Smarter Regulation of Waste in Europe (LIFE13 ENV-UK-000549) LIFE SMART Waste Project

Action B7:

The deployment of electronic tracking devices to detect and prevent waste crime

Prepared by Adrian Evans, Natural Resources Wales
17 January 2019

This report was prepared with the contribution of the LIFE financial instrument of the European Union

AN EU LIFE+ PROJECT FOR 2014–2019

Version 1.4

Table of Contents

List of Figures

Acknowledgements

The LIFE SMART Waste Project Team would like to thank all the individuals and organisations who generously gave up their time for consultation, meetings and workshops, without whose collaboration the insights presented in this report would not have been possible.

Particular recognition should be given to the contributions of:

- Northern Ireland Environment Agency (Colin Gillis);
- Environment Agency (Rob Wood and Paul Moore);
- SEPA (Alasdair Anderson, Fraser Allan and Colin Hershaw);
- Swedish Environmental Protection Agency (Jonas Lundin);
- IMPEL (Huib van Westen);
- INTERPOL;
- Apex Chambers (Lee J Reynolds & Rosamund Rutter).

Legal advice provided by:

- Harper Macleod LLP
- Apex Chambers

Abbreviations

Term	**Definition**
ECHR	European Convention on Human Rights
GDPR	General Data Protection Regulation 2018
GIS	Geographical Information Systems
GNSS	Global Navigation Satellite Systems
GPRS	General Packet Radio Service
GPS	Global Positioning System
IMPEL	EU Network for the Implementation and Enforcement of Environmental Law
LSW	LIFE SMART Waste
NIEA	Northern Ireland Environment Agency
NRW	Natural Resources Wales
RFID	Radio Frequency Identification
RoHS	Restriction of the Use of Certain Hazardous Substances
RIPA	Regulation of Investigatory Powers Act 2000
RIP(S)A	Regulation of Investigatory Powers (Scotland) Act 2000
SEPA	Scottish Environmental Protection Agency
SMS	Short Message Service
WEEE	Waste Electrical and Electronic Equipment

1.0 Executive Summary

This report takes a holistic approach to the possibility of UK environment agencies deploying tracking devices in the prevention and detection of waste crime, examining the types of tracking devices available, how the systems operate, potential application in the waste industry and the risks and challenges in doing so.

Tracking devices vary from both wide area tracking to short range devices. As the name suggests, the wide area devices allow an asset to be tracked over significant distances and are likely the more appropriate type for tracking of waste in many cases, due to the distances travelled from production points.

The potential applications of using such devices within the waste sector are explored within this report. Several approaches can be used for different purposes. The use of tracking devices as an intelligence tool, to obtain evidence, corroborate intelligence and/or to close intelligence gaps is one approach. The merits of using these devices for intelligence purposes is the resource efficiencies when compared with prolonged manned surveillance.

A further application examined is the application of such devices to test and understand local authority waste flow, with the potential to improve collection systems, infrastructure inadequacies and cost efficiencies.

Furthermore, benefits for considering the voluntary application of such devices by a waste industry company are also explored, with the added benefit of enhancing e-doc and support duty of care.

Several pilot ideas in relation to the aforementioned potential applications are illustrated to highlight the scope of use of these devices for tracking waste.

The piloting of a live deployment of tracking devices in a challenging waste stream is considered necessary to evaluate the effectiveness of using this technique, and is explored within the body of this report. It is anticipated that one of the key features to achieving a successful pilot is collaboration. However, according to legal advice and expert opinion, challenges and risks are foreseen for environment agencies in deploying such devices. Careful consideration has to be given to areas of legislation which cover Article 8 of the ECHR, and the Data Protection Act 1998, due to the aspects of processing personal data which will inevitably accompany the live deployment of a tracking device(s). As well as this, there are data security risks that need to be considered should the tracking device(s) be intercepted by third parties.

In summary, the position on the use of tracking devices both from legal advice and expert opinion is that UK environment agencies can lawfully use these devices in certain circumstances to assist in specific criminal investigations. This, of course, would require to be based upon current and reliable intelligence and authorised under a RIP(S)A/RIPA 2000 directed surveillance authorisation.

Taking into consideration both the legal advice and that of the expert group, along with the legislative limitations for environment agencies in respect of their intelligence gathering capabilities, it is recommended that the LSW team do not pilot a live deployment of tracking devices. Rather, recommendations are proposed that target changes in legislation:

- UK environment agencies should be added to Part 3 of the Police Act 1997 to make the deployment a more feasible tactic.

- UK environment agencies should be added to Part 1 of RIPA/RIPSA to allow authorities improved intelligence gathering capabilities.
- New environmental legislation is drafted which accurately reflects the grave threat on a national and international basis that is posed to the environment.

Non-legislative recommendations are also proposed:

- The findings of this report are shared with the UK government and environment agencies discovery project which is scoping a UK waste tracking service.
- The LSW Project Team engage with the Guardia Seprona in Spain and disseminate findings of this report to assist in the Spanish-led action plan under the environmental and wildlife crime EMPACT, which is evaluating and proposing the use of advanced tools such as tracking devices to increase the reaction capability and support investigations in the field of environmental crime.

2.0 Introduction

2.1 Background

The illegal dumping of waste is an international problem. The United Nations Environment Protection has reported that up to 90% of the world's electronic waste, worth nearly £12bn, is illegally traded or dumped each year. Up to 50 million tons of electronic waste - computers, television sets, mobile phones, household appliances - are discarded in the developed world. In Europe a significant proportion of electronic waste is either exported, recycled under non-compliant conditions or discarded in waste bins.[1]

In the UK, reports such as the Environmental Services Association (ESA) Re-thinking Waste Crime 2017 have described the impact and some of the weaknesses that facilitate waste crime:

"Waste crime remains an enormously serious issue. It undermines investment, growth and jobs within the waste and resources industry and threatens our natural environment…. The waste sector operates under a plethora of legislation and policy. But there are some serious failures in this framework. Regulatory effort remains overwhelmingly focused on sites where waste management operations occur. Critically, other parts of the waste management chain, such as waste carriers and brokers are not subject to this level of regulation".

The increased management of waste movements has made regulatory oversight more challenging. Waste is moved across regional, national and international borders in large quantities. A fundamental difficulty for Environment Agencies is the traceability of the waste.

Where it is going, how it is being handled and where it is leaking into the hands of criminal operators. The monitoring and enforcement powers of Environment Agencies is limited, often needing to use or have reference to general Policing Legislation which were not written to specifically target environmental crime. The current paper duty of care system offers little opportunity for regulators to trace waste. Regulators have the difficult task of piecing together a paper chain from one site to the next. This is now a significant vulnerability which criminals can exploit. The electronic tracking of waste should be a weapon readily available to Environmental Agencies to identify where waste is moving to and importantly where criminals are removing it from the legitimate system.

Tracking technology is part of a technological area often referred to as pervasive or ubiquitous computing. This generally refers to the trend towards embedding microprocessors in everyday objects so they can communicate information.[2] Electronic tracking devices are integrated systems that use a combination of different technologies (e.g. Geographical Information Systems - GIS, Global Positioning System - GPS, Global System for Mobile Communications - GSM etc.). It is possible to commission purpose built devices, select products from specialist companies or purchase them directly from a range of internet retailers.

The use of electronic tracking techniques was once an area that was very much associated with the military and covert operations of the Security Services and the Police. However more recently this technology has spread across to the commercial sector to be applied for a wide of range purposes. It is utilised for a multitude of purposes and across diverse

[1] https://unu.edu/media-relations/releases/discarded-electronics-mismanaged-in-europe-is-10x-volume-of-e-waste-exports.html
[2] https://www.techopedia.com/definition/667/pervasive-computing

industries such as transport, agriculture, construction and leisure. Tracking systems are used to manage vehicle fleets, supply chains and parcel delivery. They have become an essential part of our global information infrastructure and new uses are limited only by the human imagination.[3]

Indeed today almost all of us have access to tracking technology in the form of our mobile phones. We are able to access location services for a host of applications from assisting our navigation (e.g. Satnav) to tracking our leisure activities.

In order to provide some clarity on the potential application of tracking devices, this report will examine two types of the technology available:

- Systems which can operate over extended distances (potentially globally) and identify the key components in those systems.
- Systems that operate over a short range (up to approximately 100 metres) and the potential uses of those systems in regulating the waste sector.

The potential for using tracking technology to regulate the waste sector is an exciting prospect, however, this very much depends on the legal system and whether there is scope within it for environmental regulators to deploy such devices, and under what circumstances.

2.2 Aim & Scope

The purpose of this report is to examine the types of electronic tracking devices available, assess their suitability for tracking the movements of different types of waste, and explore the legislative capabilities of an environmental regulator for deploying such devices. The report supports the work on developing waste flow audit approaches and could help fill some of the intelligence gaps identified elsewhere in the project.

The initial part of this report provides an overview of current technology and some of the technical considerations that environmental regulators may face when trying to identify a suitable tracking device. This part of the report aims to provide an insight into the function of key components and to give the regulator a better understanding of the capabilities and limitations of the technology. It is hoped that by improving the understanding of the technology it will assist the planning and successful deployment of devices and may also lead to new applications of the technology. This part of the report will also briefly outline some ideas for possible pilot activities.

An outline pilot proposal is included within this report which aims to properly identify and evaluate the legal, reputational and tactical risks of a live deployment. It is believed that a pilot study is probably the only way of truly achieving the outcomes desired by the project action.

[3] https://www.gps.gov/applications

3.0 Methodology

This report has been developed through efforts in four areas:

3.1 An informal assessment of the current use of tracking devices

Internal assessments at SEPA and NRW were undertaken to identify any current usage of tracking devices. Contact was made through existing regulatory networks to assess usage and identify best practice from other European environment agencies. Information was provided by colleagues in England, Northern Ireland, Italy, Sweden and the Netherlands. Informal discussions were also held with Police Scotland.

3.2 Review of tracking device technology to identify potential pilot applications

Independent desktop research was carried out to further our understanding and utilisation of this technology to tackle waste and environmental crime. This was enhanced through separate research carried out by INTERPOL. The combined assessment led to the identification of potential waste crime applications and five pilot opportunities.

3.3 Legal advice

A critical element of a potential pilot would be to ensure its legality. Legal notes were obtained from Harper Macleod (Scotland) and Apex Chambers (England and Wales). The separate legal notes reflect slightly differing legislation between Scotland; and England and Wales. Part of the legal advice included an assessment of potential pilot scenarios. The full Harper Macleod legal note is included in appendix 2. The legal advice was obtained prior to the introduction of the General Data Protection Regulation 2018.

3.4 UK environmental regulators workshop

A LIFE SMART Waste workshop was held in Manchester on 17 August 2017. The workshop brought together the leading experts in the use of surveillance and tracking devices from the UK environmental agencies. The aim of the workshop was to explore options for the deployment of tracking devices by UK Agencies to detect and prevent waste crime, considering the research carried out and legal advice obtained through the LIFE SMART Waste project.

The workshop covered issues related to the deployment of tracking devices including (but are not limited to) RIPA/RIPSA, Property Interference, Technical Feasibility and Data Security.

The conclusions of the workshop have resulted in the formulation of the recommendations put forward in this report.

4.0 Types of Tracking Devices

4.1 Wide Area Tracking Components and Systems

If the planned application of the tracking device is to follow an asset over any meaningful distance then some satellite positioning and/or mobile telephony triangulation capabilities are likely to be required. The method of communication from the device back to the receptor will also need to be effective, probably beyond the borders of the country of origin, for example with respect to waste exports. The life of the device will be limited by its power source and ability to survive in the conditions in which it is placed. The longer the device remains operational the more likely it is to obtain the valuable data required. This section considers further the key elements and components of a suitable tracking system.

4.1.1 Wide Range Positioning/Location Systems and Connectivity

Satellite Positioning Communications

There are a number of satellite positioning systems now in use. Global Positioning System (GPS) is perhaps the most commonly utilised (and well known) system for determining location by triangulating with at least 3 of the 24 (operational) satellites orbiting the Earth that operate within the GPS system. Each GPS satellite transmits two low power radio signals back to the Earth where they can be picked up by GPS receivers[4]. The higher number of satellites the receiver is capable of correlating with (number of "channels") the more accurate and reliable the location is likely to be. The location is also likely to be more efficiently obtained by the receiver.

Location data can be stored in the receiver or it may be transmitted to a central database, or put on to the internet, using a mobile phone (GPRS - General Packet Radio Service or SMS –Short Message Service), radio, or satellite modem embedded in the unit[5]. This allows the location to be mapped either in real time or when analysing the track later, using Geographical Information Systems (GIS) software. GPS is an example of an extremely accurate way of tracking, capable of giving a positional accuracy of within 10 meters[6].

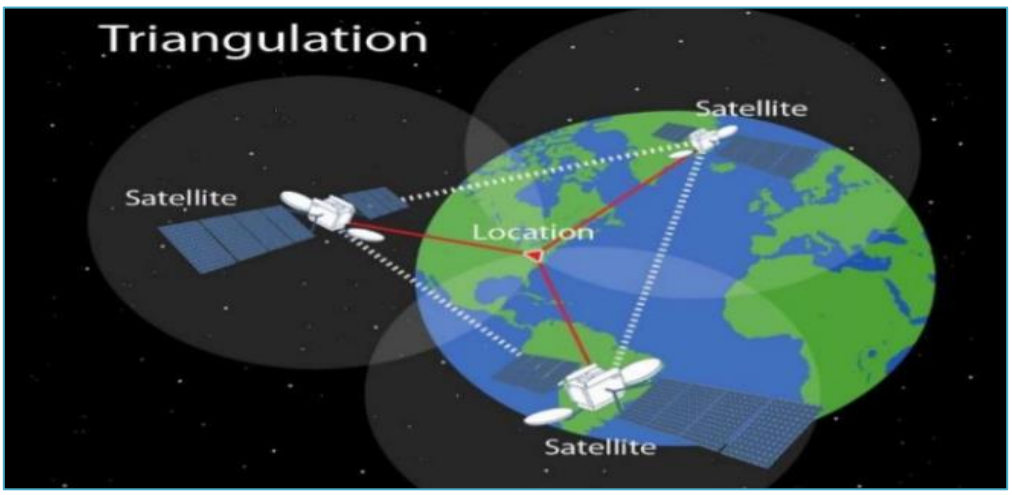


Figure 1 - Illustration of a device receiving signals from at least 3 satellites. Location accuracy can be increased through correlation with more satellites and fixed position GPS beacons on land[7]

[4] http://www8.garmin.com/aboutGPS/
[5] https://en.wikipedia.org/wiki/GPS_tracking_unit
[6] https://www.ordnancesurvey.co.uk/business-and-government/help-and-support/navigation-technology/gps-beginners-guide.html
[7] http://www.slideshare.net/fullscreen/axndj1993/latest-advances-in-gps-technology/10

Satellite positioning units can be categorised into three groups[8]:

- Data Loggers – log the position of the device in an internal memory
- Data Pushers – send data to a computer server at regular intervals
- Data Pullers – operate only when required i.e. they can be pinged to give the current location, but do not provide location data on a regular basis.

"Data loggers" normally rely on the recovery of the device in order to obtain the tracking information and that data is after the fact i.e. not provided real time. "Data pushers" offer the most consistent tracking information providing the ability to plot regular points during the transit of the device. However the regular operation of the device will drain battery life more quickly than "data pullers". Data pullers can be designed to hibernate and only send communications in particular circumstances or conditions. This may be a significant factor (see 2.2 below) if the device is needed to operate for extended periods such as to track waste shipments overseas.

Whilst they are able to operate in cloudy weather conditions a limitation of a satellite positioning receiver in terms of application to covert tracking is the necessity for the receiver to have direct line of sight to the sky. The receiver cannot operate within solid objects or inside buildings and the positioning of an external antenna is a factor to consider in the design and application of the device.

Satellite positioning is likely to continue to improve with co-operation and interoperability between Global Navigation Satellite Systems (GNSS) including American (GPS), European (Galileo), and Russian (GLONASS) systems. Reliance on this technology for accurate navigation and positioning is likely to continue for the foreseeable future. Research on alternative systems appears in the main to be being carried out for military applications that are unlikely to be available to environmental regulators for many years[9].

Mobile telephone tracking (e.g. GSM - Global System for Mobile Communications)

This component allows the device to emit a signal to mobile phone masts and location is determined based on distances between the device and masts at a certain time. Data is stored or communicated back in the same way as a satellite unit, via mobile (for example GPRS - General Packet Radio Service or SMS – Short Message Service), radio, or satellite communications networks.

This system is a less accurate positioning system than that obtained from satellites, but is advantageous in that it does not rely on having direct line of sight to the mobile masts (as GPS needs to the satellites). The device is able to provide approximate location data from inside objects and buildings.

[8] https://en.wikipedia.org/wiki/GPS_tracking_unit
[9] http://www.darpa.mil/news-events/2014-07-24

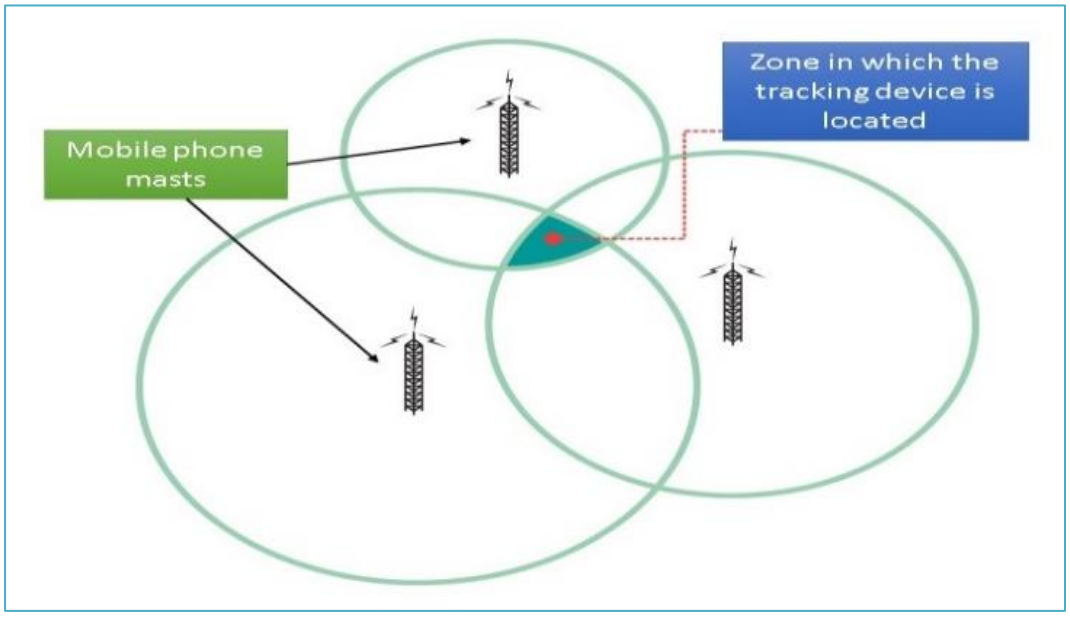


Figure 2 - Adapted diagram illustrating triangulation of mobile phone location[10]

In practice it is perhaps desirable for the device to have the capability of providing location data using both systems operating together. INTERPOL[11] advise that "each method of connectivity has its pros and cons. Law enforcement must ensure that it uses the connectivity option best suited to the specific scenario".

4.1.2 Device Power

The battery is a key component in an electronic tracking device. The type of battery selected should be determined based on the power requirement of the system it supports, intended use and the likely length of service required from the device.

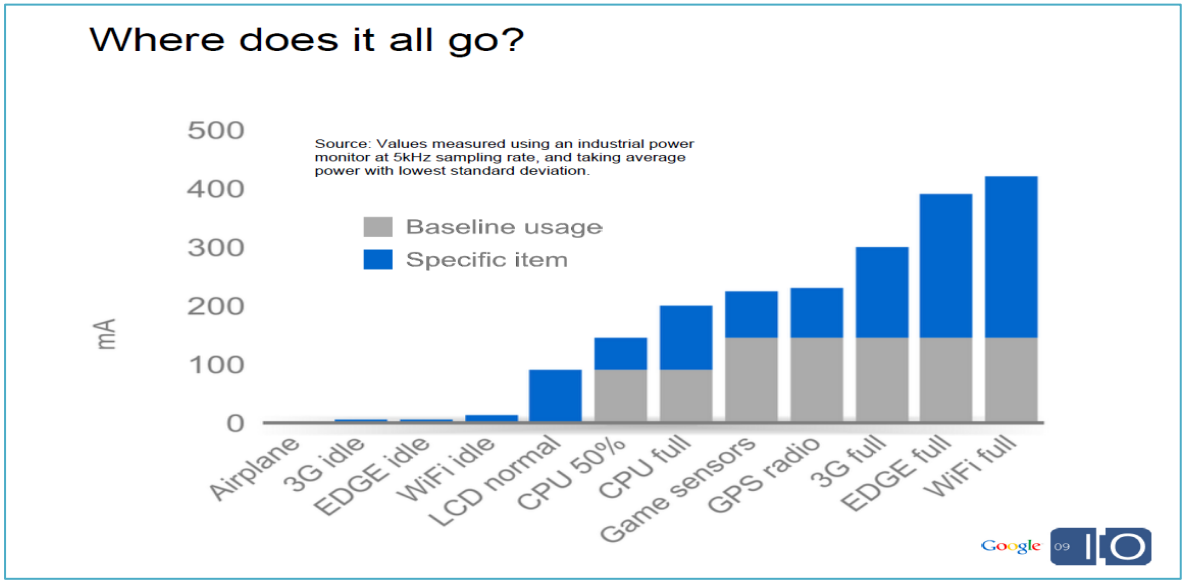
Most commercially available electronic tracking devices appear to operate using rechargeable lithium ion batteries that can operate in a low duty/deep cycle (lower power output and full discharge). Generally lithium ion batteries are advantageous in having better power output to size and weight ratios than other batteries currently available (e.g. lead acid, NiCad etc.).

Battery technology has developed more slowly that other areas and may be a limiting component in the current design of electronic devices. There are significant potential advancements currently in development such as "fuel cell" and solid state batteries which have the potential to be more durable and long lasting than lithium ion. Other advancements including flexible and foldable batteries, wireless recharging using ultrasound and batteries that can be charged by simply adding water are expected within the next few years. In future these developments could significantly alter how electronic devices are constructed and deployed.

However when considering current technology thought needs to be given to how battery life can be preserved as long as possible. A satellite based device transmitting its location continuously is only likely to last a few days.

[10] https://www.safaribooksonline.com/library/view/windows-phone-8/9780133383959/ch17lev2sec2.html
[11] INTERPOL Environmental Security Sub-directorate - "Analysis of Tracking Devices"

Figure 3 - Analysis by Google of effect of mobile phone functions on power usage. The communications functions are likely to be similarly applicable to electronic tracking devices[12]



INTERPOL research[13] states that "the use of each connectivity method can have a great influence on how long the battery will last". A device with an average battery life of days could be made to last months with the correct settings. The key to extending battery life seems to be designing the device to operate mainly in a sleep/hibernation mode with pre-set or sensor activated transmitting periods. The sensor activated approach has been used successfully by regulators in Sweden where devices only became active and sent signals when movement was detected. Conserving power in this way can significantly extend the life of a deployment. INTERPOL[14] suggest the option of adding additional batteries within the tracking device where space allows. Another option that might be considered is the use of solar cells to trickle charge in to the battery. However in practice this may potentially cause difficulties in terms of device concealment and attachment.

4.1.3 Device attachment and concealment

INTERPOL analysis[15] of tracking devices suggests that the physical size of the device is an important consideration.

It is envisaged that for most applications the presence of a tracking device would be concealed from view to avoid accidental or deliberate removal. The method of attachment may vary depending of the waste type being tracked. Some waste types, such as WEEE, may allow the tracking device to be embedded within the waste. Other wastes may allow the use of magnetic attachment, adhesive or tether. The communication mechanism and waste type will also have an effect on if and how the device can be concealed. Concealment can be made easier through encasement in plastic moulds of materials appearing similar to the waste or vessel being tracked.

The most appropriate method of attachment and the concealment of the device are factors to consider when planning deployment.

[12] https://dl.google.com/io/2009/pres/W_0300_CodingforLife-BatteryLifeThatIs.pdf
[13] INTERPOL Environmental Security Sub-directorate - "Analysis of Tracking Devices"
[14] INTERPOL Environmental Security Sub-directorate - "Analysis of Tracking Devices"
[15] INTERPOL Environmental Security Sub-directorate - "Analysis of Tracking Devices"

4.1.4 Geographical information systems (GIS)

The device co-ordinates, whether provided in real-time, via occasional alerts or subsequent to the recovery of the device, will likely need to be geographically plotted. There are a host of software applications that can be employed to display the "results", including free to use programs (freeware), commercial GIS software packages and specialised service arrangements with the device manufacturers which typically charge a monthly subscription fee.

There are issues to consider in terms of security and retention of data, ongoing support and licencing costs when selecting the appropriate package. Where possible utilising the existing "in-house" GIS systems that regulators already operate may be the most secure and cost effective method of recording and displaying the tracks. However this may require the support of GIS experts to implement.

4.1.5 Additional features / considerations

A desirable feature in any device might be the ability to be remotely disable it should it become lost. This is a particular concern if the device has a data logging and download function. For devices that transmit rather than store data, a disabling feature is probably not as much of a concern, particularly where a password or key is needed to activate the device. These considerations should form part of the procurement and planning process and be guided by legal advice. Device survival through transport and treatment should also be considered during planned deployment; while some impact protection and waterproofing is likely to be desirable. Any electronic equipment deployed should comply with the Restriction of the Use of Certain Hazardous Substances (RoHS) in Electrical and Electronic Equipment (EEE) Directive (2011/65/EU).[16]

4.1.6 Costs

A significant likely barrier to deployment will be the difficulty of retrieving the device and the potential for the device to be destroyed during the operation. Costs of replacing devices can cause anxiety and limit the potential for mass deployments as is considered later. Costs for devices readily available can vary significantly but are likely to be over £100 per device.

INTERPOL's research[17] of several devices revealed costings between approximately £250 to over £7000, with devices often coming with additional servicing and operating costs. The devices considered by INTERPOL may reflect the particular operational requirements of that organisation, and may not necessarily be the same as those required in a deployment to a waste stream.

If device development is brought in house or through partnerships then costs might be reduced significantly. Expertise may already exist within European environmental regulators who have expertise creating and maintaining telemetry systems as part of the environmental and flood monitoring network. There is also potential to develop partnerships and pool resources. Regulators in Sweden have reported successfully using cheaper devices, as are those that have been developed by the Basel Action Network. Collaboration with universities might also be a potential source of innovation with a view to research and develop new devices that are applicable to a waste stream approach to deployment.

[16] https://www.gov.uk/guidance/rohs-compliance-and-guidance
[17] INTERPOL Environmental Security Sub-directorate - "Analysis of Tracking Devices"

There is a large array of devices and manufacturers available to the environmental regulator when it comes to the procurement of trackers.

4.2 Short Range Tracking Components and Systems

4.2.1 Short Range Positioning/Location Systems

Short range positioning systems have found more and more applications in recent years such as access control, file tracking, race timing, supply chain management and smart labels. Technologies are fast emerging in this sector that can support asset management across different industries. Currently the most common (other than barcodes) is Radio Frequency Identification (RFID). RFID uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information, which can be thought of as either active or passive.

Passive RFID systems use tags with no internal power source and instead are powered by the electromagnetic energy transmitted from an RFID reader. The tags usually need be within a few meters of a reader in order to activate them, however the low price per tag makes passive RFID systems economical for use in many industries. Active RFID systems use battery powered RFID tags that continuously broadcast their own signal. These tags are commonly used as "beacons" to accurately track the real-time location of assets or in high-speed environments such as tolling. Active tags can be read from a range of up to about 100 meters, but each tag is also much more expensive.[18]

Bluetooth and Wi-Fi are also being used in a similar manner to enable tags or beacons to be read by Smartphones and other common devices which have the advantage of not requiring specific and sometimes costly scanners to be deployed (as is the case with RFID).

[18] http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

5.0 Potential Applications of Tracking Devices for the Waste Sector

5.1 Wide Area Tracking Devices

The proposals below are similar in their application of the technology but offer differences in approach, purpose and use of the data obtained. The proposals are envisaged to be initially small in scale and used to test a concept.

5.1.1 Application as an Intelligence Tool

From the research conducted during the production of this report indications are that electronic tracking devices are generally used in specific and targeted operations to obtain evidence, corroborate intelligence, or to plug intelligence gaps. Deployments normally involve the placement of a handful devices with a clearly defined purpose and anticipated outcome.

There is clearly merit in the deployment of tracking devices for these purposes. Tracking devices can be a far more resource efficient way of obtaining information than, for example, prolonged manned surveillance. However, the experience of some regulators has shown that sometimes elaborate operations are needed both to deploy and retrieve the tracking device. There is also the need to have strong prior intelligence to justify the operation in terms of RIPA/RIP(S)A (Regulation of Investigatory Powers (Scotland) Act 2002). This can mean that significant resources are committed to the planning and preparation of the operation and the envisaged resource savings are not realised, particularly where deployments then fail in some way and perhaps a device is lost that can be costly to replace. These experiences and concerns in terms of the legality of the approach and costs associated with losing a device have developed reluctance by some regulators to make use of the equipment.

Pilot Idea 1

- Consideration is given to the development and piloting of simplified approaches to the deployment of electronic tracking devices to address an intelligence requirement with the aim of testing and understanding practicalities in terms of tracking different waste types, gathering information on device survival and recovery outcomes as a result of deployment to different waste streams.
- A report on the outcome of the pilot exercises is developed as reference guide to covert deployment. The guide could be hosted on the LSW communication hub where it can be updated and amended based on regulator experience across Europe.

5.1.2 Application to test, understand and report Local Authority Waste Flow

Electronic trackers have the potential to provide significant insight in the flow of waste which could help Local Authorities understand and improve their collection systems, identify infrastructure inadequacies or efficiency savings (perhaps even between neighbouring authorities), as well as report and quality assure waste data flow.

An excellent example of how technology can be deployed in this manner is illustrated by the Trash Tracking study carried out by a collaboration involving the Massachusetts Institute of Technology. In the study 2000 objects carrying electronic tracking devices were followed through Seattle's waste management system. The general aim was to determine if trash was going where it was intended to go in terms of authorised facilities (able to accept a particular material) and in accordance with City waste management contracts. The work also sought to understand if there were inefficiencies in the removal system and increase awareness of waste disposal amongst the public.[19]

The approach applied within the study could be used as a blueprint that could be built upon working alongside Local Authorities to deploy tracking systems, particularly within problematic waste streams where we may suspect the recycling and disposal is not taking place as it should or as specified by Local Authority contracts.

Pilot Idea 2

Consideration to be given to the design of a pilot, working with a local authority that would introduce electronic tracking devices to understand waste flow in problematic waste stream. It is envisaged that this deployment would be for information purposes to understand the benefits that can be realised from tracking waste through the system. Potential benefits might be improved collection and more efficient waste handling and processing, better understanding of possible infrastructure issues/deficiencies, evidence to establish the contribution waste trackers can make waste data flow reporting, potential to identify leakage and contract breeches.

5.1.3 Voluntary application by a leading waste industry company

In 2007/08 the Lombardi regional authorities in Italy equipped 200 trucks of companies carrying hazardous wastes with low cost GPS receivers, which automatically transfer in real-time the recorded data from the vehicles to the control centre, via the GSM/GPRS mobile communication network. This permitted the tracking of the vehicles' position and of their itinerary in real time and to immediately detect changes of cargos.

The companies participating in the scheme benefitted from real-time monitoring of their fleet and freight without paying for the service or the equipment. The participants, both Regional Authority and transport companies benefitted by avoiding costs on the processing of waste authorisations (duty of care) required to move the waste. The Regional Authority would immediately detect if illicit waste movements were taking place.

Perhaps through engagement with industry similar approaches could be trialled within the UK that would enhance *e-doc* and support duty of care, reduce red tape on business and provide valuable data on waste movements to the Regulator. Collaboration of this nature may be appealing in the sphere of international waste shipments, where it may be possible to engage shipping brokers to carry devices. A trial of this type may be helpful to brokers by reducing potential liabilities from illicit shipments of waste, and would also foster European collaboration and learning with possible linkages to IMPEL (European Union Network for the Implementation and Enforcement of Environmental Law) objectives.

[19] http://senseable.mit.edu/trashtrack/visualizations.php?id=2

The above mentioned are the beginnings of testing alternative approaches to deployment of electronic tracking devices. They are a move towards more widespread usage that may tell us more about the whole waste system, where it is generated, how it moves and where it is processed. This could be a significant intelligence tool and a means of obtaining the really valuable indicators of emerging waste crime activities before they become significant and obvious (e.g. reported as a complaint). It may lead us to intervene at an early stage to disrupt activities while the collected data may provide waste producers with the awareness and opportunity to change practices and contracts and to move away from the more unscrupulous operators.

Pilot Idea 3

Consideration to be given to the design of a pilot, working with an industry partner to use electronic tracking devices to track waste movements with the aim of understanding the feasibility and extent of any potential benefits to industry and the regulator.

5.2 Short Range Tracking Devices

5.2.1 Potential applications to the Waste Industry

Pilot Idea 4

Consideration to be given to the design of a pilot, working with a shipping broker and other European regulators to deploy electronic tracking devices to track international shipments of waste arising from the UK. The aim would be to understand the movement of a particular waste type through Europe. Possibly in collaboration and in light of intelligence from other European regulators a small scale pilot could be used to test the concept.

The current limitations of this technology are obvious in terms of the restricted distances over which it operates. There is scope for development and with technological advancement it may have greater uses within waste management. When compared with wide area tracking devices, short range systems have some interesting and potentially significant advantages particularly in terms of both size, since tags can be as small as a single grain of rice, and cost, which can be as low as a few pence for a passive transponder.

Clearly short range devices cannot be used in the same way as those designed for wide range tracking but that does not mean that they have no potential applications within waste tracking. The challenge for environmental regulators is to develop effective ways of utilising this technology.

One opportunity might be where they are used in conjunction with the wide area tracking devices. For example where a container carrying waste is tracked using a GPS system we can say that the container arrived in a certain location but not necessarily the waste. Obtaining evidence might be difficult if the waste is, for example, quickly buried, treated or disbursed. However it may be possible to deploy smaller devices within the waste so that it can be detected at a later date even if it has been buried. It may be possible to combine unmanned aircraft (drones) over an area to detect the transponders.

Many industries have already adopted this technology within the supply chain. There might be further opportunities for it to be developed to support the removal process and complete

the circle. Short range technology could potentially be used to automate and enhance duty of care, perhaps involving the automated update of the e-doc system, via smart phone devices as the waste is transferred through the system. This technology could also help increase recycling by demonstrating to the public where their waste is within the waste management system, it could also aid extended producer responsibility and help the management of take back schemes.

There may be significant advantages to manufacturers, retailers, consumers, the waste industry, regulators and Government if this technology was adopted to communicate at key points throughout the life cycle of a product, from manufacture to grave, but would involve the embedding of passive transponders in new products as they are designed and made.

The emerging technologies around pervasive computing could lead to exciting new applications to waste and resources and provide the ability to obtain data which provides information about supply and demand, improve recycling rates and help us understand the quantity of a given recyclate. This could provide a real time picture of the functioning of the circular economy and with that data we would be better placed to identify the demands on natural resources and how they can be sustainably managed in the longer term.

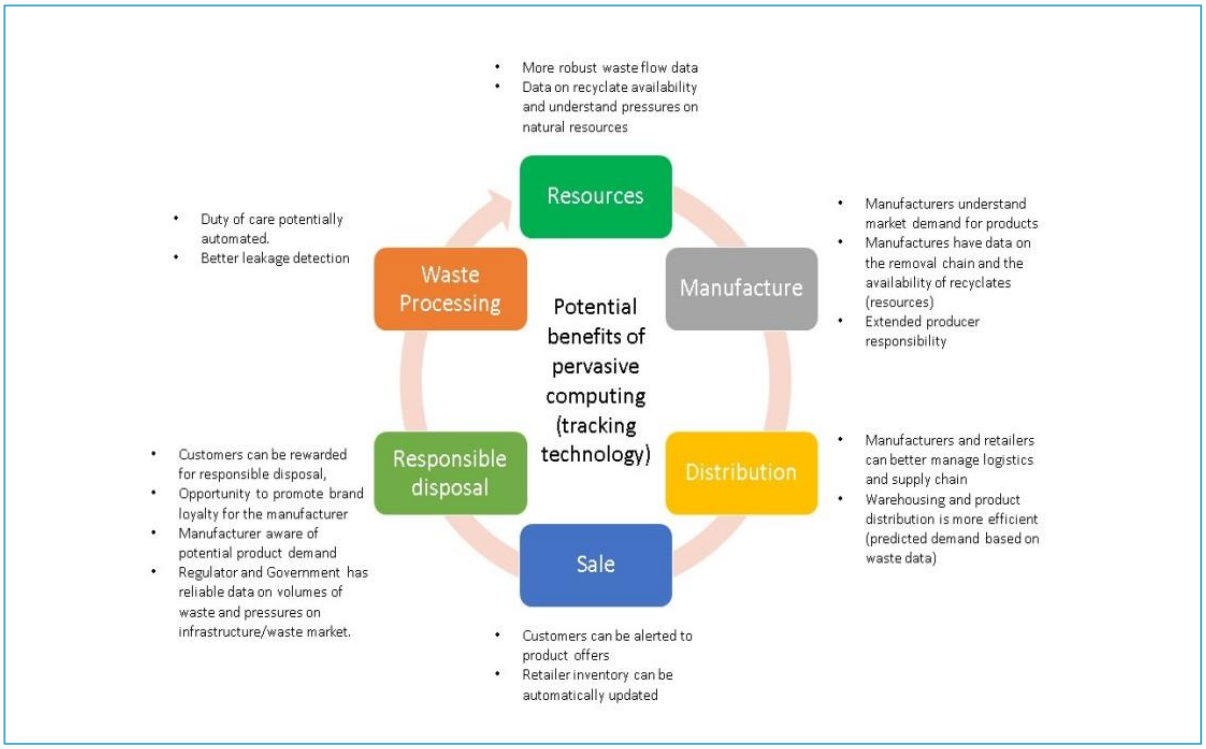


Figure 4 - Potential benefits of pervasive computing, using tracking technology throughout the life cycle of a product

Pilot Idea 5

Consideration is given to a trial of short range tracking technology and its potential as an automated duty of care record. This could involve working with industry, organisations such as WRAP (Waste & Resources Action Programme), and with academics to further understand current supply chain applications of these devices and their potential adaption to the removal chain.

6.0 Pilot Proposal for Live Deployment of Tracking Devices in a Challenging Waste Stream

Following further consideration of the technical specification for LSW Action B7, some of the expectations for the Action need to be developed and tested within the context of a practical deployment of the devices. Some degree of testing and deployment is necessary to be able to evaluate the effectiveness of the technique, and to enable the development of the desired training or guidance product.

A possible pilot could involve the physical deployment of tracking devices within a challenging waste stream. The waste material could be tracked as far as possible from collection, reprocessing and final output.

A “challenging” waste could be selected from the intelligence reports produced under Action B11, possibly where ‘intelligence gaps’ have been identified. There may also be compelling strategic drivers for selecting a particular waste stream, on which Waste Policy Advisors could be consulted. A key component of the approach is that it is the waste stream that would be targeted and not any particular site or operator. The primary purpose will be to improve our understanding of the waste story. Through focusing on understanding waste flow, multiple benefits from deployment might be achieved.

It is envisaged that collaboration would be an important feature of any pilot. Whilst devices might originate in Scotland and Wales, they may cross many borders before they reach their final re-processing or disposal point. The involvement of other UK and European regulators could prove essential. To this end it is anticipated that much planning and design work would take place through the LIFE SMART Waste Hub, which offers the opportunity to bring together expertise in this area to ensure the deployment design can be refined to overcome the risks and realise the outcomes described above. The Hub could also provide the forum where learning can take place and training materials shared as the proposed pilot progresses. The hub could also provide the secure environment in which the results of the pilot can be shared with others, where a living information resource can be created containing methodology and information resources about tracking assets that could become the go to repository for other regulators wishing to carry out this type of activity. A staged approach would be necessary to bring about a successful pilot. An outline pilot plan is presented in Appendix 1.

7.0 Proposal for the Development of a Tracking Device Catalogue Resource

A large number of devices and manufacturers have been identified whilst researching the technology. The B7 LSW project action states that the "team will work to investigate the types of waste tracking devices available and assess their suitability for tracking the movements of different waste types". Given the range and number of devices available on the market to undertake this activity would take an extended period of testing that could last beyond the project itself.

An alternative approach has been adopted that will see a catalogue of tracking devices developed and hosted on the LIFE SMART Hub. The proposed catalogue will contain basic information about the tracking devices that have been identified, including:

- Manufacturer
- Type
- Connectivity / Communications
- Key features
- Description
- Costs (if available)
- Hyperlink to the manufacturer for further information

It is intended that the catalogue is a living resource. The initial list is unlikely to be exhaustive, nor contain full details included about all of the devices that are listed; rather this will be added to over time. Partners using the Hub will add feedback regarding the devices and as things develop this should lead to the identification of the most suitable devices depending on context and objectives of the deployment. The research carried out by INTERPOL may also support this development.

It is possible that should the proposed pilot activity take place and be successful this may trigger a surge of interest in the technique. Should this happen then the Hub will be at the forefront of the development of a one stop resource to identify devices, obtain training materials, understand the legal constraints and view effective tactics on deployment.

8.0 Legal Considerations

As detailed in previous sections of this report, significant research has been conducted into the types of tracking devices available for use by regulators, along with possible deployments and guidance. However, alongside this is the suitability and legal considerations which must be considered. Relevant legal opinion was sought from Harper Macleod LLP (Scotland) and from Apex Chambers (England and Wales). Legal Notes were produced on the use of remote sensing and tracking devices in relation to deployment by environment agencies in Scotland, England and Wales.

The legal advice sets out responses to a range of specific queries and case study scenarios which were provided by SEPA. The legal advice was obtained prior to the implementation of the new European Union General Data Protection Regulation (GDPR) 2018. GDPR contains a wider definition of personal data than the Data Protection Act 1998. Authorities considering deploying tracking devices may wish to seek further legal counsel with regards to the implications of GDPR. The full details of the Harper Macleod Legal Note can be found in Appendix 2 of this report.

The salient points from this legal advice are as follows:

- The use of tracking devices by environment agencies may give rise to the processing of personal data under the Data Protection Act 1998, particularly where information relating to the geographical location of waste is combined with publicly available information associated with the owner or resident of a domestic property.

- In processing personal data, environment agencies must comply with the data protection principles contained in the Data Protection Act 1998, particularly the requirement to notify individuals who are identifiable from the use of tracking devices, unless an exemption applies.

- A relevant exemption in the present case is the exemption for personal data processed for the purposes of the prevention or detection of crime, which would allow environment agencies to collect and use personal data identifying individuals without informing them, provided that the personal data is used for law enforcement functions.

- RIPA/RIP(S)A 2000 applies when using tracking devices to collect private information about individuals' private or family life through covert surveillance. The form of surveillance envisaged (using tracking devices) is likely to constitute "directed surveillance" under RIPA/RIP(S)A 2000.

- Directed surveillance by environment agencies can be justified in one of the following three ways: (1) Environment agencies can self-authorise its directed surveillance under RIPA/RIP(S)A 2000; (2) Environment agencies can rely on a Data Protection Act 1998 exception, which allows the processing of personal data for prevention or detection of crime purposes; or (3) Environment agencies can rely on a RIPA/RIP(S)A 2000 exception, which allows for directed surveillance undertaken in pursuit of their general observational duties.

- There is a risk that the deployment of tracking devices by environment agencies may interfere with the right to respect for family life, home and correspondence enshrined in Article 8 of the European Convention on Human Rights. Environment agencies should undertake a human rights impact assessment to assess if the use of such devices is proportionate.

- Environment agencies need a legal basis if they require organisations to deploy tracking devices in produced waste. Environment agencies would be responsible for legal compliance as instigator of the deployment. We are satisfied that environment agencies have a number of legal bases for doing so under the Data Protection Act 1998 and / or RIPA/RIP(S)A 2000, all as noted above.

- There are data security risks if the tracking devices are intercepted by third parties. Environment agencies must take steps to ensure that the personal data is secure and that it can remotely disable the devices and technologies in the event of interception.

- The use of tracking devices may also involve intrusion on and interference with private property in terms of the Police Act 1997 and environment agencies may be required to liaise with the Police for the purposes of obtaining an authorisation.

In summary, according to legal advice, environment agencies within the UK (specifically England, Scotland and Wales) are not precluded from using tracking devices lawfully under certain circumstances, to assist in specific criminal investigations. This is also the view held by the expert knowledge group, consisting of representatives from the four UK environment agencies, who engaged in a consultation meeting on behalf of the LSW Project to explore this Action.

9.0 Expert Knowledge and Practical Advice

In order to progress this Action, in conjunction with the legal advice and guidance sought by the LSW team, it was considered prudent to seek further advice and guidance from expert individuals with experience (either law enforcement or environmental regulation) in the use of tracking devices for criminal investigations. Accordingly, a meeting of such experts from the four UK Environment Agencies (some of whom were ex-law enforcement personnel) was convened to discuss a potential pilot for the deployment of electronic tracking devices and make recommendations for consideration.

As stated in the previous section of this report, the expert group are of the opinion that UK Agencies can lawfully use tracking devices in certain circumstances to assist in specific criminal investigations. However, a deployment would need to be based on current and reliable intelligence and authorised under a RIP(S)A / RIPA (2000) directed surveillance authorisation.

The expert group fully considered the realistic opportunities for deployment and do not believe suitable opportunities or intelligence would allow such a deployment to currently be piloted. When other limitations within which the Agencies operate are considered, the opportunities continue to narrow significantly:

- Environmental Agencies are not named in the Police Act 1997 and cannot lawfully interfere with property. This hampers Agencies in terms of how they might conceal and later recover a tracking device. Limitations on powers to enter land are also a factor in the feasibility of deployment, maintenance and recovery of any device.

- The intelligence gathering capabilities of Agencies are limited. Agencies frequently do not or cannot operate Covert Human Intelligence Sources and are unable to access more intrusive sources of intelligence under part 1 RIPA. Therefore, developing the sort of intelligence picture that supports deployment is challenging.

- The activity is resource intensive requiring teams who have the relevant training and expertise in this field to deploy, maintain, recover and manage such deployments.

Agencies may seek to deploy tracking devices in collaboration with the Police, however, the following points would have to be considered:

- Authorising this activity would have to be by means of making an application to a Police authorising officer after a full feasibility and risk assessment is conducted by trained staff.

- Careful management by trained police staff would be required at all stages.

- Protocols for operational and data management would also need to be established.

The covert use of a tracking device is a high-end policing tactic. Deployment must be proportionate and necessary to the targeted investigation, supported by current reliable intelligence. It is currently used by Policing Agencies when other tactics have been explored or would be likely to fail.

10.0 What Needs to Change

RIPA, RIP(S)A and Part 3 Police Act 1997 are subject/target specific and do not address the challenge that environment agencies have which is, a requirement to track and monitor waste streams on a national and international basis across the European Member States and beyond.

11.0 Recommendations

- It is recommended that the LSW Project do not pursue a pilot of tracking devices. Alternatively, policy recommendations are proposed and outlined below.

The following recommendations are considered to be short term:

- The findings and recommendations of this report are shared with the UK Government and environment agencies discovery project, which is scoping a UK waste tracking service, to inform the discussion on whether UK environmental regulators should be given powers, detailed within Part 3 of the Police Act 1997, that would enable feasible waste tracking device deployment.

- The LSW Project Team engage with the Guardia Seprona in Spain and disseminate findings of this report to assist in the Spanish-led action plan under the environmental and wildlife crime EMPACT, which is evaluating and proposing the use of advanced tools such as tracking devices to increase the reaction capability and support investigations in the field of environmental crime.

- Since 2000 the way waste is managed has changed significantly. European Directives have increased the volume of waste handled above ground and recycled. This has also led to new opportunities for criminals to prosper in the waste industry. There is a requirement to re-visit environmental legislation and produce a new up-to-date Act that accurately reflects the environmental threat currently facing the UK and European Union from illegal movements of waste and infiltration by serious and organised crime groups.

In the longer-term, it is recommended that:

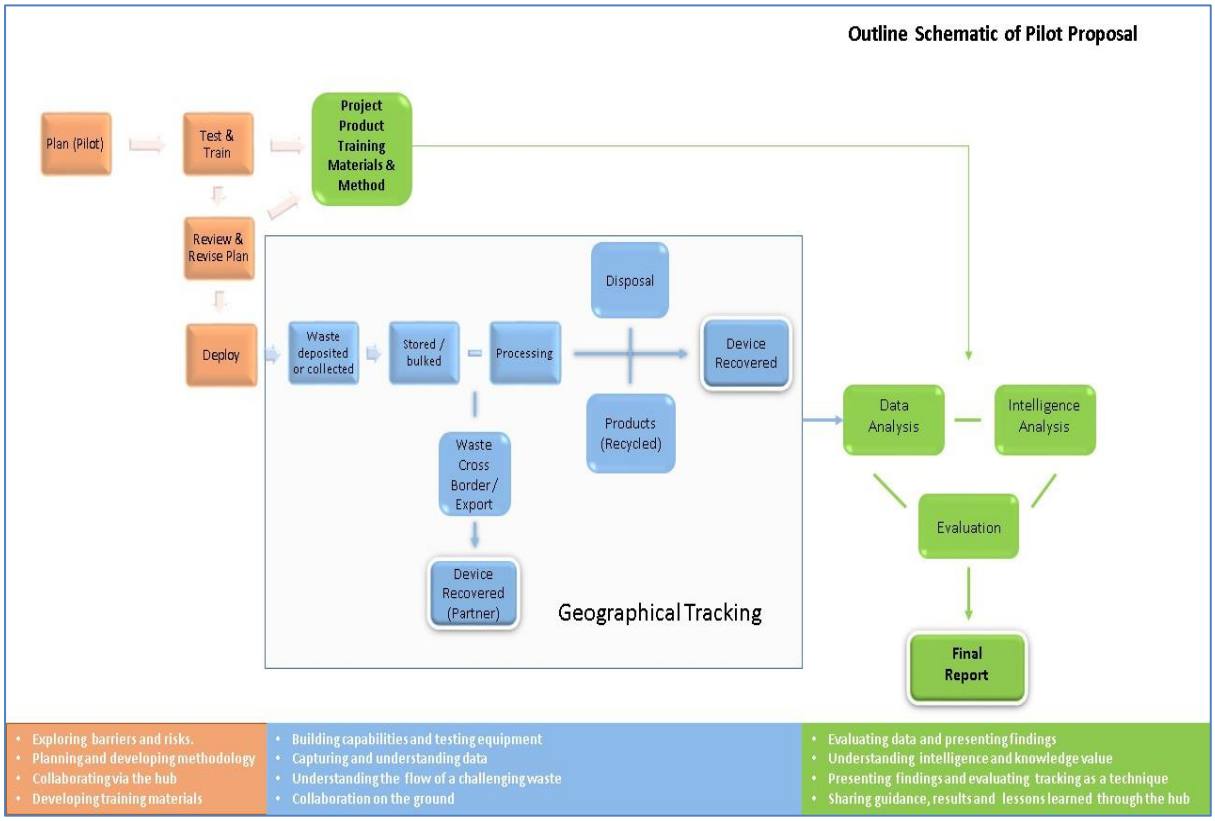
- Consideration is given to expanding the legislative powers of EU Environmental Agencies to monitor the flow of waste using electronic tracking and other techniques.

Annex I - Proposed steps and activities to pilot tracking devices on a challenging waste stream

Plan Stage	Tasks	Aims/Outcomes	Timescales
1. Pilot Outline	• Development of a Wiki on the Hub in order to enable a collaborative creation process to develop an outline proposal for a pilot scheme for the deployment of tracking devices. • Write up of the outline proposal and integration in to the B.7 Final Report.	• Outline proposal presented to the Project Board for consideration, along with background paper associated with B.7 action	
2. Feasibility and detailed assessment	The Life Smart Hub will be the primary forum for the design and development of the detailed pilot plan. Activities will include: • Discussion and evaluation of proposals with RIP(S)/RIPA experts, including submissions to Surveillance and Information Commissioners Offices. • Discussions/Collaboration with tracking industry and/or experienced law enforcement colleagues in terms of devices, techniques and training. • Discussions with other law enforcement agencies with particular regard to reputational and compromise risks. • Discussions surrounding intelligence and the selection of a suitable, “challenging” waste stream to be targeted.	• Identification and testing of legal and technical barriers to the use of tracking devices	
3. Procurement	• Undertake procurement of tracking devices and training for designated SEPA/NRW Officers	• Obtain necessary external support and equipment	

Plan Stage	Tasks	Aims/Outcomes	Timescales
4. Training and Safe (Test) Deployment	• Hold training session(s) for relevant staff. • Produce guidance / training materials • Test equipment in a safe environment. • Update the tracking information resource on the Hub with findings (e.g. what works, what doesn't)	• Up-skill staff • Meet B.7 project objective of developing a training / guidance package. • Assess equipment and test feasibility	
5. Plan live deployment	• Use the Hub to develop detailed operational plan for live deployment • Review planned deployment based on test outcomes • Engage with partners using the hub as the preferred forum / communications route	• To ensure a clear workable methodology is in place, along with risk assessments, communications and retrieval plans.	
6. Deployment	• Environmental Agencies (SEPA/NRW) with 3rd party support deploy tracking devices in "challenging waste type", via a handful of non-targeted receptor sites or through waste collectors depending on the waste type selected • The tracks of each device are recorded for more detailed analysis • Final destination of waste and tracking devices is identified, and device recovery procedures are implemented	• To test the application of the technology • To understand if tracking devices can be used as a new capability to track the flow of a challenging waste stream. • To record the methodology and results for the benefit of other European Regulators	
7. Evaluation of results	• Assessment of the legality of processing points and end destinations of the waste • Evaluate the quality of data received • Evaluate the "intelligence" value of the results • Publish initial findings on the Hub to share results with partners and facilitate peer evaluation/review	• Potential increase in understanding of the flow of a challenging waste • Potential new intelligence source regarding leakage • Increase in understanding of the effectiveness of the technology as tool for Environmental Regulators	

Plan Stage	Tasks	Aims/Outcomes	Timescales
8. Presentation of findings / final report	• Write-up of report and key findings • Creation of a presentation video displaying the methodology and results obtained hosted as an information accessible to other regulators via the Hub	• Key findings are reported and products shared with European Environmental Regulators • To fully meet objects of Action B.7	



Annex II - Legal note on the use of Remote Sensing and tracking devices

Author: Harper MacLeod LLP

Introduction

We understand that SEPA intends to appoint a contractor to deploy tracking devices and remote sensing technology on its behalf as part of its "LIFE SMART Waste Project" for the purposes of gathering intelligence data on illegal activities associated with waste depositing. The tracking devices and remote sensing technology will track waste movements through the supply chain with a view to understanding the genesis of waste and its destination, and if waste streams are being illegally diverted during this process.

This note sets out our advice in response to a range of specific queries raised by SEPA in relation to the key legal issues presented by the "LIFE SMART Waste Project".

We would be happy to provide more detailed advice on any aspect of this note and to develop the case studies once SEPA has reached a final decision as to the precise nature of the tracking devices and remote sensing technologies to be deployed.

Executive Summary

- The use of tracking devices by SEPA may give rise to the processing of personal data under the Data Protection Act 1998, particularly where information relating to the geographical location of waste is combined with publicly available information associated with the owner or resident of a domestic property.
- Deploying remote sensing technologies in the form of drones could give rise to the processing of personal data in terms of the Data Protection Act 1998 where the quality of the captured footage is high and the drones are operating on a continuous basis and not subject to triggers.
- RADAR and LIDAR technologies, given their limitations, are unlikely to give rise to the processing of personal data in terms of the Data Protection Act 1998.
- In processing personal data, SEPA must comply with the data protection principles contained in the Data Protection Act 1998, particularly the requirement to notify individuals who are identifiable from the use of tracking devices or remote sensing technologies, unless an exemption applies.
- A relevant exemption in the present case is the exemption for personal data processed for the purposes of the prevention or detection of crime, which would allow SEPA to collect and use personal data identifying individuals without informing them, provided that the personal data is used for SEPA's law enforcement functions.
- The Regulation of Investigatory Powers (Scotland) Act 2000 applies when using tracking devices and remote sensing technologies to collect private information about individuals' private or family life through covert surveillance. The form of surveillance envisaged by SEPA is likely to constitute "directed surveillance" under the Regulation of Investigatory Powers (Scotland) Act 2000.

- Directed surveillance by SEPA can be justified in one of the following three ways: (1) SEPA can self-authorise its directed surveillance under the Regulation of Investigatory Powers (Scotland) Act 2000; (2) SEPA can rely on a Data Protection Act 1998 exception, which allows SEPA to process personal data for prevention or detection of crime purposes; or (3) SEPA can rely on a Regulation of Investigatory Powers (Scotland) Act 2000 exception, which allows for directed surveillance undertaken in pursuit of SEPA's general observational duties.

- There is a risk that the deployment of tracking devices and remote sensing technologies by SEPA may interfere with the right to respect for family life, home and correspondence enshrined in Article 8 of the European Convention on Human Rights. SEPA should undertake a human rights impact assessment to assess if the use of such devices and technologies is proportionate.

- SEPA needs a legal basis if it requires organisations to deploy tracking devices in produced waste, and SEPA would be responsible for legal compliance as instigator of the deployment. We are satisfied that SEPA has a number of legal bases for doing so under the Data Protection Act 1998 and / or Regulation of Investigatory Powers (Scotland) Act 2000, all as noted above.

- There are data security risks if the tracking devices and remote sensing technologies are intercepted by third parties. SEPA must take steps to ensure that the personal data is secure and that it can remotely disable the devices and technologies in the event of interception.

- The use of tracking devices and remote sensing technologies may also involve intrusion on and interference with private property in terms of the Police Act 1997 and SEPA may be required to liaise with the Police for the purposes of obtaining an authorisation.

- The new European Union General Data Protection Regulation contains a wider definition of personal data than the Data Protection Act 1998, as a consequence of which it is likely that location data in isolation will be sufficient to constitute personal data. SEPA would therefore be required to comply with the requirements of the Regulation in deploying tracking devices and remote sensing technologies. The Regulation comes into force in 2018.

1. What does the law say about the use of tracking devices and remote sensing generally by public sector agencies?

The key issue is whether the tracking devices and remote sensing technology collect information relating to individuals. If they do then the following legislation must be considered:

- Data Protection Act 1998 (the "**DPA**");
- Human Rights Act 1998 (the "**HRA**");
- Regulation of Investigatory Powers (Scotland) Act 2000 ("**RIPSA**");
- Regulation of Investigatory Powers Act 2000 ("**RIPA**"); and
- Part III of the Police Act 1997 ("**PA**").

Reference has been made to the above legislation within the responses to the questions below.

2. What does the law say about the use of tracking devices and remote sensing by environmental authorities to trace waste movements?

As noted in response to Question 1 above, the legality of the use of tracking devices and remote sensing technologies by environmental authorities depends principally upon the extent to which the devices and technologies collect and process information which is capable of identifying specific individuals.

We understand that the activities which SEPA is considering include, without limitation, the use of tracking devices attached to waste products to assist in the tracking of waste within the waste stream. While the primary purpose of the tracking devices is not to collect information capable of identifying specific individuals, we consider that individuals may be identified or may be capable of being identified from the tracking information and other information which may be available to SEPA. In determining what is available to SEPA, it is irrelevant if SEPA is in actual possession or may come into possession of the information that allows it to make that link. The linking information may derive from, for example, the waste disposal company's records, proprietor information available from the Land Register (where the tracking device was attached to a waste product emanating from particular domestic property) or the address of the domestic property at which commercial vehicles containing waste are stored overnight before the waste is transported to its ultimate destination.

Similarly, the capability of the remote sensing technologies to identify specific individuals depends principally upon the format which such technologies assume.

If the remote sensing technology assumes the form of a drone, for example, which captures photographic or video footage of the ground below, either on a continuous basis or upon detection of heat signals or other triggers, then a number of factors are relevant in determining whether the captured footage is capable of identifying specific individuals. First, the quality of the captured photographs or footage is paramount. If the quality is not particularly high, this then reduces the likelihood of individuals being capable of identification within captured photographs or footage.

Secondly, similar considerations are relevant with regard to the height at which the drone operates. The higher the flight height, the less likely individuals will be capable of being readily identified, although this is, again, subject to the quality of the footage (higher quality footage captured from a height could be "zoomed into" without significant loss of quality and individuals may be identified from the "zoomed in" footage).

Thirdly, if the operation of the drone is not automatic and continuous but is subject to certain triggers then the principal focus of the captured footage is, in our view, the trigger event and not individuals who may be captured within the footage on an incidental basis.

If the technology makes use of RADAR and / or LIDAR technologies, based on our understanding of such technologies, we do not consider that the capture of topographical features using such methods would give rise to the identification of individuals at the point of capture. If, however, the captured output was subsequently analysed and it was possible to create a link between a particular waste stream entering the waste management infrastructure and a domestic property then this could give rise to information that is capable of identifying specific individuals e.g. the owner of the property as listed in the Land Register.

In relation to the specific legislation which SEPA will need to consider when undertaking waste tracking or remote sensing activities, the key legislative provisions are as follows:

DPA

This section of our advice note considers whether data captured by tracking devices and remote sensing technologies (other than LIDAR or RADAR) constitutes personal data for the purposes of the DPA.

The DPA defines personal data as data which relates to a living individual who can be identified: (a) from that data; or (b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

(A) Data identifying an individual

The first part of the test requires that it must be possible for a living individual to be identified from the data or from that data and other information in the possession of, or likely to come into the possession of, the data controller. The ability of an individual to be identified relates to the extent to which it is possible to distinguish that individual from other members of a group. An individual can be distinguished from others using direct or indirect identifiers. Name is the only direct identifier with all other identifiers, including address, being indirect identifiers. One or more indirect identifiers can render data identifiable in the absence of a name.

In circumstances where it is not immediately obvious whether an individual can be identified from data, all of the means reasonably likely to be used, either by the data controller or a third party to whom the data may be disclosed, to identify the individual should be taken into account in determining if an individual can be identified. The means reasonably likely to be used will depend on the state of the art at a given time and if such means are readily available. The available means include not only those which an ordinary individual would utilise but also what a determined individual, who may wish to identify individuals for a particular purpose, would consult.

In our opinion, geographic data relating to the location or movement of environmental waste may be personal data for the purposes of the first part of the statutory definition of "personal data" contained within the DPA for the reason that this data may be capable of distinguishing one individual from another. The likelihood of identification increases when account is taken of all of the means available to assist in identification. In the present state of art, it is possible to crosscheck geographic data against a public register, such as the Land Register or the electoral register, or undertake a Google search to distinguish one address from another and identify individual proprietors or residents of a property. This is consistent with the Information Tribunal's (as it then was) decision in Mr Colin P England, London Borough of Bexley and the Information Commissioner, where the tribunal noted that if a property address is known, it is possible to obtain access to owner or resident information by other means, such as land registers, speaking with neighbours and carrying out Google searches. As the Tribunal noted at pp.32-3 of its decision that: "the Tribunal finds that knowing the address of a property makes it likely that the identity of the owner will be found…The address alone, in our view…amounts to personal data because of the likelihood of the identification of the owner".

(B) Data relating to an individual

The second part of the personal data test contained in the DPA requires that the data relates to a living individual. Data relates to a living individual if:

- it is obviously about an individual;
- the data can be linked to an individual and thereby provides particular information about that individual;
- the data is to be used to make, or influence the making of, decisions affecting the individual; or
- The use of the data is likely to have an impact on an individual's rights and interests.

Geographic data relating to the location or movement of environmental waste is, in our view, personal data relating to individuals for the purposes of the second personal data test contained in the DPA. While this data is not obviously about an individual on the face of it, means are readily available allowing for a connection to be made between the geographic data and the resident or owner of a property (as per the first part of the DPA personal data). This is more likely to be the case with regard to domestic property, where it is possible to readily identify the individual proprietor(s) of property from publicly available information, although similar considerations apply to commercial premises of sole proprietor businesses where the geographic data can be related back to a specific individual.

(C) Practical application of the DPA personal data tests

In Durant v The Financial Services Authority, the English Court of Appeal determined that data is likely to be – but is not conclusively – personal data if it (broadly):

- is of biographical significance in relation to an individual i.e. the data goes beyond recording the individual's involvement in a matter and affects the individual by, for example, assisting in determining the location of the individual at a particular time; or
- Focuses upon the individual instead of another individual, transaction or event.

The tests contained in the Durant decision were regarded as narrowing the meaning of personal data, as the data had to affect an individual's privacy and focus on an individual before it would constitute that individual's personal data. This gave rise to particular difficulties in practice. For example, a communication addressed to an individual would not constitute the recipient's personal data unless the communication also concerned the recipient. This resulted in the Information Commissioner's Office ("**ICO**") confining the applicability of the Durant decision to those situations where personal data is not obviously about or linked to an individual i.e. those situations where the application of the two parts to the DPA personal data test do not readily relate to or identify the data to an individual.

The English Court of Appeal in the recent case of Efifiom Edem v Information Commissioner noted that the tests contained in the Durant decision only apply where the data is not obviously about an individual or otherwise linked to an individual and therefore endorsed the ICO's approach. In our view, this establishes the ICO's approach as the dominant test for determining whether data is personal data for the purposes of the DPA.

In the further recent case of R (Kelway) v The Upper Tribunal (Administrative Appeals Chamber) and Northumbria Police, the English High Court confined the Durant decision to the most complex of cases where the ICO approach did not readily provide a solution.

The above overview of recent case law supports the view that personal data is once again being accorded a broad interpretation by the courts. There appears to be a gradual shift away from the tests contained in the Durant decision towards the ICO's approach, which is based on the application of the two part DPA test. Following on from this, we consider that, depending on the nature of and manner in which the tracking devices and remote sensing technologies will operate (other than LIDAR and RADAR), it is possible for geographic data relating to the location of environmental waste to constitute personal data for the purposes of the DPA insofar as it is capable of relating to and identifying individuals.

(D) Data protection principles

SEPA must therefore comply with the requirements of the DPA, namely the data protection principles, unless an exemption from some or all of the DPA requirements is available. The first data protection principle is the most relevant for present purposes. This requires personal data to be processed fairly and lawfully. In processing personal data fairly, regard must be had to the manner in which personal data is obtained or collected. Fairness relates to transparency and an organisation informing individuals from whom personal data is collected of:

- the identity of the organisation processing the personal data;
- the purposes for which the organisation will use that personal data; and
- any other information that is necessary to ensure fairness, including, for example, informing the individuals of any direct marketing that the organisation will undertake, the identities of any third parties to whom the personal data will be disclosed and whether it is intended to transfer the personal data to a country outwith the European Economic Area that does not provide the same levels of data protection as the EU.

Best practice dictates that this information is provided in the form of a "data protection statement" or "fair processing notice" that an individual has sight of at the point of personal

data capture. This can be problematic in the case of drones, particularly if individuals are captured in footage without their knowledge and / or consent.

The ICO has issued a Code of Practice on Surveillance Cameras and Personal Information in which the ICO has provided guidance on complying with the DPA's fair processing requirements in the context of the use of drones. The Code applies in the event that SEPA wishes to make use of drones on an overt – rather than covert – basis. The Code provides that drone operators must wear high visibility clothing to ensure that they are identifiable and that clear and prominent signage must also be placed in the area in which drones are operating notifying individuals of the purposes for which drones are in operation, that SEPA is responsible for their operation and SEPA's contact details. Supplementary fair processing information can be provided by means of website notice and / or social media communications.

Similar considerations apply in the case of tracking devices. The individuals whose geographic movements are being tracked by such devices on an incidental basis during the overt tracking of waste movements must be made aware of the potential for the capture and processing of their personal data from a DPA fair processing point of view. SEPA's responsibility for providing this information and complying with this requirement depends principally upon whether SEPA has a direct relationship with the individual subject to the tracking (for example, where the tracking device has been installed by SEPA with the consent of the individual) or whether SEPA has required an employer organisation to install tracking devices on SEPA's behalf to monitor, for example, the movements of its vehicles carrying waste (which may give rise to the processing of personal data relating to the individual drivers of the vehicles, as outlined above). While SEPA is responsible for complying with the DPA's fair processing requirements in both situations, SEPA could place the responsibility for compliance on the employer organisation in the second situation in terms of the contractual arrangements that it enters into with the employer organisation. The requirement for SEPA to enter into a written agreement with the employer organisation is considered further under Question 8 below.

Lawful processing concerns the overall lawfulness of the processing from the point of view of compliance with common law and statutory legal requirements.

There are partial exemptions contained within the DPA from the requirement to process personal data fairly. We understand that SEPA intends to use tracking devices and remote sensing technologies for a number of purposes, including the detection of illegal waste diversion and to take action in response to such activity by means of reliance on its statutory powers.

We consider that the DPA exemption relating to personal data processed for the purposes of the prevention or detection of crime is the most relevant for present purposes. This exemption permits SEPA to process personal data for the purposes of the prevention and detection of crime without having to comply with the fair and lawful processing elements of the first data protection principle where to comply with these requirements would be likely to prejudice those purposes.

In our view, SEPA could rely on the prevention or detection of crime exemption and make use of tracking devices and remote sensing technologies on a covert basis without having to comply with the fair and lawful processing requirements of the DPA, provided that SEPA does not use the collected personal data for purposes other than the prevention or detection of crime. If SEPA was to use the collected personal data for any other purpose than the

prevention or detection of crime, the benefit of the exemption would not be available and SEPA would be required to comply with the entirety of the DPA, including the fair and lawful processing requirements.

RIPSA

RIPSA is also relevant to the use of tracking devices and sensing technologies where they will result in obtaining private information about a person's private or family life through covert surveillance undertaken in Scotland. Covert surveillance for RIPSA purposes includes any activity involving monitoring or observing persons, their movements or their other activities or communications or recording anything being so monitored or observed, including surveillance via the use of a monitoring device, if the individuals who are subject to the surveillance (irrespective of whether the surveillance is directed to that specific individual) are not aware of the fact that it is taking place. RIPSA does not apply where the covert surveillance is unlikely to result in the obtaining of private information about a person.

In our view, "private information" under RIPSA is wider than the definition of "personal data" under the DPA. This is because "private information" includes information relating to an individual's family life, which, on a literal interpretation, could extend to information relating to other members of the individual's family. In other words, "private information" has the scope to cover both personal data and third party personal data. "Personal data" in terms of the DPA is therefore a subset of "private information" for the purposes of RIPSA. The covert collection and processing of personal data will accordingly give rise to interaction with RIPSA.

In light of the above analysis of the DPA issues, the use of tracking devices and remote sensing technologies to track waste movements has the potential to give rise to the processing of personal data for the purposes of the DPA, particularly since it involves the collection of information relating to identifiable individuals and because it assists in tracking the geographic movements of individuals. For these reasons, in our view, it is likely that the use of such devices and technologies by SEPA, where they are deployed without the knowledge of the individuals, would constitute covert surveillance for the purposes of RIPSA.

RIPSA provides that an authorisation to carry out surveillance is not required where a public authority has another legal basis to undertake the covert surveillance that gives rise to private information. This would apply if SEPA was to rely on the DPA prevention or detection of crime exemption as its legal basis to justify the covert surveillance, as outlined in our response to Question 2.

The Scottish Government's Code of Practice on "Covert Surveillance and Property Interference", which is issued pursuant to RIPSA, is admissible as evidence in civil or criminal proceedings and with which organisations undertaking surveillance activities must comply, provides that authorisation under RIPSA is not required where the surveillance is undertaken pursuant to the general observational duties of a public authority in furtherance of its statutory powers. SEPA's general functions and duties are set out within SEPA's founding statute, the Environment Act 1995 (the "**EA**"). Section 20A of the EA provides that the general purpose of SEPA is to carry out the functions conferred on it by or under the EA or any other statute for the purposes of protecting the environment, including managing natural resources in a sustainable way. Section 33A of the EA sets out the general duties of SEPA with regard to the state of the environment and the effects of pollution, and provides

that SEPA may, for the purposes of carrying out its functions or enabling it to form an opinion on the general state of the environment, compile information on the general state of the environment, whether this information is acquired by SEPA when carrying out its obligations or is obtained in any other way. In our view, the proposed deployment of tracking devices and remote sensing technologies by SEPA accords with SEPA's statutory functions to protect the environment (by detecting and reducing the incidence of illegal diversion of waste) and also SEPA's general observational duties in compiling information on the general state of the environment. On this basis, we consider that SEPA does not require an authorisation under RIPSA for any surveillance that arises from the deployment of tracking devices and remote sensing technologies, provided that such deployment is limited to purposes which are related to SEPA's relevant statutory functions and duties.

RIPSA sets out an authorisation framework for covert surveillance consisting of either:

- intrusive surveillance, which takes place on residential premises or in a private vehicle and involves the presence of an individual in the residential premises or in the private vehicle or the use of a surveillance device placed outside the premises or the vehicle that provides information of the same quality as a device placed inside; or

- Directed surveillance, which is not intrusive but is carried out in relation to a specific investigation or operation and is likely to give rise to private information about any person, irrespective of whether this is the person at whom the investigation is directed.

For the purposes of directed surveillance, private information includes any information relating to a person's private or family life and professional or business relationships and may include personal data, such as names or address details.

RIPSA provides that authorisations to undertake directed surveillance must only be granted by those persons holding such offices, ranks or positions within "relevant public authorities" as may be prescribed by the Scottish Ministers. SEPA is a relevant public authority for this purpose and the persons designated within SEPA to grant authorisations are the chief executive, executive director or the chief officer. In effect, this means that SEPA may "self-authorise" the undertaking of its own directed surveillance activities.

Authorisations for intrusive surveillance may be granted by Chief Constable of the Police Service or the Police Investigations and Review Commissioner and may only be granted if the person granting the authorisation is satisfied that:

- the authorisation is necessary for the purpose of preventing or detecting serious crime; and

- The authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

A "serious crime" is:

- a crime involving the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or

- the offence is one for which a person who is at least 21 years of age and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.

In considering whether the authorised surveillance is proportionate, regard is to be had to whether the information to be obtained by the surveillance could reasonably be obtained by other means.

A single authorisation may cover both directed and intrusive surveillance, but the different statutory tests relevant to each form of surveillance (outlined above) must be considered separately.

In our view, the use of tracking devices and remote sensing technologies is likely to fall within the scope of directed surveillance on the basis that the devices and technologies are being deployed for the purposes of SEPA's crime detection and prevention investigations. We consider that SEPA will not require an intrusive surveillance authorisation on the basis that its investigations will be directed towards illegal waste flows generally and are not intended to be restricted to serious crime.

We are happy to provide more detailed advice in relation to the authorisation process, if required.

If the surveillance mainly takes place or is intended to commence outwith Scotland then SEPA must comply with RIPA, which contains similar provisions to RIPSA with regard to surveillance.

It is clear from the above analysis that SEPA has three alternative grounds on which it could potentially justify the deployment of tracking devices and remote sensing technologies:

- the covert processing of personal data arising from the deployment is necessary for the prevention or detection of crime and is therefore exempt from the fair and lawful processing requirements of the DPA;
- the directed surveillance associated with the deployment is undertaken pursuant to SEPA's general observational duties in furtherance of its statutory powers and an authorisation under RIPSA is not required; or
- SEPA obtains an authorisation from its designated person to undertake the directed surveillance that forms part of the deployment.

In granting an authorisation, SEPA's designated person must be satisfied from a proportionality and necessity point of view, namely that:

- the authorisation is necessary: (i) for the purposes of preventing or detecting crime or preventing disorder; (ii) in the interests of public safety; or (iii) for the purpose of protecting public health; and
- The authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

The designated person must balance the seriousness of the intrusion against the need for the surveillance from an investigatory point of view. The surveillance to be undertaken must be proportionate and must assume the least intrusive form available relative to the gravity of the conduct being investigated.

In our view, it may be prudent for SEPA to combine the three alternatives set out above and self-authorise the directed surveillance in terms of RIPSA in addition to relying upon the DPA crime and taxation exemption and the fact that the surveillance is undertaken in furtherance

of its general observational duties and statutory powers. We would recommend that SEPA retain a detailed audit trail of its reasoning and the points it considered in following this approach.

The requirements of the HRA are considered in response to Question 6 below and the requirements of the PA are considered in response to Question 12 below.

3. What other non-law enforcement public sector agencies have used this technology and what legal challenges have they faced?

We understand that the UK Environment Agency ("**UKEA**") has deployed drones at landfill sites in Manchester to detect the presence and escape into the atmosphere of methane gas and to mitigate the risk of fires. We have not been able to find any information regarding the legal challenges that the UKEA may have faced in this project.

We have also not been able to find any information with regard to the legal basis that the UKEA relied upon in deploying drones at the above site.

4. What are the differences in law between Scotland, England, Northern Ireland, Wales and Ireland?

As a firm of Scottish solicitors, we are only qualified to provide advice in relation to the law of Scotland and are not qualified to provide advice with regard to the law of any other jurisdiction, including England, Northern Ireland, Wales or Ireland.

However, the provisions underlying the DPA are based on and give effect in UK law to an EU Directive, which applies throughout the EU, including Ireland. RIPSA and RIPA are identical in all material respects and the PA and the HRA apply across the UK.

5. Has the ICO undertaken inquiries into the use of tracking devices and remote sensing by environmental authorities; and, if so, what judgements have they published that environmental authorities need to be aware?

We are not aware of the ICO having undertaken inquiries into or taken enforcement action in connection with the use of tracking devices and remote sensing technologies by environmental authorities.

The ICO has not issued guidance concerning the use of tracking devices and remote sensing technologies by environmental authorities.

6. Are there impacts upon privacy by the tracking of waste carried by company or business vehicles?

In our view, this is predicated upon the nature of the tracking technologies and the extent to which their use will give rise to information regarding the geographic location and movement of individuals who are responsible for the operation of vehicles, and also the extent to which the individuals have been made aware of the technologies (subject to exemption from the

fair processing requirements of the DPA, discussed above). If it is possible to attribute the geographic location and movement of a vehicle to a particular individual then this is, in our view, likely to impact on the privacy of the individuals concerned.

Article 8 of the European Convention on Human Rights ("**ECHR**"), which is incorporated into UK law by the HRA, provides that everyone has the right to respect for family life, home and correspondence. A public authority must not interfere with this right unless it is in accordance with the law and only to the extent that it is necessary in a democratic society (i.e. that the interference with the right is a proportionate response) in pursuit of a number of specified interests, including national security, public safety, or for the prevention of disorder or crime. It is well-established in case law that electronic surveillance and data collection may constitute an interference with the right but only where such activities go beyond mere observation and involve active monitoring of individuals.

It is likely that if the deployment of tracking devices and remote sensing technologies is undertaken pursuant to a RIPSA authorisation then it would be compliant with the ECHR and the HRA.

However, even if the tracking devices or remote sensing technologies are deployed in accordance with the provisions of the DPA, there is still a risk that their deployment could be found to be in breach of Article 8 of the ECHR.

7. Can environmental authorities legally ask waste businesses and companies to place tracking devices in produced wastes so that the movement of this waste can be tracked?

We understand that activity would involve the placing of tracking devices directly in produced wastes with a view to tracking their movement and location within commercial waste streams.

In our view, this would only require a legal basis to the extent to which it would be possible for produced wastes to move from commercial waste streams and into domestic waste streams. If this is possible then the continued tracking of the produced waste after its entry into domestic waste streams may, for the reasons outlined in response to Question 2, give rise to the processing of personal data by SEPA.

In the event that the tracking devices do not enter domestic waste streams then we do not consider that there are legal restrictions on an environmental authority requiring waste businesses and companies to place such tracking devices in produced wastes.

8. In these circumstances, is the environmental authority or the third party company legally responsible?

In our view, the environmental authority would continue to assume responsibility for legal compliance (if a legal basis is required), as it is the instigator of the tracking device into commercial produced wastes, even if the waste businesses and companies place the tracking devices into the wastes on the environmental authority's behalf.

In the event that the tracking devices move from the commercial waste stream to the domestic waste stream, we consider that the environmental authority would assume the role of data controller for the purposes of the DPA. The data controller is the person who determines the purposes for which and the manner in which personal data is processed. The environmental authority would be responsible for determining the manner in which the tracking devices are to operate and the purposes for which the collected data will be used. In complying with its responsibilities under the DPA, we consider that the environmental authority could limit the processing of personal data undertaken by the tracking devices if and when they enter the domestic waste stream by incorporating a "remote disable" function within the tracking devices in order that operation of the devices can be disabled in this event.

On the other hand, we consider that the businesses and companies would be data processors for the purposes of the DPA in this situation insofar as they would be deploying the tracking devices on behalf of the environmental authority, strictly in accordance with its instructions. This applies irrespective of whether the businesses and companies are responsible for transferring the collected data to the environmental authority or if the data is collected directly by the environmental authority from the tracking devices.

If personal data is processed by the tracking devices in the manner outlined above, the DPA requires the data processing relationship to be formalised in a written agreement, in terms of which the businesses and companies are required to comply with the environmental agency's instructions and to put in place appropriate technical and organisational security measures to protect the collected personal data against loss, destruction or damage.

9. Are there any legal implications for an environmental authority using tracking devices and remote sensing if the equipment is compromised and uncovered by a third party?

In our view, this depends on the format that the tracking devices and remote sensing technologies assume. If they are only conduits through which personal data is collected and transmitted to the environment agency then the risks associated with the compromise by a third party are negligible, as the collected data is not stored on the device and nothing will be intercepted.

However, if the tracking devices and remote sensing technologies are capable of data storage and there is a risk that the stored data could consist of personal data for the purposes of the DPA then the environment agency would be required to comply with DPA data security principle and put in place appropriate technical and organisational security measures to protect the collected personal data against loss, destruction or damage. This could include, for example, password protecting the tracking devices and remote sensing technologies, encrypting the contents or incorporating a remote disable function in terms of which the environmental authority can disable the operation of the devices and technologies in the event of their compromise.

10. In what circumstances does tracking devices and remote sensing become covert and require legal authorisations?

Please refer to response to Question 2 above.

11. Does the use of tracking devices and remote sensing require, at all times, a directed surveillance authorisation; and, if so, what level of authorisation is required for deployment? Would the use of tracking devices meet the definition of intrusive surveillance?

Our response to Question 2 above highlights the differences between directed surveillance and intrusive surveillance. As outlined in that response, the need for an authorisation under RIPSA depends on whether the use of the tracking devices and remote sensing technologies will give rise to private information about individuals. If they do then RIPSA is engaged and either a directed surveillance or intrusive surveillance authorisation is necessary, unless the surveillance can be justified on an alternative legal basis, such as the DPA.

In our view, if and to the extent that personal data is collected and processed by the tracking devices and remote sensing technologies to be deployed by SEPA (as outlined in our response to Question 2), SEPA may wish to rely on the DPA crime exemption as its legal basis for undertaking the surveillance. As a consequence of this, we do not consider that SEPA would be required to seek either a directed or intrusive authorisation under RIPSA.

If, however, SEPA does not wish to rely on the DPA exemption then we recommend that a directed surveillance authorisation is obtained for the reasons outlined above in response to Question 2.

12. Would the proposed activity involve intrusion on or interference with private property as defined within the PA?

The PA authorises interference by the Police with property where the authorising officer believes that the taking of such action is necessary for the purposes of preventing or detecting serious crime and the taking of such action is proportionate to what the action seeks to achieve.

“Serious crime” has the same definition in the PA as in RIPSA, set out above in our response to Question 2.

In Scotland, an application for authorisation under the PA must be made by a constable of the Police Service of Scotland to the chief constable of the Police Service of Scotland or any deputy or assistant chief constable as is designated by the chief constable. In granting an authorisation, the authorising officer is to consider whether what is sought to be achieved by the authorisation could reasonably be achieved by other means.

Property interference includes entry on or interference with property. If the tracking devices were to move from the commercial waste stream to the domestic stream and into specific properties then it is likely that this would involve an interference with property for the purposes of the PA. We understand from SEPA that it is highly unlikely that tracking devices would move from one waste stream to the other and the PA is therefore unlikely to be engaged.

13. If the proposed activity falls within the scope of Part 3 of the PA, does the criminality under investigation constitute "serious crime" as defined within the PA?

Please refer to response to Question 12.

14. Does the legislation allow for collaborative working where an authorised agency could make application/conduct activity on behalf of a partner agency?

In our view, there is nothing within the PA prohibiting an environmental agency from approaching the Police and requesting that an application for an authorisation to interfere with property be submitted to the authorising officer, provided that the relevant statutory tests were met.

An environmental agency could apply for a combined RIPSA and PA authorisation or individual authorisations.

Similarly, the DPA does not prohibit SEPA from working in collaboration with other enforcement agencies in relation to waste tracking and sharing data with them, provided that this is undertaken in accordance with the terms of a data sharing protocol into which all of the parties have entered. The protocol would set out: the relationship amongst the parties (identifying who the data controllers and data processors are); the purposes of the data sharing; and the legal basis for the data sharing, including the underlying statutory powers authorising the sharing and the relevant confidentiality, privacy and human rights considerations.

15. Does the tracking of waste from the point of production impact upon privacy?

Please refer to response to Question 8 above.

16. Does the tracking of waste by specific companies or businesses impact upon privacy?

Please refer to response to Question 8 above.

17. What are the civil liberty / ECHR considerations for SEPA in the use of tracking devices and remote sensing?

Please refer to response to Question 8 above.

18. What corroboration, if any, would be required to confirm the details or information gathered by the use of tracking devices and remote sensing?

In our experience, one of the main difficulties encountered in illegal waste depositing prosecutions is being able to identify, from an evidential point of view, the party that engaged in the illegal depositing of waste. The waste may have left company A's factory in vehicle B, destined for site C, at which point company D assumes responsibility for the depositing of the waste (company D being outsourced to provide this service by company A for this purpose). If the waste is subsequently illegally deposited, it may not be clear whether company A was responsible, if vehicle B had been used by an unauthorised party for this

purpose or if company D was responsible. Company A, as the company who presumably authorised the transporting of the waste, may deny responsibility and, from an evidential perspective, it may be difficult to attribute responsibility to any one party.

The Procurator Fiscal will also require a robust trail of evidence to proceed with prosecution.

The use of tracking devices and remote sensing technologies in the form of, for example, drones that capture and track the movement of waste from its origin through to its ultimate disposal destination would assist in providing an evidential trail and corroborating the identity of the perpetrator or those concerned in the perpetration of the illegal depositing.

19. What are the likely, future legal developments in this field about which environmental regulators need to take account?

The DPA will be superseded by the new EU General Data Protection Regulation (the "**GDPR**") in 2018. While the GDPR broadly builds upon the existing DPA framework, the definition of personal data is widened to include any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified by reference to one or more specified factors, including location data. This is consistent with the case law considered in response to Question 2, where the courts have accepted geographic location in isolation as sufficient to constitute personal data for the purposes of the DPA.

The GDPR also enhances the DPA fair processing principle to include the requirement to process personal data transparently. This necessitates a data controller providing individuals with significantly more information than the present DPA fair processing requirements, including details of the rights that individuals may exercise against the data controller. Data controllers are also required to maintain and retain detailed records in relation to their data processing activities under the new accountability principle and must conduct an impact assessment before undertaking any data processing activity that presents specific privacy risks, such as large-scale surveillance of public areas. The GDPR grants EU Member States scope to exempt data processing which is necessary and proportionate to safeguard the prevention, investigation, detection or prosecution of criminal offences from some or all of the data protection principles contained within the GDPR.

The DPA only permits data controllers to transfer personal data to non-EU countries where those countries ensure an adequate level of data protection. This is relevant in the tracking device and remote sensing technologies contexts where the underlying data processing and storage infrastructure (including servers and cloud storage facilities) may be located outwith the EU, for example, in the United States. The United States is not regarded as providing an adequate level of protection for the purposes of the DPA. The "Safe Harbor" arrangement that was put in place to legitimise the transfer of personal data from the EU to the United States was annulled by the European Court of Justice in October 2015 on the basis that it did not provide the requisite adequate level of data protection. The EU Commission and the United States are currently in the process of negotiating a revised data transfer arrangement. While a political agreement was reached earlier this month on the new "Privacy Shield", it is expected that the legal agreement will not be finalised until later in the month. Environmental authorities looking to legitimise data transfers to the United States as part of waste tracking projects will need to ensure that United States' recipients are "Privacy Shield" accredited going forward.

Case Studies (provided by SEPA)

Case Study 1

SEPA wishes to map the flow of waste tyres in Scotland. SEPA will approach tyre producers and ask them to support SEPA in placing tracking devices in waste tyres in order that SEPA can monitor movement of the tyres in the waste stream. SEPA has not identified or targeted particular waste collection organisations. The tyres could be picked up by unknown tyre businesses. SEPA wishes to determine where the tyres are going.

The relevant issues are as follows:

- We assume that the reference to "tyre producers" refers to "tyre retailers" to whom, we understand, used and worn tyres are typically returned at the end of their useful life for disposal by waste collection organisations. We further assume that the waste tyres will be transported by waste collection organisations using vehicles;

- we note that SEPA will not engage directly with waste collection organisations and will not be in possession of information to identify the waste collection organisations involved in the collection and disposal of specific tyres from tyre retailers;

- SEPA's ability to identify the drivers of the waste collection organisations' vehicles is conditional upon the drivers parking or unloading the vehicles at their residential addresses in order to, for example, dispose of the tyres via their domestic waste streams. Only in these circumstances could SEPA be in a position to link the geographic data collected by the tracking devices to the individual drivers in terms of the DPA. Otherwise, in our view, SEPA will experience inevitable difficulties in this regard if the drivers live in, for example, a block of flats, park the vehicles on a main road away from their residences or are staying at places other than their usual addresses. We do not therefore consider that the use of tracking devices by SEPA in this manner would be likely to give rise to SEPA processing personal data relating to individual drivers for the purposes of the DPA, although there may be exceptional circumstances in which SEPA may be processing personal data where, for example, the vehicles are parked in driveways forming part of residential addresses;

- For the reasons outlined above, we consider that SEPA will experience difficulties in obtaining access to information that could assist in linking the geographic location of the tracking devices to the waste collection organisations' vehicles' drivers. As a consequence of this, it is likely that the use of tracking devices by SEPA in this manner will not give rise to private information concerning the movements of the waste collection organisations' drivers and will not constitute directed surveillance for the purposes of RIPSA for which SEPA would be required obtain a directed surveillance authorisation. However, SEPA is empowered by RIPSA to grant directed surveillance authorisations and may in any case wish to self-authorise to mitigate the risk of the tracking devices giving rise to private information relating to the waste collection organisations' drivers. In exceptional circumstances in which the use of tracking devices by SEPA may give rise to private information concerning the movements of the drivers, SEPA's surveillance may constitute "intrusive surveillance" for RIPSA purposes on the basis that it takes place on residential premises, involves the use of a surveillance device attached to waste tyres loaded on the vehicle and is directed towards the prevention or detection of serious crime. SEPA may obtain authorisation to undertake intrusive surveillance from the Chief Constable of the Police Service;

- If SEPA does not self-authorise the directed surveillance under RIPSA, we would recommend that SEPA undertake an HRA impact assessment to verify that the deployment of tracking devices is necessary, proportionate and the least intrusive means of achieving its aims. If it is not, there is a risk of interference with the drivers' right to respect for private life enshrined in Article 8 of the ECHR (if personal data or private information relating to the drivers is revealed by the tracking devices); and
- If the tracking devices move from the commercial waste stream to the domestic waste stream, by for example, being placed within the waste collection organisations' drivers' domestic waste streams then the continued use of the tracking devices could potentially involve an interference with property for the purposes of the PA. SEPA is not empowered to make an application for authorisation for interference with property under the PA but could collaborate with the Police and request that an application be submitted.

Case Study 2

SEPA wishes to map the flow of waste tyres in Scotland. SEPA has received intelligence that some tyre collectors are illegally storing tyres in unknown warehouses and that there is a link to criminal groups. SEPA wishes to map the flow of waste tyres in the hands of specific tyre collection and recycling businesses to: (1) work out where the tyres are going; and (2) support the prevention and detection of crime.

The relevant issues are as follows:

- we have assumed that SEPA will undertake the waste tyre mapping exercise on a covert basis without the knowledge and co-operation of the tyre collection organisations, as the underlying crime prevention and detection purpose would be defeated if the organisations were aware of the exercise; and

- In this situation, SEPA is concerned with whether the vehicles belonging to a particular tyre collection organisation are travelling to and from the same or similar destinations. This will, in turn, assist in the identification of the locations of the unknown warehouses. In doing so, however, there is a risk that SEPA could obtain information relating to the drivers' residential addresses in the manner outlined in relation to Case Study 1 and the same considerations would be relevant in this context from DPA, RIPSA and HRA points of view.

Case Study 3

SEPA suspects that waste is moving between Scotland and England (or between Scotland and Ireland) and that some of this waste is being disposed of in illegal waste sites on the other side of the border from which it emanated. SEPA wishes to track waste carried by specific organisations that SEPA's intelligence suggests are engaged in this activity and to verify whether it is being disposed of at properly licensed waste management sites or illegally stored or disposed of elsewhere.

The relevant issues are as follows:

- We assume that the waste is being transported by vehicle. We note that SEPA wishes to make use of the tracking devices for the purposes of confirming its intelligence that specific organisations are engaged in illegal waste disposal in jurisdictions other than those in which the waste originated;

- we have also assumed that SEPA will be tracking the waste on a covert basis without the knowledge and co-operation of the organisations concerned, as the underlying crime prevention and detection purposes would be defeated if the organisations were aware of SEPA's tracking activities;

- the geographic data collected by the tracking devices regarding the movement of the waste will not in and of itself relate to and identify the drivers of the vehicles being used to transport the waste, unless: (1) SEPA has access to intelligence that could assist in the identification of the drivers; and / or (2) the drivers park or unload the vehicles at residential addresses at the final destination. However, in our view, SEPA will inevitably experience difficulties in attributing residential addresses to individual drivers, as the addresses may be unrelated to the drivers or if they are the drivers' residential addresses, the drivers may live in, for example, a block of flats or park the vehicle on a main road away from the property. The same considerations apply in relation to the owners or residents of the residential addresses at the final destination. In light of this, we do not consider that the use of tracking devices by SEPA in this manner would be likely to give rise to SEPA processing personal data relating to individuals for the purposes of the DPA, although there may be exceptional circumstances in which SEPA may be processing personal data where, for example, the vehicles are parked in driveways forming part of residential addresses;

- for the reasons outlined in relation to the DPA considerations, it is likely that the use of tracking devices by SEPA in this manner will not give rise to private information relating to individuals and will not constitute directed surveillance for the purposes of RIPSA for which SEPA would be required obtain a directed surveillance authorisation. However, SEPA is empowered by RIPSA to grant directed surveillance authorisations and may self-authorise. On that basis, SEPA may wish to self-authorise in any case to mitigate the risk of the tracking devices giving rise to private information relating to individuals. In exceptional circumstances in which the use of tracking devices by SEPA may give rise to private information concerning the movements of the drivers, SEPA's surveillance may constitute "intrusive surveillance" for RIPSA purposes on the basis that it takes place on residential premises, involves the use of a surveillance device attached to waste loaded on the vehicle and is directed towards the prevention or detection of serious crime. SEPA may obtain authorisation to undertake intrusive surveillance from the Chief Constable of the Police Service. The RIPSA authorisation will allow SEPA to engage in

surveillance anywhere in the UK for a period of up to three weeks at a time while the RIPSA authorisation remains in force. No separate authorisation under RIPA is necessary when the waste moves from Scotland to England; and

If the final destination addresses of the waste consist of residential addresses then the deployment of tracking devices attached to such waste could potentially involve an interference with property for the purposes of the PA. SEPA is not empowered to make an application for authorisation for interference with property in terms of the PA but could collaborate with the Police and request that an application be submitted.

Case Study 4

Paragraph 19 exemptions under Paragraph 19 of Schedule 1 to the Waste Management Licensing (Scotland) Regulations 2011 are often used by illicit operators to conceal large scale offending. SEPA wishes to use remote sensing to regularly check the scale and volume of waste imports onto Paragraph 19 sites to assess whether the data collected through this means is consistent with the scale and nature of the activities legally permissible by the exemption conditions and if the operator is abiding by the limits stated in the operator's original application to SEPA. SEPA intends to use remote sensing to review land use at regular intervals throughout the life of the exemption (one year). The exempt sites are not principally residential, but may, on occasion, have a private residence located within or associated with the exempted area.

The relevant issues are as follows:

- We have assumed that the remote sensing technologies to be deployed will consist of drones that scan the scale and volume of waste imports onto the relevant sites in the manner described above. We have further assumed that the drones will be controlled by a pilot in close proximity to the drones and will function on a continuous basis and not be subject to triggers which activate the video capture function. The operator of the site and where the waste is stored and residents may not be aware of the fact that drones are in operation, by whom and for what purposes.

- while SEPA's primary purpose in deploying the drones is to detect levels of specified waste authorised by the Paragraph 19 exemption, drones, by dint of their modus operandi, are likely to process personal data relating to individuals who feature within the captured frames for the purposes of the DPA, including the site operator's staff and any individuals who reside within or in close proximity to the site. The prospect of this is significantly exacerbated when the drones are operating on a continuous basis and are not subject to activation triggers. The height at which drones typically operate will be likely to result in the captured footage being of high quality, even if the footage is "zoomed into". With a view to minimising the personal data captured, SEPA should implement a solution which only captures video footage in response to specified trigger events, such as detection of specified waste substances. SEPA, as the data controller for the purposes of the DPA, is required to comply with the requirements of the DPA. As part of this, SEPA must ensure that the drones are not capable of being compromised, the channel of communication between the drones and the pilot's equipment is secure and there is a "remote disable" function in the event that the drones are compromised, enabling SEPA to "switch off" the drones remotely. SEPA need not comply with the DPA's fair and lawful processing requirements if it can justify its processing of the personal data captured by the drones with reference to the DPA's prevention or detection of crime exemption. If SEPA engages a third party contractor to operate the drones and capture footage on SEPA's behalf, SEPA must enter into a written contract with the contractor, as SEPA's data processor, in terms of which the contractor is required to comply with SEPA's instructions and the data security principle contained within the DPA;

- given that the drones will likely result in SEPA obtaining private information concerning the movements of individuals captured within the footage, particularly if the drones' flight path covers residential areas, this is likely to constitute directed surveillance for the purposes of RIPSA for which SEPA would be required to obtain a directed surveillance

authorisation, unless an exception under RIPSA is available. SEPA is empowered by RIPSA to grant directed surveillance authorisations and may self-authorise. Alternatively, SEPA may proceed without an authorisation if it is satisfied that there is an alternative legal basis justifying the surveillance (the prevention or detection of crime exemption contained within the DPA) or the surveillance is undertaken pursuant to SEPA's general observational duties contained within the EA;

- If SEPA does not self-authorise the directed surveillance, SEPA should undertake an HRA impact assessment to verify that the deployment of drones is necessary, proportionate and the least intrusive means of achieving its aims. A material issue is the fact that the drones will operate on a continuous basis at a relatively low height. If the drones' flight path covers residential areas, this will give rise to video footage being captured of areas where individuals would reasonably expect privacy, such as gardens attached to private dwelling houses. Accordingly, the result of the HRA impact assessment may be that SEPA is required to implement a drone system that only captures video footage in response to specific trigger events. Otherwise, there is a risk of interference with the right to respect for private life enshrined in Article 8 of the ECHR; and

- If the drones' flight path covers residential areas then this could potentially involve an interference with property for the purposes of the PA, depending on the level of intrusion into private areas. SEPA is not empowered to make an application for authorisation for interference with property in terms of the PA but could collaborate with the Police and request that an application be submitted. When determining whether to grant an authorisation, the authorising officer may decide that what is sought to be achieved by the authorisation could reasonably be achieved by other, less intrusive means. This could include implementing a drone system that only captures video footage in response to specific trigger events.

Case Study 5

SEPA understands that waste metals are being stolen from a local authority's recycling centre. SEPA wishes to track metals because this is about recycling targets, leakage, circular economy, etc. Of course, SEPA knows that this information will be of interest to the Police.

- While SEPA only intends to track the movement of waste metals, we assume that the underlying purpose to the tracking is to obtain information concerning identifiable individuals with a view to SEPA and / or the Police taking appropriate enforcement action against the said individuals. The movement of waste is therefore likely to give rise to information concerning identifiable individuals, particularly where the stolen waste metals are removed to or disposed of by the perpetrators of the thefts to residential addresses that SEPA is able to identify using the geographic location of the tracking devices and publicly available resources. If this results in the identification of residential addresses, SEPA must comply with the data protection principles contained within the DPA, unless it is able to rely on a partial exemption from the principles, particularly the requirement to process personal data fairly and lawfully. SEPA could in this case rely on the prevention or detection of crime exemption contained within the DPA. This exception does not, however, provide an exemption from the data security principle and SEPA must ensure that the tracking devices are not capable of being compromised, the channel of communication between the tracking devices attached to the waste metals and the receiving equipment is secure and there is a "remote disable" function in the event that the tracking devices are compromised, enabling SEPA to "switch off" the devices remotely;

- if the use of the tracking devices results in SEPA obtaining private information concerning residential addresses where waste metal has been removed to or disposed of by the perpetrators of the theft then this is likely to constitute directed surveillance for the purposes of RIPSA for which SEPA would be required obtain a directed surveillance authorisation. SEPA is empowered by RIPSA to grant directed surveillance authorisations and may self-authorise. Alternatively, SEPA may proceed without an authorisation if it is satisfied that there is an alternative legal basis justifying the surveillance (the prevention or detection of crime exemption contained within the DPA) or the surveillance is undertaken pursuant to SEPA's general observational duties contained within the EA. In exceptional circumstances in which the use of tracking devices by SEPA may give rise to private information concerning the movements of individuals, SEPA's surveillance may constitute "intrusive surveillance" for RIPSA purposes where it takes place on residential addresses, involves the use of a surveillance device attached to waste metal located at and is directed towards the prevention or detection of serious crime. SEPA may obtain authorisation to undertake intrusive surveillance from the Chief Constable of the Police Service;
- If SEPA does not self-authorise the directed surveillance, SEPA should undertake an HRA impact assessment to verify that the deployment of tracking devices is necessary, proportionate and the least intrusive means of achieving its aims. If it is not, there is a risk of interference with the drivers' right to respect for private life enshrined in Article 8 of the ECHR;
- If the waste metal has been removed to or disposed of by the perpetrators of the thefts to residential addresses then this could potentially involve an interference with those properties for the purposes of the PA. SEPA is not empowered to make an application

for authorisation for interference with property in terms of the PA but could collaborate with the Police and request that an application be submitted; and

- SEPA would not be prevented from sharing any personal data or private information with the Police, provided that SEPA is only sharing the minimum necessary for the purposes of crime prevention or detection.

Case Study 6

Waste is being collected from residential addresses by a sole trader. SEPA has intelligence that this waste is then being "flytipped" by the trader. Can SEPA legally track this waste, if an opportunity presents itself?

- If SEPA attached the tracking devices to waste at the domestic property level prior to the waste being uplifted by the sole trader, SEPA will be able to identify the addresses of the properties at which the tracking devices have been installed. SEPA also has available to it public registers allowing it to identify the owners and residents of the properties in the form of the Land Register and electoral register. In deploying the tracking devices in this manner, SEPA will therefore be processing the personal data of the owners and residents of the properties at which the tracking devices have been deployed;

- Once the waste to which the tracking devices are attached is in the possession of the sole trader, SEPA will collect information in relation to the geographic location of the waste. Given the nature of a sole trader business, and provided that the sole trader's identity is known, any information relating to the geographic movements of the waste will constitute the personal data of the sole trader for the purposes of the DPA, as the geographic data will relate to and identify the sole trader. SEPA must comply with the data protection principles contained within the DPA, unless it is able to rely on a partial exemption from the principles, particularly the requirement to process personal data fairly and lawfully. SEPA could rely on the prevention or detection of crime exemption contained within the DPA, given that the purpose underlying the waste tracking is to target illegal waste disposal activities. This exception does not, however, provide an exemption from the data security principle and SEPA must ensure that the tracking devices are not capable of being compromised, the channel of communication between the tracking devices and SEPA's receiving equipment is secure and there is a "remote disable" function in the event that the tracking devices are compromised, enabling SEPA to "switch off" the devices remotely;

- since the use of the tracking devices results in SEPA obtaining private information concerning the sole trader's movements then this is likely to constitute directed surveillance for the purposes of RIPSA for which SEPA would be required obtain a directed surveillance authorisation. SEPA is empowered by RIPSA to grant directed surveillance authorisations and may self-authorise. Alternatively, SEPA may proceed without an authorisation if it is satisfied that there is an alternative legal basis justifying the surveillance (the prevention or detection of crime exemption contained within the DPA) or the surveillance is undertaken pursuant to SEPA's general observational duties contained within the EA. Attaching tracking devices to waste located at residential addresses may also constitute intrusive surveillance for RIPSA purposes, provided that the surveillance gives rise to private information relating to individuals, involves the use of a surveillance device attached to waste and is directed towards the prevention or detection of serious crime. SEPA may obtain authorisation to undertake intrusive surveillance from the Chief Constable of the Police Service;

- If SEPA does not self-authorise the directed surveillance, SEPA should undertake an HRA impact assessment to verify that the deployment of tracking devices in this manner is necessary, proportionate and the least intrusive means of achieving its aims. If it is not, there is a risk of interference with the sole trader's right to respect for private life enshrined in Article 8 of the ECHR; and

- Deploying tracking devices into the domestic waste stream potentially involves an interference with property for the purposes of the PA. SEPA is not empowered to make an application for authorisation for interference with property in terms of the PA but could collaborate with the Police and request that an application be submitted.