



Drone Use Cases and their Privacy Impacts: A Taxonomy

JOSHUA HOVSHA 

DARAGH O BRIEN

*Author affiliations can be found in the back matter of this article

RESEARCH ARTICLE

 ubiquity press

ABSTRACT

Drones and drone-mounted sensors provide a litany of potential uses for local authorities and municipalities. Early-adopters have piloted and tested the use of drones for specific scenarios. However, widespread implementation requires appropriate planning and development of relevant governance, oversight, and controls to ensure that privacy and data protection rights are respected.

This article provides an overview of the evolution of drone-use scenarios and a snapshot of the current state of the art in respect of balancing the utility of drone-mounted sensors against the data protection and privacy impacts of these technologies. We set out a taxonomy of use case scenarios for drones and drone-mounted sensors. The ambition of our taxonomy is to provide guidance and support for policymakers and users of these technologies in assessing and mitigating data protection risks in the operation of drones and drone-mounted sensors.

CORRESPONDING AUTHOR:

Joshua Hovsha

Marie Skłodowska-Curie Fellow
in data protection Law, Trinity
College Dublin, Dublin, Ireland
hovshaj@tcd.ie

KEYWORDS:

Drone Use; data protection;
Right to privacy; GDPR; Public
Authority; Taxonomy

TO CITE THIS ARTICLE:

Joshua Hovsha and Daragh O
Brien, 'Drone Use Cases and their
Privacy Impacts: A Taxonomy'
(2022) 27(1) *Tilburg Law
Review* pp. 60–80. DOI: [https://
doi.org/10.5334/tilr.281](https://doi.org/10.5334/tilr.281)

1 INTRODUCTION

The modern revolution in the use of drones, particularly by local governments and municipalities has accelerated in recent years due to technological advances in the (i) manufacture of drone airframes, (ii) evolution in battery technologies, and (iii) innovation in sensor and communications technologies and software for data analytics. This is represented in Figure 1 below.

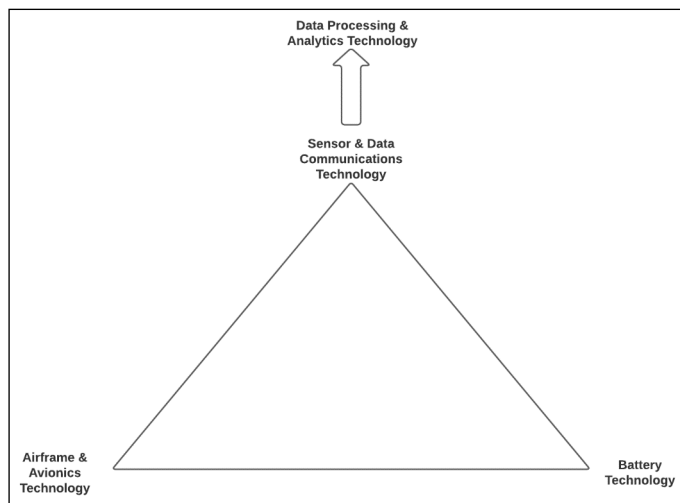


Figure 1 Enablers of the evolution in drone use.

These factors have resulted in an increase in the potential utility of unmanned vehicles to individuals, private companies, as well as local and national authorities. This article provides an overview of the evolution of drone use scenarios and a snapshot of the current state of the art in respect of the balancing of the utility of drone-mounted sensors against the data protection and privacy impacts of these technologies. The specific context for these use cases is within the framework of local authorities and municipalities.

We set out a taxonomy of use case scenarios for drones and drone-mounted sensors. By adopting a structured framework for identifying use cases and scenarios for the deployment of drones and drone-mounted sensors, it will be possible to (i) identify commonly occurring areas of risk, (ii) standardise templates for the documentation of data protection impact assessments for the deployment of drones in specific circumstances, (iii) apply a 'design pattern' approach to any new use cases or emerging technologies that local authorities might wish to deploy.

It is recommended that this taxonomy is developed as a structure framework to support scalable and repeatable processes for assessing and mitigating data protection risks in the operation of drones and drone-mounted sensors.

2 THE REGULATION OF DRONE USE

The first challenge in establishing a legal and ethical framework for drone use in the public sector is that of terminology. Five overlapping terms may be relevant under the general category of drone usage:

- UAV (Unmanned Aerial Vehicle)
- UA (Unmanned Aircraft)
- UAS (Unmanned Aerial System)
- RPA (Remotely Piloted Aircraft)
- RPAS (Remotely Piloted Aircraft System)

All terms are covered by European Regulation under the broad category of "drones." In this article we adopt a similar general approach. Prior to 2018, the regulation of small aircrafts within the EU was the responsibility of Member States. However, per Regulation 2018/1139,¹ The European Aviation Safety Agency established in 2018 now holds regulatory responsibility for drone use.

¹ Regulation 2018/1139, of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency OJ L 212, 22.8.2018, p. 1–122.

The harmonized rules for drone usage may be found in Commission Delegated Regulation 2019/945,² and Commission Implementing Regulation 2019/947.³ These regulations provide specific rules for manufacturers, pilots, and operators.

In terms of real-world implementation within the EU, different member state bodies will take responsibility. For instance, The Irish Aviation Authority (IAA) supervises and implements these Regulations in Ireland. Additionally, Commission Implementing Regulation 2019/947⁴ outlines the need for drone usage to comply with privacy legislation, including the General data protection Regulation (the GDPR).⁵

3 DATA PROTECTION AND DRONES

It is important to note that data protection legislation applies not to the aerial vehicle platform (the drone) but to the processing of personal data by any sensor technologies. Common examples include video cameras and microphones which are mounted on a drone.

The use to which a drone is employed will necessitate that it be equipped with different types of sensor and analytics technologies. These technologies will carry distinct impacts on privacy and data protection. In certain circumstances it will be sufficient to implement mitigations, however in other instances the risks will simply outweigh the benefits and thus the intended use will not be lawful. Common types of sensor equipment include:

- Optical sensors capable of capturing photographic images and recording video surveillance.
- Thermal sensors measuring heat.
- Humidity sensors.
- Wind strength and direction sensors.
- Audio sensors and microphones capable of recording audio, including directional microphones.
- LiDAR⁶ or similar sensor technologies.

Other types of sensors that can be mounted on a drone platform include proximity sensors (to measure distance from objects or other drones), GPS (to identify the location of the drone at a point in time or to manage navigation or set boundaries on the flightpath of the drone), or optical gas imagery (to detect the presence of hazardous gases), and gas sensors to measure air quality. In addition, technologies such as Automatic Number Plate Recognition (ANPR), biometric facial recognition, or similar machine learning analytics can further enhance the capability of drone mounted sensors to support additional use cases.

However, the combination of different sensor types with information processing technologies in different contexts can give rise to a range of potential privacy and data protection challenges that must be balanced against the benefits that might arise from the use of a drone-mounted sensor technology.

3.1 UNDERSTANDING PRIVACY AND DATA PROTECTION

The right to privacy and the right to data protection are two distinct rights enshrined in EU law in Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union, respectively. Both are relevant to the use and operation of drones, drone mounted sensors, and associated technologies. The right to privacy is defined in Article 7 '[e]veryone has the right to respect for his or her private and family life, home, and communications.'

² Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. OJ L 152, 11.6.2019, p. 1-40.

³ Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft OJ L 152, 11.6.2019, p. 45-71.

⁴ *ibid.*

⁵ Regulation (EU) 2016/679, 27 April 2016, General data protection Regulation ('GDPR') OJ L 119.

⁶ Laser Imaging, Detection, and Ranging. A technology which involves the targeting of distances from above with lasers and measuring the time taken for the reflected light to return to the receiver. These readings can be used to create three-dimensional representations of an area.

The use of optical sensors (e.g., cameras) and/or audio sensors (e.g., directional microphones) in areas that overlook homes or areas where people might enjoy a presumption of privacy needs to be carefully planned and executed to mitigate the risks to this right.

The Right to Data Protection is outlined in Article 8 of the Charter of Fundamental Rights of the European Union:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Thus, when personal data of any individual is obtained and processed by an organisation, it must be done for specific purposes with a clear legal basis. This right is given effect through legislation such as the General Data Protection Regulation (GDPR). The definition of 'personal data' is given in Article 4(1) of the GDPR:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

From here the definition of 'data subject' is drawn to be the identified or identifiable natural person to whom personal data pertains. Recital 26 of the GDPR provides guidance on the threshold for the possibility of identification. The mere hypothetical possibility of identification is not sufficient to meet the standard of 'identifiable' and thus does not constitute personal data under the GDPR.⁷ Rather, the boundaries of 'identifiable' is limited to 'all the means reasonably likely to be used.' Recital 26(4) of the GDPR explains:

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

However, for information to be treated as 'personal data' within the meaning of EU Data Protection Law, there is no requirement that all the information enabling the identification of the data subject must be held by the same individual or entity.

As with the definition of 'personal data', the term 'processing' is intentionally far-reaching. Article 4(2) of the GDPR defines 'processing' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.' A long, but not exhaustive list of activities which meet this definition is provided:

'processing' such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processing, therefore, includes the capture and recording of personal data, the consultation or use of that data, and the onward transmission or publication of data. In the case of drone-mounted cameras data processing includes the viewing of the cameras in real time, as well the later viewing of any recordings which are made. In the context of drone usage personal data processing occurs when:

⁷ Mac Macmillan, 'Data Protection Concepts', in: Ustaran, Eduardo et al. *European Data Protection* (Second, IAPP Publications 2019).

- Clear footage of a person's face is recorded.
- An individual can be identified in another manner such as through the GPS location, visible address, car registration, and personal items including clothing.
- Information about an individual's private life, behaviour, bodily characteristics are revealed through the footage or images.
- Recordings are made of an individual's voice or conversation
- A person's heat signature can be identified revealing behaviour.
- Intimate imagery exposing home life is recorded.

It is also important to consider the risk of a drone-mounted sensor capturing data which could be categorised as 'special category data' under the GDPR, which carries with it a higher standard of protection. Under Article 9 of the GDPR special category data is data which can reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The category additionally includes all genetic and biometric data as well as information concerning and individual's health, sexual history, or sexual orientation.

Drones which monitor home life as well as religious, political or trade union buildings may reveal personal information about these types of special category data in a manner that can be associated to an identifiable person. A common example is the recording of those entering a mosque or synagogue at prayer times.

The European Union's *DroneRules*. EU⁸ project outlined the risks to privacy associated with different technologies used with drones. We have expanded on their classification in Table 1 below. Our purpose in doing so is to clearly differentiate between the sensors used and the processing of sensor data either on-device or off-device after data transfer.

Table 1 Category of Sensors and Potential Privacy Impacts.

CATEGORY OF SENSOR /PROCESSING	PAYLOAD/CAPABILITY	POTENTIAL PRIVACY IMPACTS
Optical Sensor (Cameras)	High-Definition Camera	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home
	Camera with zoom capability	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home
Audio Sensors	Directional Microphone	• Privacy of voice/spoken word and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of Communications
Environmental Sensors	Thermal Sensor	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of home
	Multi-spectrum NDVI ⁹ used to assess health of vegetation	• Potential impacts if normal optical camera capability is employed as well • Combination with other data sets could result in data protection/privacy risk.
	Gas Sensor	• Privacy of home
	Humidity Sensor	• Privacy of home
	Air Quality Sensor	• Privacy of home
	GPS/Geolocation Sensors	• Privacy of location and space
	LiDAR	• Privacy of home

(Contd.)

⁸ DroneRules.eu is an awareness campaign tool that aims to inform and educate the drone user community and the general public how to fly legally in the different EU member states, and Norway and Switzerland. The project is co-financed by the European Commission under the COSME Programme. See <https://dronerules.eu/en/faq>.

⁹ Normalized Difference Vegetation Index (NDVI) is a measurement of the amount of live vegetation in an area and is commonly used for agricultural assessment.

CATEGORY OF SENSOR /PROCESSING	PAYLOAD/CAPABILITY	POTENTIAL PRIVACY IMPACTS
AI matching and recognition	Facial Recognition	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home
	ANPR	• Privacy of image and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of home
	Audio/Speech recognition	• Privacy of voice/spoken word and data • Privacy of behaviour and action • Privacy of association • Privacy of beliefs (political/religious/philosophical) • Privacy of communications
General Platform Capability Concerns	First Person View	Risk of dehumanising data subjects arising from them being “othered” as collateral data capture not related to the primary focus of the processing.
	Battery Endurance/Range	Out of sight, out of mind” risk. Drone platform could fly at altitude or in a flight range that risks more secondary capture of personal data than anticipated.

3.2 THE OBLIGATION TO CONDUCT IMPACT ASSESSMENTS

Article 35 of the GDPR mandates that a ‘Data Protection Impact Assessment’ (DPIA) must be undertaken where processing of data is likely to result in a “high risk to the rights and freedoms” of natural persons. Furthermore, Article 35 (3) outlines a non-exhaustive list of processing activities which require a Data Protection Impact Assessment.

A data protection impact assessment referred to in paragraph 1 shall ***in particular*** be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale. (*Emphasis added*)

The non-exhaustive nature of this list has been reinforced by the European Commission’s Working Party 29. As is explicitly made clear in its guidelines, which were endorsed by the European Data Protection Board on 25 May 2018 ‘the words “in particular” in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be “high risk” processing operations that are not captured by this list, but yet pose similarly high risks.’¹⁰

As such the European Data Protection Board outlines nine criteria which signal high risks and thus require a full assessment. These are derived from Article 35 of GDPR along with recitals 71, 75 and 91, and a review of the phrasing ‘likely to result in a high risk’ throughout the Regulation. These are:

- Evaluation and scoring
- Automated decision-making
- Systemic monitoring
- Processing of sensitive data or data of a highly personal nature
- Data Processed at a large scale
- Matching and Combining datasets
- Data concerning vulnerable data subjects

¹⁰ Working Party 29, ‘Guidelines on Data Protection Impact Assessment (DPIA) WP248. Endorsed by the European Data Protection Board on 25 May 2018’ (2018) <<https://ec.europa.eu/newsroom/article29/items/611236>>.

- Innovative use of technology or applying new technological or organisational solutions
- When the processing in its own right “prevents data subjects from exercising a right or using a service or a contract” as laid out in Article 22 and Recital 91 of GDPR.¹¹

The taxonomy we outline in this article has identified four main families of scenarios, with sub-types of use defined based on the specific objectives or purposes, combinations of sensor technologies, or locations for operation. For each of these families of scenarios a Data Protection Impact Assessment (DPIA) can be defined along with a standard set of safeguards and controls. More specific DPIAs can be defined for more complex or high-risk scenarios if necessary.

3.3 RECURRING DATA PROTECTION CONCERNS FOR DRONE USE

Article 5 of the GDPR outlines core principles which must be adhered to for all processing of personal data. In all cases personal data shall be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency Principle).
- Used only for the purpose for which it was gathered (Purpose Limitation Principle)
- Limited only to the minimal amount of data necessary for the purposes of processing (Data Minimisation Principle)
- Assured of accuracy and updated if necessary (Accuracy Principle)
- Always maintained with integrity and confidentiality (Integrity and Confidentiality Principle)
- Retained only for as long as is necessary (Storage Limitation Principle)
- Processed in an accountable manner, by which compliance with the other Principles can be demonstrated (Accountability Principle)

Table 2 outlines recurring issues in drone deployment which must be considered in a DPIA. These issues have been identified through an analysis of use cases examined in current industry and academic research.¹² Article 35 of GDPR makes it clear that the concern to be resolved by a DPIA is not limited to data protection. Instead, article 35 (1) lists the requirement for a DPIA to be triggered whenever there is a high risk to the ‘rights and freedoms of natural persons.’

Table 2 Recurring Data Protection Concerns for Drone Use.

ISSUE	DESCRIPTION
Lawfulness, Fairness, transparency	A lawful basis must be found for the proposed processing activities which must be identified and laid out clearly. In the case of incidental data processing a lawful basis is often not even considered. Additionally, data processing is unlikely to be fair and transparent when individuals on the ground are unaware that a drone is in operation. Individuals on the ground must be made aware that their data is being captured. They should be informed of when, how, why, and by whom the drone is being used. This allows them to adjust their privacy expectations, be prepared and keep control over their privacy by acting accordingly.
Data Minimisation	Limiting personal data captured to only that which is necessary is difficult in the case of drone use where the desire to capture as much information as possible is common.
Integrity, Confidentiality, and Storage Limitation	Data taken from drones is not often labelled as personal data and thus is not kept in line with the storage requirements under the Storage Limitation and Integrity and Confidentiality principles of the GDPR.
Privacy of thoughts and feelings	Individuals have a right not to share their thoughts or feelings or to have them revealed. This includes beliefs or religious views which may be inferred from data captured by drones.
Chilling effect on behaviour.	Individuals may perform a form of self-preservation/ self-censorship by restricting their behaviour when they are, or believe that they are, being watched. Making individuals in the area aware of the purpose of filming and what is being captured can reduce this negative effect.

¹¹ *ibid* 9–10.

¹² Anne Gerdes, ‘Drones and Privacy Issues’ (Information, Technology and Innovation Research Group at University of Southern Denmark <http://infot>, University of Southern Denmark, 2017) <http://infotechinnno.sdu.dk/pdfs/Drones%20and%20privacy%20SDU_042418.pdf>. Altawy Riham and Amr. M. Youssef, ‘Security, Privacy, and Safety Aspects of Civilian Drones: A Survey ACM Transactions on Cyber-Physical Systems, Vol. 1, Issue 2, Article 7, November 2016, 25 Pages.’ <<https://users.encs.concordia.ca/~youssef/Publications/Papers/Drone-Survey.pdf>>.

It is important to consider not just the data protection implications of the drone operation itself, but also those that will arise from any further processing of the data such as sharing with other parties or combining data with other data.

4 TAXONOMY OF DRONE USE CASES

A recurring theme in research is the lack of a taxonomy for drone use cases and associated personal data infringements. It is instead far more common to find individual use cases from industry used within academic study. Common use cases include:

- Emergency use – Drones can play a pivotal role in rescue missions and other urgent humanitarian response plans. These include search and rescue, natural disaster management, humanitarian aid delivery, and ambulance services.
- Infrastructure monitoring and inspection – Drones fitted with high resolution video recording capacity may provide simple access options for the inspection of infrastructure which would otherwise be difficult to reach safely. Such usage is common for power lines, rail tracks, wind turbines, and waste management facilities.
- Mapping – Drones may be used for mapping for numerous projects including geographic surveys for future roads or housing development, construction planning and mining.
- Earth Science – the resources required for surveying and GIS mapping are greatly reduced through drone usage.
- Filming historical/cultural sights for promotion or sale.
- Filming events for publicity and future promotion.
- Prevention, detection, and investigation of crime.

These archetypes of drone usage are reinforced through the research of Mitka and Mouroutsos¹³ who represent the categories which they have identified in Figure 2 below.

Emergency	Infrastructure Monitoring & Inspection	Environment	Earth Science	Defence and Security
• Search & Rescue • Natural Disaster Management • Humanitarian Aid • Ambulance	• Real Estate Agents • Powerline Inspection • Logistics • Insurance	• Soil moisture • Gas Level • Agricultural Studies • Crops Monitoring	• Media Business • Archaeology • GIS Professionals	• Traffic Surveillance • Drug Monitoring • Pipeline Patrol • Port Security

Figure 2 Drone Use Cases. Based on Mitka & Mouroutsos (2017).

4.1 TAXONOMY LEVEL ONE

Our analysis identified approximately 50 distinct drone use cases for local authorities and municipalities which are clustered into four main categories: (i) Monitoring and Measurement, (ii) Incident Response and Planning, (iii) Investigation and Enforcement, and (iv) Media, Publicity, and Entertainment. These are outlined in Table 3 below.

Table 3 Taxonomy Level 1 Definitions.

USE CASE TAXONOMY LEVEL 1	DEFINITION
Monitoring and Measurement	Drone mounted sensors and associated technologies are used to monitor a location to gather actionable information about a thing/event or to support statistical measurement of an aspect of the environment, infrastructure, or services that are provided by the local authority.
Incident Response and Planning	Drone mounted sensors and associated technologies are used to support the planning for or response to incidents which may pose a risk to people, property, or the environment
Investigation and Enforcement	Drone mounted sensors and associated technologies are used to record and document information related to the detection, investigation, and prosecution of criminal offences or breaches of legislation
Media, Publicity, and Entertainment	Drone mounted sensors and associated technologies are used to capture audio-visual recordings of locations, incidents, or events. Drones may also be used to provide operational or logistical support to the production or execution of public events or entertainment.

¹³ Eleftheria Mitka and Spiridon G Mouroutsos, 'Classification of Drones' (2017) 6 American Journal of Engineering Research.

It is important to note that personal data captured or recorded for one category of use case might be used for another purpose that falls under another category. Additionally, efficient use of drone assets might result in a single drone flight operation addressing requirements across one or more category of use case.

Prior planning will ensure that the appropriate sensor technologies are deployed in the correct way to ensure that appropriate safeguards are in place to protect data protection and privacy rights. Particularly any secondary use must be compatible with the purpose for which data was originally obtained in line with the *Purpose Specification Principle* outlined in Article 5 of the GDPR. For example, imagine that a drone flight is planned to capture video footage of a community litter awareness event. At the same time there is a report of an outbreak of an invasive plant species in the area where the drone will be operating, and a survey is required to assess the extent of the problem. The footage recorded by the drone will therefore support objectives across two categories of use case. However, the processing of footage of people would not be necessary for the environmental monitoring use case. Therefore, the drone operation will need to be planned to record the footage of the community event and then carry out a separate survey pass with people excluded from the area where the drone is operating.

4.2 TAXONOMY LEVEL TWO

At level two of our taxonomy the four main categories are further divided and elaborated upon as is presented in Table 4.

TAXONOMY LEVEL 1	TAXONOMY LEVEL 2	DEFINITION
Monitoring and Measurement	Environmental Monitoring	Use of drone mounted sensors and associated technologies to survey, monitor, or measure features of the natural environment to detect positive and negative changes in the environment and inform policy responses and remedial action.
	Built Environment Monitoring	Use of drone mounted sensors and associated technologies to survey, monitor, or measure features of the built environment to detect positive and negative changes in the built environment, including impact on the natural environment and inform policy responses and remedial action.
	Population Movement Measurement	Use of drone mounted sensors and associated technologies to survey, and measure population movements within the area to support the development of and validation of statistical models to inform policy responses and remedial action.
	Surveying and Mapping	Use of drone mounted sensors and associated technologies to survey and map features of the natural or built environment for the purposes of producing geospatial and navigation data sets.
Incident Response and Planning	Pre-Incident Planning	Use of drone mounted sensors and associated technologies to survey locations to identify issues and risks to be mitigated through the development of an incident response plan.
	Event Monitoring	Use of drone mounted sensors and associated technologies to actively monitor an event to support event management and inform response to incidents at the event.
	Incident Response	Use of drone mounted sensors and associated technologies to support the response to an emergency incident event by the relevant agencies and to inform decision-making during the incident handling. Different categories of incident may require different technology responses.
Investigation and Enforcement	Scene of Crime Response	Use of drone mounted sensors and associated technologies to assist the gathering of evidence and recording of information related to the scene of an accident or criminal incident to support the investigation of any offence and the prosecution of any offender.
	Local Authority Statutory Function Enforcement	Use of drone mounted sensors and associated technologies to assist the gathering of evidence and recording of information related to the scene of a breach of regulations in an area which the local authority has a statutory investigative or enforcement role to support the investigation of any offence and the prosecution of any offender.
Media, Publicity, and Entertainment	Media Recording	Use of drone mounted sensors and associated technologies to record video, audio, still imagery, or other data for publication or dissemination by the local authority or another party.
	Event Production	Use of drones without any additional sensor technologies other than those required for the safe flight operations of the drone for the purposes of supporting the production of an entertainment event (e.g., drone-enabled light displays, event lighting, or equipment transport).

Table 4 Taxonomy of Drone Use: Levels 1 and 2.

The two top levels of our taxonomy are represented in [Figure 3](#) below:

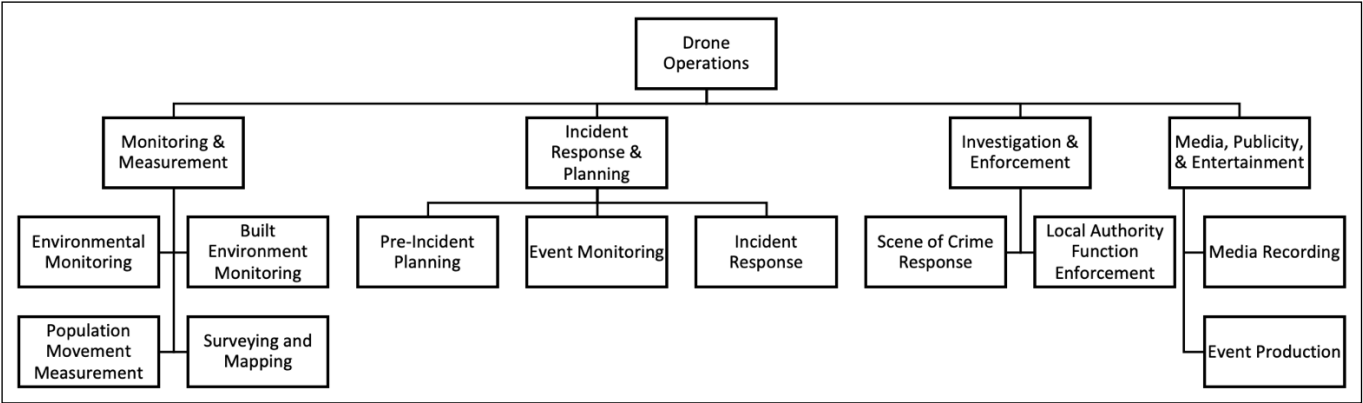


Figure 3 Taxonomy Levels 1–2.

4.3 TAXONOMY LEVEL THREE

The scenarios and use cases identified at Level Three of this taxonomy are examples of specific use cases or categories of specific use case. Within each of these categories it should be possible to identify a defined approach and method for data analysis, and to determine what types of drone-mounted sensor would be used for the acquisition of the data being processed. If necessary, an additional level of classification could be introduced for a more granular definition of use cases and scenarios.

At this level of use case definition, it should be possible to identify the commonly occurring data protection and privacy issues that may arise in the context of the use case and define a set of recommended mitigations to be applied in each case. These can then be aggregated into Standard Operating Procedures for the type of drone use envisaged.

The third level of our Taxonomy is presented in [Tables 5](#), [6](#), and [7](#) below. It should be noted that the examples provided in the tables below are for illustrative purposes only in this article. In the interest of brevity, we do not examine the legal basis for any processing in the scenarios discussed. It should be additionally noted that the taxonomy of use cases and scenarios presented here is not exhaustive. Scenarios may arise which can be added over time. This article aims to provide a structured way of classifying scenarios so that common data protection risks and issues can be identified. In turn the governance controls and decision-making processes around the use of drone-mounted technologies can be simplified.

Table 5 Environmental Monitoring.

4.3.1 Taxonomy Level Three: Monitoring and Measurement

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Algal Bloom Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure the extent of algal bloom outbreaks and inform planning around remedial actions	Acquisition of Data: Drone survey of an area using optical and hyperspectral imagery. Example Risk: overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. Example Mitigations: • Activate optical sensors only when over target area (measured by GPS mapping). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable
Invasive Species Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure the extent of invasive species outbreaks and inform planning around remedial actions.	Acquisition of Data: Survey of an area using optical and hyperspectral imagery. Example Risk: Overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. Example Mitigations: • Activate optical sensors only when over target area (measured by GPS mapping). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable.

(Contd.)

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Wastewater Discharge Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure, the discharge of wastewater into the environment.	Acquisition of Data: Drone survey of an area using optical, multi-spectrum or thermal imagery. Example Risk: overflight of homes or individuals in public or private areas while optical sensors are active and/or recording. Example Mitigations: • Activate optical sensors only when over target area (defined by GPS and/or geofencing). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable.
Waste Management Monitoring	Use of drone mounted sensors and associated analytics technologies to identify, map, and measure, the operation of approved waste disposal locations. This could include the use of gas sensors to measure emission of methane or other gases.	Acquisition of Data: Drone survey of an area using optical, multi-spectrum imagery or gas sensors. Example Risk: Risk of secondary capture of individuals visiting or working at the waste management facility. Example Mitigations: • Activate optical sensors only when over target area (defined by GPS and/or geofencing). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Restrict access to areas that are subject to drone flight. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable.
Air Quality Monitoring	Use of drone mounted sensors and associated analytics technologies to gather statistical data on air quality in an area.	Acquisition of Data: Survey of air quality in an area using drone-mounted pollution sensors. Example Risk: Use of optical sensors on drone for flight/navigation may capture imagery of homes/private areas or individuals in public or private areas. Example Mitigations: • Activate optical sensors only when over target area (defined by GPS and/or geofencing). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable.
Noise Pollution Monitoring	Use of drone mounted sensors and associated analytics technologies to gather statistical data on noise pollution and ambient noise levels in an area.	Acquisition of Data: Survey of air quality in an area using drone-mounted microphones and audiometry sensors Example Risks: • Use of optical sensors on drone for flight/navigation may capture imagery of homes/private areas or individuals in public or private areas. • Retention of recordings may include personal data (secondary obtaining). Example Mitigations: • Activate optical sensors only when over target area (defined by GPS and/or geofencing). • Apply narrow framing of optical imagery to reduce risk of secondary capture. • Select optical sensor with appropriate resolution to reduce risk of unnecessary capture of high-definition video imagery in which people could be identifiable. • Retain only metric data calculated on-device not raw recordings.

Table 6 Built Environment Monitoring.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Building Safety Monitoring	Use of drones to survey buildings, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess risks to public from defects or damage	Acquisition of Data: Survey of building using optical sensors (cameras) to capture high-definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. Example Risks: • High-definition optical sensors increases risk that individuals will be identifiable in recordings. • Recordings may capture imagery of homes/private areas or of individuals in public or private areas. • Retained recordings may contain personal data. Example Mitigations: • Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording. • Advise public/residents in advance of the use of drones for recording • Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Preventative Maintenance Planning & Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess, identify, and prioritise requirements for preventative maintenance	Acquisition of Data: Survey of building using optical sensors (cameras) to capture high-definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. Example Risks: • High-definition optical sensors increases risk that individuals will be identifiable in recordings. • Recordings may capture imagery of homes/private areas or of individuals in public or private areas. • Retained recordings may contain personal data. Example Mitigations: • Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording. • Advise public/residents in advance of the use of drones for recording. • Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Energy Efficiency Measurement & Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to assess, identify, and prioritise requirements for preventative maintenance	Acquisition of Data: Survey of building using optical sensors (cameras) to capture high-definition images of features or defects. Might also include use of gas sensors to detect emissions or toxic gases. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remediation. Example Risks: • High-definition optical sensors increases risk that individuals will be identifiable in recordings. • Recordings may capture imagery of homes/private areas or of individuals in public or private areas. • Retained recordings may contain personal data. Example Mitigations: • Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording. • Advise public/residents in advance of the use of drones for recording. • Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Hazardous Material Storage Monitoring	Use of drones to survey buildings or other built environment, particularly areas that are inaccessible or difficult to access without other safety equipment, to identify any risks associated with the storage of hazardous or potentially hazardous materials.	Acquisition of Data: Survey of locations using optical sensors (cameras) to capture high-definition images of areas where hazardous or potentially hazardous materials are stored. Might also include use of gas sensors to detect emissions or toxic gases or LIDAR mapping of areas obscured by foliage. Imagery/sensor data would usually be recorded for inspection or to be shared with other stakeholders involved in remedial action. Example Risks: • High-definition optical sensors increases risk that individuals will be identifiable in recordings. • Recordings may capture imagery of homes/private areas or of individuals in public or private areas. • Retained recordings may contain personal data. Example Mitigations: • Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording • Advise public/residents in advance of the use of drones for recording • Only retain recordings if required to support planning and execution of remedial works, investigation of suspected criminal offences, or if more detailed inspection of footage is required.

Table 7 Population Movement Measurement.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Traffic Flow Measurement	Use of drones to survey traffic flow for defined short periods (statistical sampling)	Acquisition of Data: Capture of optical image data of vehicles to be analysed off-line using machine learning technologies or human inspection to generate statistical analysis of traffic flow. Example Risks: - Optical sensor may capture images of that individuals who will be identifiable in recordings. - Recordings may capture imagery of homes/private areas or of individuals in public or private areas. - Retained recordings may contain personal data. Example Mitigations: - Activate cameras only in the area where inspection is taking place and for the duration of the recording - Frame the recording to reduce risk of recording footage of private homes or private areas - Advise public/residents in advance of the use of drones for recording - Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required. - Limit access to recorded data.
People Movement Measurement	Use of drones to survey pedestrian movements for defined short periods (statistical sampling)	Acquisition of Data: Capture of optical image data of vehicles to be analysed off-line using machine learning technologies or human inspection to generate statistical analysis of traffic flow. Example Risk: - High-definition optical sensors (if used) increases risk that individuals will be identifiable in recordings. - Recordings may capture imagery of homes/private areas or of individuals in public or private areas. - Retained recordings will contain personal data. Example Mitigation: - Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording - Avoid use of technologies such as APNR unless a clear statutory justification is identified. - Advise public/residents in advance of the use of drones for recording. - Only retain recordings if required to support planning and execution of remedial works or if more detailed inspection of footage is required.
Surveying and Mapping	Use of drone mounted sensors and associated technologies to survey and map features of the natural or built environment for the purposes of producing geospatial and navigation data sets	Acquisition of Data: Capture of optical image data of landscape and landscape features. Example Risks: - High-definition optical sensors (if used) increases risk that individuals will be identifiable in recordings. - Recordings may capture imagery of homes/private areas or of individuals in public or private areas. Example Mitigations: - Activate high-definition cameras only in the area where inspection is taking place and for the duration of the recording. - Operate drone at an altitude which reduces the risk of individuals being identifiable from any recorded image or video. - Consider use of alternate technology such as LiDar to carry out mapping and surveying to reduce risk of secondary capture of identifiable data.

4.3.2 Taxonomy Level Three: Incident Response and Planning

The Taxonomy of incident response and planning is represented in [Figure 4](#) and detailed in the [Table 8](#) below:

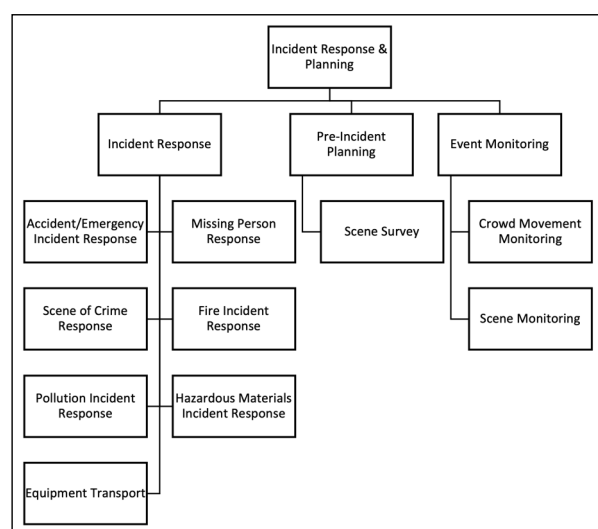


Figure 4 Incident Response and Planning.

Table 8 Incident Response and Planning.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Accident/ Emergency Response	Use of drones to assess scene of an accident or emergency incidents to provide information on the incident and associated risks.	Acquisition of Data: - Survey of an incident location using high definition optical/thermal/ gas sensors to provide real-time overview of scale of incident and provide advance warning of risk factors or identify blocked roads etc. - Record incident response for post-incident review and training purposes - Use of LiDar or similar technologies for rapid mapping of incident area. Example Risks: - High-definition video recording will capture identifiable people. - Imagery may include data relating to health if injured persons are captured. Example Mitigations: - Activate HD cameras only where necessary to provide operational information for incident response. - Ensure drone device is visible and identifiable as an emergency service asset. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Missing Person Response	Use of drones to assist in the search for missing persons	Acquisition of Data: - Survey of an incident location using high definition optical/thermal/ audio sensors/ LiDAR mapping - Record incident response for post-incident review and training purposes. Example Risk: High-definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. Example Mitigations: - Activate HD cameras only where necessary to provide operational information for incident response. - Ensure drone device is visible and identifiable as an emergency service asset. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Pollution Incident Response	Use of drones to assist in the execution of response to a pollution incident	Acquisition of Data: - Survey of an incident location using high definition optical/thermal/multi-spectrum imagery. - Record incident response for post-incident review and training purposes. - Use of LiDar or similar technologies for rapid mapping of incident area. Example Risks: - High-definition video recording will capture identifiable people. - Imagery may include data relating to health if injured persons are captured. Example Mitigations: - Activate HD cameras only where necessary to provide operational information for incident response - Ensure drone device is visible and identifiable as an emergency service asset. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Fire Incident Response	Use of drones to assess scene of a fire safety incidents to provide information on the incident and associated risks.	Acquisition of Data: - Survey of an incident location using high definition optical/thermal/multi-spectrum imagery to provide real-time information to responders. - Record incident response for post-incident review and training purposes - Use of LiDar or similar technologies for rapid mapping of incident area. Example Risks: - High-definition video recording will capture identifiable people. - Imagery may include data relating to health if injured persons are captured. Example Mitigations: - Activate HD cameras only where necessary to provide operational information for incident response. - Ensure drone device is visible and identifiable as an emergency service asset. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

(Contd.)

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Hazardous Materials Incident Response	Use of drones to assess scene of emergency incident where there is a known or potential Hazardous materials risk to provide information on the incident and associated risks.	Example Risks: • High-definition video recording will capture identifiable people. • Imagery may include data relating to health if injured persons are captured. Example Mitigations: • Activate HD cameras only where necessary to provide operational information for incident response. • Ensure drone device is visible and identifiable as an emergency service asset. • Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. • Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Pre-Incident Planning (Scene Survey)	Use of drones to survey a location in advance of an event or as part of a risk assessment and mitigation planning for a location.	Acquisition of Data: • Survey of an incident location using optical/ thermal/multi-spectrum imagery/LiDAR to support risk assessment and planning • Record imagery for off-site analysis Example Risks: • Drone may overfly private homes or other private spaces. • Cameras may capture individuals in public or private locations. Example Mitigations: • Activate Cameras only where necessary to carry out the survey activity. • Consider necessity of resolution of imagery for the planning purpose. • Ensure drone device is visible and identifiable as an emergency service asset. • Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. • Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Monitoring	Use of drones to monitor crowd movements at events to provide feedback to event security and support personnel	Acquisition of Data: Survey of an event location using optical sensors and audio sensors to provide real-time information to event staff. Example Risk: High-definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured Example Mitigations: • Use cameras only where necessary to carry out the survey activity. • Consider necessity of resolution of imagery for the planning purpose. • Ensure drone device is visible and identifiable as an emergency service asset. • Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. • Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Equipment Transport	Use of drones at incidents or events to transport equipment to inaccessible or hazardous areas	Acquisition: • Use of GPS and drone mounted sensors to support piloting of drone to required location. • Record imagery for off-site analysis, incident response review, training. Example Risks: • High-definition video recording will capture identifiable people. • Imagery may include data relating to health if injured persons are captured. Example Mitigations: • Use cameras only where necessary to carry out the transport activity. • Consider necessity of resolution of imagery for the transport purpose. • Ensure drone device is visible and identifiable as an emergency service asset. • Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. • Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

4.3.3 Investigation and Enforcement

The taxonomy of Investigation and Enforcement is represented in Figure 5 and detailed in the Table 9 below:

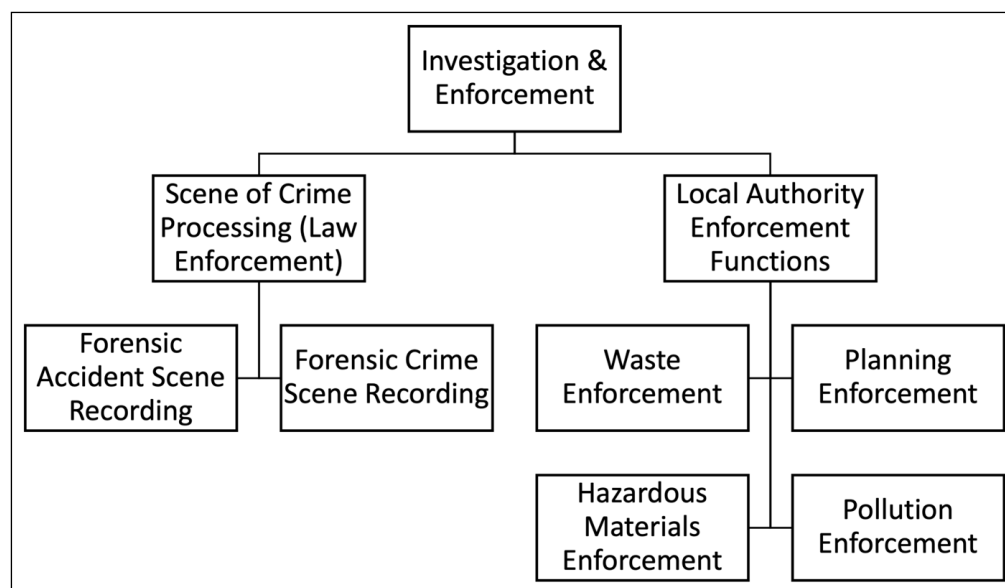


Figure 5 Investigation and Enforcement.

Table 9 Investigation and Enforcement.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Forensic Accident Scene Recording [Note: processing may be covered by Part 5 of Data Protection Act 2018]	Use of drones to conduct survey of an accident scene to support investigation process	Acquisition of Data: Survey of accident area using high-definition video/thermal imagery or other sensors Use of LiDAR or similar technologies for rapid mapping of incident area. Example Risks: - High-definition video recording may capture identifiable people. - Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigations: - Activate HD cameras only where necessary to record the accident location and scene. - Ensure drone device is visible and identifiable as an emergency service asset when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Forensic Crime Scene Reporting [Processing is covered by Part 5 of Data Protection Act 2018]	Use of drones to conduct survey of an a known crime scene to support investigation process	Acquisition of Data: - Survey of accident area using high-definition video/thermal imagery or other sensors - Use of LiDAR or similar technologies for rapid mapping of incident area. - Analyse data off-site to support accident investigation and potential criminal prosecution. Example Risk: High-definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigation: - Activate HD cameras only where necessary to record the accident location and scene. - Ensure drone device is visible and identifiable as an emergency service asset when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Waste Management Enforcement	The use of drone mounted sensors to carry out inspections of authorised and unauthorised waste management facilities and to gather evidence of any legislative or regulatory breaches.	Acquisition of Data: - Survey of accident area using high definition video/thermal imagery or other sensors. - Use of LiDAR or similar technologies for rapid mapping of incident area. - Analyse data off-site to support investigation and any further search or response, and potential criminal prosecution. Example Risks: - High-definition video recording may capture identifiable people. - Drone may overfly private homes or other private areas. - There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigations: - Activate HD cameras only where necessary to record the inspection location. - Ensure drone device is visible and identifiable as being operated by the local authority asset when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Planning Enforcement	The use of drone mounted sensors to carry out inspections of any building or development to assess compliance with planning permissions and gather evidence of any legislative or regulatory breaches.	Acquisition of Data: - Survey of accident area using high definition video/thermal imagery or other sensors - Use of LiDAR or similar technologies for rapid mapping of incident area. - Analyse data off-site to support investigation and any further search or response, and potential criminal prosecution. Example Risks: - High-definition video recording may capture identifiable people. - Drone may overfly private homes or other private areas. - There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigations: - Activate HD cameras only where necessary to record the inspection location. - Ensure drone device is visible and identifiable as being operated by the local authority asset when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Pollution Enforcement	The use of drone mounted sensors to gather evidence to support prosecutions for pollution offences.	Acquisition of Data: - Survey of accident area using high-definition video/thermal imagery or other sensors - Use of LiDAR or similar technologies for rapid mapping of incident area. - Analyse data off-site to support accident investigation and potential criminal prosecution. Example Risk: High-definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigation: - Activate HD cameras only where necessary to record the inspection location. - Ensure drone device is visible and identifiable as being operated by the local authority when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Hazardous Materials Storage Enforcement	The use of drone mounted sensors to gather evidence to support the detection of and removal of materials and the execution of any criminal or administrative sanctions.	Acquisition of Data: - Survey of accident area using high-definition video/thermal imagery or other sensors - Use of LiDAR or similar technologies for rapid mapping of incident area. - Analyse data off-site to support accident investigation and potential criminal prosecution. Example Risk: High-definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigation: - Activate HD cameras only where necessary to record the inspection location. - Ensure drone device is visible and identifiable as being operated by the local authority when active. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

4.3.4 Taxonomy Level 3: Media, Publicity, and Entertainment

The taxonomy of Media, Publicity, and Entertainment is represented in Figure 6 and detailed in the Table 10 below:

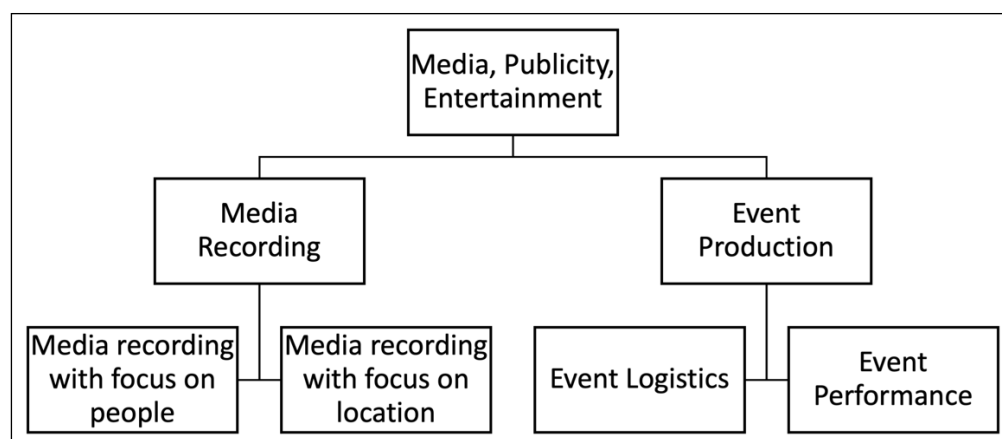


Figure 6 Media, Publicity, and Entertainment.

Table 10 Media, Publicity, and Entertainment.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Media Recording with focus on people	Use of drones to capture video, still images or footage of events or activities where the focus of the recording is an individual or a group of individuals with the intention of publication.	Acquisition of Data: Use of optical or audio sensors to record video, still images, or other audio-visual information. Acquisition of Data: High-definition video recording may capture identifiable people. Drone may overfly private homes or other private areas. There is a risk of secondary capture of personal data of bystanders if they are recorded. Example Mitigation: - Activate HD cameras only where necessary to record the people at the location and scene. - Ensure that people are aware that there will be recording taking place and ensure that individuals can “opt-out” by being able to avoid the flight path of the drone. - Ensure appropriate controls over storage and use of recordings for secondary purposes. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.

TAXONOMY LEVEL 3	DEFINITION	EXAMPLE RISKS AND MEDIATION
Media Recording with focus on location	Use of drones to capture video, still images or footage of events or activities where the focus of the recording is an individual or a group of individuals with the intention of publication.	Acquisition of Data: Use of optical or audio sensors to record video, still images, or other audio-visual information. Example Risk: Flight path of drone may overlook private homes or other private areas. There may be secondary capture of identifiable data subjects. Example Mitigation: - Plan flight plan for recording to avoid private homes where possible. - Activate HD cameras only where necessary to record the event location and scene. - Ensure that people are aware that there will be recording taking place and ensure that individuals have the ability to “opt-out” by being able to avoid the flight path of the drone. - Edit footage to remove secondary capture of individuals. - Ensure appropriate controls over storage and use of recordings for secondary purposes. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Logistics	Use of drones to provide logistics/transport support for the execution of an event or publicity activity.	Acquisition of Data: Use of GPS and drone mounted sensors to support piloting of drone to required location. Record imagery for off-site analysis, incident response review, training. Example Risk: Video sensors will capture identifiable people or may capture footage of private homes or private locations. Example Mitigation: - Use cameras only where necessary to carry out the transport activity. - Cameras should not be flown over private homes while recording. - Consider necessity of resolution of imagery for the transport purpose. - Consider the necessity of recording/retaining imagery from the specific drone. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties.
Event Performance	Use of drones to carry out a planned flight path as part of the execution of a performance activity.	Acquisition of Data: Use of GPS and drone mounted sensors to support piloting of drones in a defined flight path to execute a performance event. Example Risk: High-definition video recording will capture identifiable people. Imagery may include data relating to health if injured persons are captured. Audio sensors Example Mitigation: - Use cameras only where necessary to carry out the transport activity. - Cameras should not be flown over private homes while recording. - Consider necessity of resolution of imagery for the transport purpose. - Consider the necessity of recording/retaining imagery from the specific drone. - Ensure appropriate controls over storage and use of recordings for secondary purposes such as training and response planning. - Ensure appropriate controls to restrict disclosure/publication of recorded video to 3rd parties

5 CONCLUSION AND RECOMMENDATIONS

There is no “one size fits all” approach or template that can be applied to the deployment of drones and drone mounted sensors by local authorities. However, adopting a structured and strategic approach to assessing and planning for the responsible use of drones will enable local authorities and to quickly adopt and adapt appropriate technologies to their needs. Our contribution may serve as the starting point for this work.

By developing a taxonomy of use cases for drone-mounted sensor it will be possible to develop appropriate processes, procedures, and safeguards for the operation of drones and drone-mounted sensor technologies that is both simple to use but also supports the continued development of data protection governance in this area that can keep pace with the rapid evolution of technologies and potential scenarios for use.

For each use case scenario that is defined, a DPIA with associated controls and standard procedures to mitigate risks should be developed. These should be made available as a centralised resource. New use case scenarios should be compared against this central library of data protection impact assessments.

This will have the benefit of improving standardisation and consistency of approaches between drone users and reducing the time required to carry out DPIAs for drone operations.

Technologies such as facial recognition, ANPR, and Artificial Intelligence applications will need to be considered carefully and deliberately to ensure that their impact on data protection rights and other rights and freedoms is necessary and proportionate. This will require careful attention to the technologies being procured and deployed as often these additional analytics capabilities are acquired as a bundled by-product of procuring otherwise straightforward systems.¹⁴

Local Authorities should aim to develop these libraries of Use Case Scenarios, DPIAs, and associated safeguards as the basis of a Code of Conduct for data protection compliance in the use of drone-mounted sensors and associated technologies. Within this there should be recognition that there are use cases for drones which do not require the capture or processing of personal data at all, but even then, there is a need to 'trust but verify' through appropriate governance, controls, and transparency.

FUNDING INFORMATION

This article is an output of the Protect Project which has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 813497.

COMPETING INTERESTS

The authors have no competing interests to declare.

AUTHOR AFFILIATIONS

Joshua Hovsha  orcid.org/0000-0002-7498-2217

Marie Skłodowska-Curie Fellow in data protection Law, Trinity College Dublin, Dublin, Ireland

Daragh O'Brien

Director, Castlebridge, Dublin, Ireland

¹⁴ *Facial Recognition technology latest woe at National Children's Hospital*, Irish Times, 12th December 2019 <https://www.irishtimes.com/business/technology/facial-recognition-technology-latest-woe-at-national-childrens-hospital-1.4112451>.

TO CITE THIS ARTICLE:

Joshua Hovsha and Daragh O'Brien, 'Drone Use Cases and their Privacy Impacts: A Taxonomy' (2022) 27(1) *Tilburg Law Review* pp. 60–80.
DOI: <https://doi.org/10.5334/tilr.281>

Published: 17 February 2023

COPYRIGHT:

© 2022 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See <http://creativecommons.org/licenses/by/4.0/>.

Tilburg Law Review is a peer-reviewed open access journal published by Ubiquity Press.