICO report suggests the deployment of such devices, are a breach of the Data Protection Act 1998. This is not necessarily so. In circumstances when the deployment of such devices can be justified are proportionate and the Privacy Impact Assessment is properly thought through and logged, I suggest the ICO would be hard pressed to make a case to prosecute. It is the ABI's view that whilst such electronic devices and their supporting software may process personal data, providing the processing is carried out in compliance of the DPA the use of the device is not 'illegal'

[6] https://iconewsblog.wordpress.com/2016/04/12/private-investigator-crackdown-by-ico/

6. TRESPASS

6.1. A civil trespass to land occurs where a person directly enters upon another's land without permission, or remains upon the land, or places or projects any object upon the land. This tort is actionable per se without the need to prove damage. Walking onto land without permission, or refusing to leave when permission has been withdrawn, or throwing objects onto land are all example of trespass to land.

6.2. A civil trespass, however, is not a crime.

6.3. It may be a civil trespass to deploy a GPS Electronic 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) [7], 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'.

6.4. The judiciary has described this concept of trespass as 'de minimis' (*the law cares not for small things*) [8] and would not countenance a complaint.

6.5. This could be further bolstered if the investigator could provenance the lawfulness of the surveillance and demonstrate integrity and necessity with proportionality and reasonableness.

6.6. However, on the basis as recommended above that investigators in the private sector should be RIPA compliant, to enter the private land of anyone in order to deploy a GPS Electronic Tracking Device would be moving away from directed surveillance and exceeding the acceptable boundaries of RIPA and the human rights regulations. This is unacceptable practice and contrary to ABI policy.

6.7. Surveillance from a common area is not intrusive surveillance due to the definition of 'residential premises'. Under RIPA (Part II), 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. As long as the device is supported by physical surveillance the device will do no more than give a location of the vehicle corroborated by physical surveillance and the direct evidence of the investigator(s). Evidence of the location of a vehicle at a specific location at a specified date and time on private land would be provided by the investigator(s) and supported by their choice of media.

[7] http://www.telegraph.co.uk/news/politics/6194581/Government-officials-track-cars-and-trespass-on-private-property-report-shows.html
[8] For example, an act that is technically an infringement can be called *de minimis* if it is thought to be outside the purpose of the law to catch it; the claim can then be dismissed with costs.

7. HARASSMENT & STALKING

7.1. Surveillance in all of its forms can sometimes be misinterpreted by the public as stalking.

7.2. Stalking is a term used to describe a particular kind of harassment. Generally, it is used to describe a long-term pattern of persistent and repeated contact with, or attempts to contact, a particular victim. Recent legislation criminalises this form of harassment [9].

7.3. Examples of the types of conduct often associated with stalking include: direct communication; physical following; indirect contact through friends, work colleagues, family or technology, or, other intrusions into the victim's privacy. The behaviour curtails a victim's freedom, leaving them feeling that they constantly have to be careful.

7.4. In many cases, the conduct might appear innocent (if it were to be taken in isolation), but when carried out repeatedly so as to amount to a course of conduct, it may then cause significant alarm, harassment or distress to the victim.

7.5. If the subject of enquiry is aware of the tracking, then this may amount to harassment under the Protection from Harassment Act 1997.

7.6. It is also possible that if the subject of enquiry becomes aware of the GPS Electronic Tracking Device, this may amount to harassment under the Protection from Harassment Act 1997 if they pursue a course of conduct:

7.6.1. Which amounts to harassment of another, and

7.6.2. Which he knows or ought to know amounts to harassment of the other.

7.7. Conducting any surveillance should only be contemplated based on the guidance provided within the legislation enacted to control the covert activities of public bodies such as police, government agencies etc. RIPA.

7.8. Therefore using a GPS Electronic Tracking Device without contemplating the need for manned surveillance may be construed as harassment/stalking or even voyeurism in some cases.

[9] Protection from Harassment Act 1997 http://www.legislation.gov.uk/ukpga/1997/40/section/2A

8. HUMAN RIGHTS ACT 1998 (HRA)

8.1. The principal consideration in the use of a GPS Electronic Tracking Device is reputational in that whilst their use is lawful, there is a widely held view, that it could be considered as distasteful, underhand or unethical.

8.2. There is only ever a need for public authorities to consider RIPA authorisation where the covert surveillance is likely to breach Article 8 of HRA and a criminal prosecution is contemplated.

8.3. A widely held interpretation is that simply obtaining data about the movements of a lump of metal (i.e. a car) does not breach an individual's Article 8 rights. Even if you can identify the driver through conventional surveillance this only gives you a record of that person's movements from A to B (and possibly C, D and E).

8.4. Police may use a GPS Electronic Tracking Device deployed on the exterior of a vehicle but must have a warrant to place one inside a vehicle. Intrusive surveillance is covert surveillance in residential premises or private vehicles where someone would have a greater expectation of privacy than in a public place. The surveillance is intrusive if it involves the presence of either an individual or a surveillance device on the premises or inside the vehicle. It does not include a tracking device fitted to the vehicle's exterior - 'The use of a mere tracking device does not equate to intrusive surveillance as it is excluded from the definition'.

8.5. **Jones v Warwick**

8.5.1. Whilst the HRA was brought about to control the activities of Public Authorities, anyone could breach the human rights of another. The case on this is that of Jean F Jones v University of Warwick (2003) - Whilst the video footage was admitted into evidence, as it went to disprove the claim, the deception perpetrated by the investigators was held by the court to amount to a breach of the claimant's human rights. This isn't quite right. By virtue of Section 6 of the HRA only public authorities are prohibited from acting incompatibly with the Act. The court is a public authority but insurance companies and investigators in the private sector patently are not (unless acting as agents for a Public Authority).

8.5.2. In the above case, investigators, acting on behalf of an insurer gained useful video footage of the claimant having tricked their way into her house using a pretext. The court criticised the tactics of the investigators, particularly around the trespass to land, but it did not, and could not, rule that it had breached HRA. The matter before the court was about the admissibility in subsequent proceedings of the evidence obtained. The court dismissed that claim. The potential significant impact of this case is worthy of greater scrutiny when considering the human rights position on deploying a GPS Electronic Tracking Device. A useful article on the case was written by Barrister, Rosalind English, 1 Crown Office Row[10].

[10] http://www.1cor.com/1315/section.nc?startpointt1159i115=810

9. POLICY (investigations in the private sector)

9.1. All directed surveillance activities should be lawful, justified, reasonable and proportionate.

9.2. A Privacy Impact Assessment must be carried out prior to considering the justification in deploying a GPS Electronic Tracking Device [11].

9.3. When deploying a GPS Electronic Tracking Device intrusive surveillance should never be attempted or undertaken.

9.4. A GPS Electronic Tracking Device is a covert surveillance aid and should be treated with respect and confidentiality.

9.5. At no time should a GPS Electronic Tracking Device be deployed on private land without the proprietor's permission. A device may only be deployed when the subject vehicle is in a place to which the public have legitimate access, whether on payment or otherwise.

9.6. Save in exceptional evidence gathering circumstances, a GPS Electronic Tracking Device must only be used in conjunction and as an aid to physical surveillance.

9.7. No reference to the use of a GPS Electronic Tracking Device or the automated software produced log needs to or indeed should be made outside the confidentiality of the client and surveillance deploying agency.

9.8. The data produced by a GPS Electronic Tracking Device should not form the sole basis of any evidential statement, or report.

9.9. Save where the client so instructs, under no circumstances must GPS Electronic 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.

9.10. Any data obtained from a GPS Electronic Tracking Device is a covert aid to the physical surveillance - the data is to be used and classified as 'intelligence only' and should not be communicated or introduced as unsupported 'evidence' in any investigation.

9.11. The use and deployment of GPS Electronic Tracking Devices is covert and therefore an investigator should not openly advertise their use or availability other than in hardware or software sales, without reference to compliance with this Policy.

9.12. Details of the data gathered with the aid of a GPS Electronic Tracking Device should in the interests of both transparency and compliance, be recorded and retained by the investigator after every surveillance deployment.

[11] A data protection risk assessment template is annexed

File Ref:	
Date:	
Principal Operative	

Association of British Investigators
Upholding Professional Values

Privacy Impact Assessment	Check	Action	Comment
1. Are the instructions and investigation justified?			
2. Are the requirements lawful?			
3. Is the deployment of surveillance reasonable?			
4. What alternative methodology has been applied or considered?			
5. Why is a GPS Electronic Tracking Device necessary?			
6. Is the use of a GPS Electronic Tracking Device proportionate?			
7. Is the target vehicle accessible on a public right of way?			
8. Are the Operatives deploying and recovering the Device familiar with the Policy?			
9. Is the GPS Electronic Tracking Device being used in support of physical surveillance?			
10. Is data to be gathered evidenced by physical surveillance?			
11. Are the supporting software and log-in details secure and kept confidential?			
12. Are there secure facilities to collect/store the data for the duration of the operation?			
13. Is the agency notified with the ICO and for the correct purpose (show registration number)?			
14. Do all operatives understand the use of the GPS Electronic Tracking Device is covert?			
15. Do all operatives understand the data is not to be introduced as unsupported evidence?			
16. Has an operative been appointed to secure the data after deployment?			
17. If any operative is not an ABI member, do they meet the ABI membership criteria?			
18. Have all operatives confirmed compliance with the ABI Code of Ethics & Professional Standards?			
19. Have all operatives read, understood and confirmed compliance with this Policy?			
20. Who in the agency privy to the surveillance is the data protection reporting officer?			