European Commission

Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations

Summary for Industry

Rachel L. Finn and David Wright,
Trilateral Research & Consulting, LLP

Laura Jacques and Paul De Hert,
Vrije Universiteit Brussel

November – 2014

Trilateral Research & Consulting

Vrije Universiteit Brussel

EUROPEAN COMMISSION

Directorate-General Enterprise and Industries

Directorate G— Aerospace, Maritime, Security and Defence Industries

Unit G5— G.5 Defence, Aeronautic and maritime industries

Contact: Jean-Pierre LENTZ, Policy Officer

E-mail: Jean-Pierre.LENTZ@ec.europa.eu

European Commission

B-1049 Brussels

EUROPEAN COMMISSION

Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations

Summary for Industry

Directorate-General for Enterprise and Industries
COSME

2014

EUR [number] EN

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-79-44127-1
doi: 10.2769/964439

Printed in Belgium

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

PRINTED ON TOTALLY CHLORINE-FREE BLEACHED PAPER (TCF)

PRINTED ON RECYCLED PAPER

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

Image © Eléonore H, image # 52539663, Source: Fotolia.com

TABLE OF CONTENT

1 INTRODUCTION

The deployment of Remotely Piloted Aircraft Systems (RPAS, actually an old 20th century technology[1]) entails many benefits for European manufacturing and operating industries and citizens. The technology of RPAS applied to civil applications – commercial, non-commercial and governmental non-military – can contribute to boost industrial competitiveness, promote entrepreneurship and create new businesses in order to generate growth and jobs. Although RPAS are not new, there have been significant recent advances in their relative size, weight, the payloads they carry and, consequently, the novel and emerging applications for which they may be used. These developments, particularly in the "civil" sphere (i.e., commercial, non-commercial and government non-military), yield several potential benefits for European industry and its citizens. Specifically, the European RPAS Steering Group has argued "the emerging technology of RPAS… can contribute to boost industrial competitiveness, promote entrepreneurship and create new businesses in order to generate growth and jobs."[2]

It is already apparent that existing RPAS capabilities and applications raise a number of privacy, data protection and ethical issues, some of which are recognised in the RPAS *Roadmap*. In relation to privacy, the use of aerial surveillance technologies in Europe is covered by Article 7 (Respect for private life) and Article 8 (Data protection) of the Charter of Fundamental Rights of the European Union, 2000/C 364/01(CFREU), by the Right to respect for private life of Article 8 European Convention on Human Rights (ECHR, Rome, 4 November 1950). RPAS are also covered by the Data Protection Directive 95/46/EC (DPD 95/46). Data protection applies whenever personal data are processed, and applies during the monitoring of public or private spaces, especially if the images are recorded. The only real bottle-neck for the applicability of data protection is that the footage needs to contain *personal data*[3], that is, images of natural persons that are clear enough to lead to an identification, in order to fall under the scope of the Data Protection Directive. Consequently, any use of RPAS for visual surveillance, as well as certain other tasks, that captures members of the public and records the footage must comply with this instrument. In addition to these European legislative mechanisms, national-level legislation related to privacy and data protection might also be applicable to RPAS usage. All European countries are required to abide by the Charter of Fundamental Rights of the European Union, and they are required to transpose the Data Protection Directive into appropriate national legislation. However, privacy laws may be weaker or stronger in some countries, and the transposition of the DPD into national laws has introduced some significant differences in the data protection regimes in different countries. For example, some Member States, e.g., the Czech Republic, would only

[1] The first unmanned aircraft was used by the US Navy in WWI. Quoted from Aviation Safety Unmanned Aircraft Programme Office, 2008, in McBride, Paul, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations", *Journal of Air Law and Commerce*, Vol. 74, 2009, p. 628.

[2] European RPAS Steering Group, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, June 2013, p. 5. http://ec.europa.eu/enterprise/sectors/aerospace/uas/

[3] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007.

consider video footage that is recorded to be personal data, whilst other countries, e.g., France, would consider the monitoring of video footage without recording to include a processing of personal data. Furthermore, some countries, such as France, have CCTV legislation that is applicable to the use of RPAS, while other countries (e.g., the UK) have laws covering police surveillance operations.

Large-scale civil RPAS deployment also introduces privacy and ethical concerns including issues of safety, discrimination, a "chilling" effect and function creep. Current civil deployments of RPAS often focus on persons and groups who are already marginalised in society, thus introducing risks associated with discrimination.[4] Other ethical impacts include the potential dehumanisation of the surveilled, where the distance between the controller of the RPAS and the surveilled diminishes the sense of moral responsibility for the actions of the RPAS (i.e., "gamification of reality").[5] Additionally, conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person "to take measures to keep private those activities that they do not wish to expose to public view".[6] In contrast, RPAS, and especially small RPAS, offer no such warning. This could lead to a self-governing or "chilling" effect, where individuals believe they are being watched, even when no RPAS are in operation.[7] Finally, function creep refers to the possibility that a system originally acquired for one purpose, is expanded to fulfil additional purposes, where, for example, RPAS originally used to inspect infrastructure at a chemical plant ends up being used to film workers. Each of these ethical issues could lead to public discomfort with the use of RPAS which would need to be overcome in order to allow innovation and economic opportunities in this area.

This report will discuss each of these privacy, data protection and ethical issues. Given this framework above, this report uses the following schema in relation to privacy, data protection and ethical issues:

Privacy

- Chilling effect
- Dehumanisation of the surveilled
- Transparency and visibility, accountability and voyerism
- Function creep
- Bodily privacy
- Privacy of location and space
- Privacy of association

[4] Finn, Rachel, and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", *Computer Law & Security Review*, Vol. 28, No. 2, 2012, pp. 184-194.

[5] Wall, Tyler, and Torin Monahan, "Surveillance and violence from afar: The politics of drones and liminal security-scapes", *Theoretical Criminology*, Vol. 15, No. 3, 2011, pp. 239-254.

[6] McBride, op. cit., 2009, p. 659.

[7] Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, Vintage, New York, 1977.

Data protection

- Transparency
- Data minimisation
- Proportionality
- Purpose limitation
- Consent
- Accountability
- Data security
- Rights of access, correction and erasure
- Third country transfers

Ethical issues

- Safety
- Public dissatisfaction
- Discrimination

This specialised summary report will outline the privacy and ethical issues associated with the use of RPAS in civil air space by commercial operators (enterprises offering RPAS services), or corporate operators (enterprises using RPAS internally for their own needs, either a big company like SNCF or the self-employed like a farmer), and identify the relevant data protection legislation associated with the civil use of RPAS for industry. It is important to understand that the issues related to privacy, data protection and ethics are intentionally vague in order to ensure that they are technology neutral. This means that they can apply to RPAS, CCTV, Body scanners, etc. Furthermore, these issues are very much context dependent. While an image of the top of a person's head may not count as personal data in some circumstances and contexts, in others it would. This, plus the heterogeneity of RPAS, their payloads and their associated missions requires RPAS operators to consider each mission type independently and to gain some basic knowledge about these legislative instruments. This report provides some initial information in this regard, and provides some concrete advice. We examine five different typical RPAS scenarios relevant to commercial and professional uses. For each, we undertake a risk analysis relevant to the issues identified above and provide guidance on how these issues can be mitigated. Finally, the project has resulted in a series of policy recommendations, in consultation with a range of relevant RPAS stakeholders (e.g., Data Protection Authorities, Civil Aviation Authorities, RPAS operators and civil society organisations, etc.), to support European innovation whist protecting privacy, personal data and ethical safeguards. These guidelines and recommendations contain specific items relevant to industry, and these will be outlined in the final chapter.

The recommendations are broadly focused on two key ideas – that the RPAS industry and needs to act to minimise the risks associated with privacy, data protection and ethics, and that they need tools and expertise to assist them in doing so. Furthermore, it is important that these tools and expertise do not represent a significant additional "cost" to the RPAS industry, regulators or members of the public. This issue of cost is particularly important as the current state of affairs is unsustainable. First, the research has found that many RPAS operators are probably collecting and processing personal data. As such, they have clear obligations under current European and national laws as well as the forthcoming General Data Protection Regulation. However, many RPAS industry representatives do not appear

to be aware of these obligations and are consequently not meeting them. This places the RPAS industry, European and national policy-makers and members of the public at risk. Industry representatives are leaving themselves open to liability and penalties that could negatively impact the sector. Citizens are at risk of serious infringement of their fundamental rights. European and national policy-makers, as well as the RPAS industry, are leaving themselves open to a loss of trust by the public as a result of these infringements, which can negatively impact those stakeholders. As such, the current situation is associated with clear and serious vulnerabilities for all of the stakeholders involved.

2 RPAS TECHNOLOGY AND EUROPEAN PRIVACY AND DATA PROTECTION LAW

Currently, there are no RPAS technology specific privacy or data protection legislative instruments at national or European levels. However, two major legal issues relate to the use of RPAS technology, namely privacy laws governing observation and surveillance activities with RPAS and data protection implications resulting from the collection, storage and use of personal data collected by RPAS. Some advocate for a regulation by analogy, arguing that the existing privacy and data protection regulatory framework is enough, while others suggest the adoption of specific regulation for RPAS.[8] The European Commission seems to take an intermediary position, holding that "part of the existing regulatory framework may be applicable to the use of RPAS and the existing case law on data collection and handling may provide guidance in the drafting and implementation of regulation specific to RPAS".[9] Given this lack of clarity, the applicability, and or adaptability, of existing legislation to RPAS use require examination. In that regard, this chapter focuses on the relevant European privacy-related laws applicable to the civil use of RPAS. We provide an analysis of the principles provided by those laws through an examination of, first, the regulations governing the right to private life, and second, the relevant provision of the data protection legislation.

2.1 Privacy law

The right to privacy broad and protects the secrecy of personal information as well as the different facets related to the private sphere of each individual against intrusions form outside, including the possibility of self-determination with regard to one's body, sexual orientation, relations with others, construction of one's own identity, etc.

This right to privacy is recognised at Article 8 of the European Convention on Human Rights (ECHR), but it is regulated by the principles set up by the jurisprudence of the European Court of Human Rights (ECtHR)

The Article 8 of the ECHR provides:

[8] European RPAS Steering Group, op. cit., 2013.

[9] Hesselink, Henk, *ULTRA Unmanned Aerial Systems in European Airspace – Deliverable 3, Identification of Social Dimension*, 2013, p.58.

> *1. A person has a right to respect for their private and family life, home and communications.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Article 8 is divided into two parts. The first paragraph enunciates the precise rights that guaranteed by the State including the right to respect for private life, family life, home and correspondence[10]. The second paragraph outlines a limitation to the respect of those rights[11], providing that "it may be acceptable to interfere with Article 8 rights in certain circumstances"[12]. The analysis finds that the use of RPAS to monitor someone within this private sphere will undoubtedly interfere with the EHCR and that the EHCR may also be applied in public areas if the individual concerned could reasonably expect a certain degree of privacy.

Applied in the context of the use of RPAS technology in public space, jurisprudence related to the EHCR means that when a drone is used for simple monitoring activities (without recording), there will be no interference with Article 8 rights. Conversely, the use of RPAS in a public space for the following purposes may cause interference in breach of Article 8:

(i) when RPAS operators monitor and record data in a systematic and permanent way, regardless of whether the surveillance is covert or overt;
(ii) when RPAS operators disclose images of someone previously collected;
(iii) when RPAS operators do not record images, but monitor a public space through "sophisticated" means.

Nevertheless, this interference may be justified if the interference is for "a legitimate and foreseeable purpose", such as public security, and also if it meets the requirements set out at Article 8(2).[13] Furthermore, when government-operated civil RPAS simply monitor with "non-sophisticated means" in a surveillance context, for example through the means of a ordinary camera, they do not interfere with Article 8(1).

---

[10] Kilkelly, Ursula, *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights. Human Rights Handbook 1,* Council of Europe, Strasbourg, 2003, p. 6.

[11] De Hert Paul, "L'Article 8 CEDH", in Cécile de Terwangne (Eds.), *Le Manuel Vie privée et données à caractère personnel,* Politeia, Brussels, 2013, p. 1.

[12] Kilkelly, 2003, p. 6.

[13] Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer, Berlin, 2012, p. 39.

2.2 Data protection law

RPAS operators recording images, videos, sounds, biometric data, location data, telecommunication data related to an identified or identifiable natural person that have been collected and processed by data processing equipment embedded in RPAS technology are also subject to the application of European data protection law. The European data protection legislation establishes various obligations, restrictions and rights depending on the type of operator recording the data. For commercial RPAS operators and public authorities (excluding law enforcement bodies) using drones to capture personal data, the Data Protection Directive 95/46/EC applies. According to the Article 29 Working Party Opinion on the concept of personal data:

> Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly,….[14]

First, the Art. 29WP explains that the Data Protection Directive applies to image and sound data processed by means of CCTV and other video surveillance systems. Relevantly, biometric data, location data, and traffic data are also generally considered to be personal data.[15] Second, it also states:

> Image and sound data relate to *identified or identifiable* nature person is personal data: a) even if they are not associated with a person's particulars, b) even if they do not concern individuals whose faces have been filmed, c) irrespective of the media used.[16]

Thirdly, the Art.29 WP gives more detail on what it means by "identify someone indirectly". It explains that every day it is easier to connect different data together to identify someone through the new analytical systems, and the scope of the Directive concerns all personal data which are indirectly identifiable by "all the means likely reasonably to be used".[17] By saying that it takes into account of the possibilities of future technologies but also it narrows the broad concept of personal data. Therefore, for instance if the footage taken by an RPAS only shows the top of a person's head and you cannot identify that person without using sophisticated means, it is not a personal data. However, the same photograph is taken in the backyard of a house with additional images that may

[14] A29WP Opinion 4/2007.

[15] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP193, Brussels, 27 April 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf ("A29WP Opinion 3/2012"); Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN, WP 215, Brussels, 10 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf ("A29WP Opinion 04/2014").

[16] A29WP Opinion 4/2007.

[17] Kindt, Els J., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Springer, 2013, Dordrecht, pp. 112-113.

enable an identification of the house and/or the owner, that footage would be considered as a personal data. Thus, personal data is very much context-dependent.

Applied to the RPAS technology, the right to the protection of their personal data will only protect individuals when the RPAS has collected personal data. This differs from the right to privacy, which protects people monitored by RPAS in a systematic way or through the means of intrusive payloads regardless of whether data is collected. As stated above, the Data Protection Directive is intended to be enabling, in that it sets out the requirements for the legal processing of personal data, rather than prohibiting that processing. As such, RPAS operators who do collect personal data must respect the following rights and obligations. First of all, according to the *transparency principle*, RPAS operators should notify the data protection authority and members of the public that they plan to use RPAS that may capture personal data. Such notification must contain different information about the collector and the purposes of the data processing. Furthermore, RPAS operators, as data processors as well as sometimes data controllers, must ensure the following the data protection principles are met during the processing.

Personal data must be:

(a) processed fairly and lawfully (*lawfulness and fairness principles*);

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (*purpose limitation principle*);

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (*proportionality and data minimisation principles*);

(d) accurate and, where necessary, kept up to data (*data quality principle*);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (*retention principle*).[18]

They should also comply with the individual's rights by informing data subjects that the collection is taking place, and they must set up procedures that enable data subjects to exercise their rights to can access and rectify the information captured, and in some specific circumstances, block or erase the personal data.

Furthermore, the principles included in the Proposed General Data Protection Regulation[19] will require RPAS operators who are collecting personal data to verify that the equipment

[18] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, Article 6.

they will be using will meet the principle of privacy and data protection by design (PbD), both at the time of the determination of the means for processing and at the time of the processing itself. Additionally, RPAS operators should undertake a privacy impact assessment (PIA) to identify potentially risky collections of personal data and to identify potential means to address those risks.

Finally, although governmental RPAS operated by *law enforcement authorities* may pose some data protection challenges, they are not regulated at the European level. Similarly, *private individuals* using RPAS to capture information in a household context are not subject to any European data protection regulations. Nevertheless, although the main data protection directive excludes its application to private individuals and law enforcement bodies using RPAS, these groups must respect Article 8 of the EU Charter of Fundamental Rights, which recognises the right to data protection including the main data protection principles and individuals' rights.

3 RISK ASSESSMENT FOR TYPICAL RPAS SCENARIOS

This undertakes a privacy, data protection and ethical analysis of typical and realistic RPAS scenarios. The purpose of this examination is to link actual practices to the legal framework described above and to identify realistic risks to privacy, data protection and ethics based on information gleaned from the consultation exercises and the legal analysis in the main report. This information is used to assign a risk "level" for each issue, and is intended as a guide to assist RPAS operators in identifying what the level of risk associated with particular RPAS applications may be. The analysis focuses on five different scenarios meant to relate to typical commercial uses. These scenarios have been validated with industry associations and RPAS operators and manufacturers.

In this section, we provide a brief overview of each of the relevant privacy, data protection and ethical "risk" categories.

- A chilling effect - This refers to situations where individuals are unsure about whether they are being observed, and "attempt to adjust their behaviour accordingly".[20]
- Dehumanisation of the surveilled - This may occur when RPAS pilots are physically and psychologically removed from the act of observation or information collection, and do not consider the impacts of their activities on individuals on the ground.
- Transparency and visibility – This refers to the fact that individuals on the ground may not know an RPAS is in operation, and if they do, may be unsure about who is operating the RPAS and the purpose for which it is being used.

---

[19] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation"), 2012/0011 (COD), 25.01.2012.

[20] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of Privacy", in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, p. 16.

- Function creep - This occurs when the purposes of RPAS usage expand, either to additional operations or to additional activities within the originally envisaged operation.[21]
- Body privacy – This refers to "the right to keep body functions and body characteristics (such as genetic codes and biometrics) private".[22]
- Privacy of location and space – This "encompasses the right of individuals to move in their 'home' and other public or semi-public places without being identified, tracked or monitored".[23]
- Privacy of association – This refers to "the freedom of people to associate with others".[24]

In addition to privacy, this analysis also examines the data protection issues associated with each of these scenarios. As noted above, these data protection issues are limited to instances where "personal information", including identifiable images, is collected and processed. Practically speaking, understanding ways in which each data protection principle can be observed can also assists RPAS operators in understanding the interrelationship between some of the principles. In turn, understanding how the principle are related, enables RPAS operators to take practical steps to observe one principle that enables them to indirectly meet the requirements of another, related principle. For example, understanding how the transparency principles may be observed and taking practical steps in that regard (such as notifying individuals of the purpose of the data collection) may also satisfy the consent principle, because individuals will not be able to provide consent if they are not informed about the activity to which they are consenting. The following data protection issues will be considered for each scenario, both individually and where relevant, when there exists a relationship between the principles that assists RPAS operators to effectively discharge all of their obligations under the data protection framework:[25]

- Transparency – This principle requires that the data collector notify the data subject of the personal information collected, the purpose of that collection and use of the data, as well as details of the RPAS operator to enable the data subject to exercise their rights of access, correction and erasure. Transparency is also related to the principle of Consent in that informing the data subject of the purpose and extent of the data collection places the data subject in a position to provide "free and informed consent", which is the degree of consent required by the Data Protection Directive. Transparency is also related to the principle of purpose limitation in that

[21] Statewatch, "Commission Wants Drones Flying in European Skies by 2016", Statewatch News Online, September 2012. http://www.statewatch.org/news/2012/sep/eu-com-drones.htm

[22] Finn, et al., op. cit., 2013, p. 15.

[23] Ibid., p. 16.

[24] Ibid.

[25] Unless indicated otherwise, all quotes come from the text of the 1995 Data Protection Directive 95/46/EC.

the purpose for which the data is used reflects only that purpose that the data subject was informed about, and consented to.

- Data minimisation – Data must be "relevant" to the purpose for which it is being collected and the data collected must be the minimum amount of data necessary for the purposes pursued. Data minimisation is related to the principle of proportionality, and ensuring that data collected is minimised assists in observing the principle of data proportionality.
- Proportionality – The data must not be "excessive in relation to the purposes for which they are collected and/or further processed" and data collectors must assess whether they are using the least intrusive means to collect the data required.
- Purpose limitation – The collector must "specify the purpose of the collection and process the data collected only for purposes compatible with that collection".[26] Purpose limitation is related to the principles of transparency and consent, as set out above.
- Consent – Individuals must give consent to their data being collected, either though explicit consent, or by entering public spaces where they have been informed that data collection is taking place. Consent is closely related to the principle of transparency in the manner outlined above.
- Accountability – This refers to the fact that the data controller must be identifiable and accountable to individuals and regulatory authorities. It requires data controllers to make themselves known to individuals and authorities in order to enable individuals to exercise their rights and to enable authorities to pursue investigations. Thus, Accountability is related to transparency.
- Rights of access, correction and erasure – This ensures that individuals retain control over the information that is collected about them. This is related to the principle of transparency by which data subjects are made aware of their rights in this regard.
- Data security – This refers to the fact that data controllers are obligated to ensure that personal data are stored and processed securely and protected from inadvertent disclosure and unlawful intrusion.
- Third country transfers – Data controllers must ensure that any country to which personal data are transferred has an "adequate" level of data protection regime. This requires the data controller to have secure and total control over the data collected, and also understand which third countries that the European commission has deemed not to offer "adequate protection."

In practical terms, an understanding of the data protection principles provide RPAS operators with separate opportunities to address the risks posed to privacy and data protection when employing RPAS.

Finally, the analysis examines ethical issues related to the scenarios. These include:

[26] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, Brussels, 2 April 2013, pp. 4-5. http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf ("A29WP Opinion 03/2013").

- Safety – This refers to the possibility that living things or buildings could be harmed or damaged by crashes or other negative impacts (e.g., noise) associated with RPAS use.
- Public dissatisfaction – This refers to the possibility that people could become disillusioned with RPAS use based on the possibility that they are compromising safety or privacy and data protection rights.
- Discriminatory targeting – This refers to the fact that RPAS use (and the potential safety, privacy and data protection impacts) may be more prevalent in relation to certain populations or areas which are less likely to be able to effectively voice or act upon those concerns (e.g., marginalised populations or areas).

The analyses that follow examine each of these issues in relation to the scenarios presented. For each medium or high risk, we detail the reasons we have made this determination and describe steps to mitigate the risk. While it is not possible for this report to consider all of the potential infringements associated with RPAS, especially as RPAS capabilities and applications expand, it is meant to act as a starting point to assist detailed a consideration of potential RPAS impacts in order to facilitate responsible and informed RPAS operations.

3.1 Commercial operators

As evidenced by the consultation exercises with industry, the use of RPAS by commercial operators is primarily focused on infrastructure inspection, mapping, earth observation, precision agriculture and other, creative services. Commercial operators are bound by privacy laws via the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights, as well as the Data Protection Directive and the privacy and data protection legislation of the Member States in which they are operating. Furthermore, they will be subject to obligations under the General Data Protection Regulation when the European Commission enacts it. However, the applicability of these measures are dependent upon the types of data collected via the target of the mission and the equipment that is utilised.

3.1.1 Infrastructure inspection

One of the most common current missions associated with RPAS is their use for infrastructure inspection. A typical scenario for such infrastructure inspections is the following:

An RPAS operator is charged with inspecting a mobile phone tower in a rural location that provides mobile phone coverage to a few homes in the area and drivers on the near-by highway. The RPAS is fitted with a high-definition video camera, which the operator tests by scanning the landscape and taking a few close-up images of the base of the tower. Satisfied that the images are of sufficient quality for later analysis and can be enhanced to provide close-up footage of cracks or damage, the operator begins his inspection. As the RPAS ascends into the air, the operator circles the mast, moving steadily upwards. The video footage is focused on the mast, but the landscape behind the mast is visible in the shot as he makes his way around the mast and higher into the air. Although the operator and the mobile phone provider are not interested in the farms or vehicles in the background, (often blurry) images of these are captured and included in the footage provided to the mobile phone company and saved in the RPAS operator's archives.

This scenario may result in the collection of personal data about individuals living near the mast, individuals passing by and the employees who may be captured by the footage. While the footage of people may be restricted to "the tops of people's heads", once these images are contextualised by particular landmarks or other information, they may become identifiable. For example, if there is only one farm near a mast, and there is only one individual with brown hair who frequents the farm. In addition, individuals passing on the highway may be identifiable if the footage includes images of their number plates, which can be linked to their personal information. However, one industry respondent from the consultation exercises has pointed out that such background images are likely to be "blurry". Nevertheless, the potential impacts are considered below.

The privacy issues associated with these usages of RPAS fall under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

Privacy issue	Risk level	Steps to be taken
Chilling effect Individuals are unsure about whether an RPAS is in operation, or are unsure as to what a visible RPAS can see, whether it is recording and the purpose for which it is being used. This could lead individuals to adjust their behaviour.	Medium	Notification
Dehumanisation of the surveilled The fact that the RPAS operator is not interested in individuals on the ground may lead him/her to discount the potential impact of the RPAS operation on such individuals.	Medium	Impact assessment
Transparency and voyeurism Lack of information could create significant discomfort and public backlash around the use of RPAS for such operations.	High	Notification
Function creep The communications company, as well as other clients, may be interested in the information that is captured in the background. This would expand the purpose for which the RPAS is being used.	Medium	Data minimisation (blurring or anonymisation)
Body privacy	Very low	
Privacy of location and space	Low	
Privacy of association	Very low	

In this scenario, personal data may be collected inadvertently through the normal operation of the RPAS when scanning the landscape to ensure the camera is working properly (if

these images are recorded) and while capturing images of buildings, cars, etc. in the background during the mast inspection. While many of the images inadvertently captured in the background will be blurry (due to the focus on the mast), those familiar with the area and/or familiar with the individuals who may be in the vicinity may be able to identify them. Therefore, in relation to data protection, the scenario is associated the following risk levels:

Data protection issue	**Risk level**	**Steps to be taken**
Transparency It is not clear whether the RPAS operator or the communications company has alerted individuals on the ground that personal data may be collected, or whether the RPAS itself has markings on it to identify the data collector.	Medium	Notification
Data minimisation It is not clear whether the RPAS operator has taken specific steps to minimise the amount of data collected during the operation.	Medium	Data minimisation (delay recording, blur or anonymise images)
Proportionality In this scenario, a less intrusive technology could be used to collect the data in question, and the use of an RPAS for this purpose might be disproportionate.	Medium	Consider alternative means of data collection
Purpose limitation		
Consent Individuals in the vicinity would not have the opportunity to consent to the collection of their personal data.	Medium	Notification
Accountability Lack of notification means that the RPAS company is not accountable for their actions.	Medium	Notification and company logo on the RPAS
Data security	Low	
Third country transfers	Low	
Rights of access, correction and erasure If individuals are not aware who is operating the RPAS, then it is nearly impossible for them to be able to exercise their rights.	Medium	Notification

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium risk. If individuals are not aware who is operating the RPAS, then it is nearly impossible for them to be able to exercise this right. Adequately addressing transparency and accountability as detailed above would be a necessary step forward in meeting this obligation.

Finally, in addition to these privacy and data protection issues, ethical issues such as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario.

Ethical issue	Risk level	Steps to be taken
Safety	Low	
Public dissatisfaction As with any RPAS operation, the use of RPAS for infrastructure inspection may contribute to members of the public feeling "over-run" by RPAS.	Medium	Impact assessment and notification
Discriminatory targeting	Low	

The use of RPAS for infrastructure inspection is associated with relatively few serious privacy, data protection and ethical risks. These missions are focused on objects, rather than people, and may only collect personal information inadvertently or in unusual circumstances. However, it is important that RPAS operators educate themselves and members of the public about their use of RPAS and the images they collect, and provide specific information about when RPAS are being used and the purpose for which they are being used. RPAS operators should also consider privacy enhancement and data minimisation practices like blurring irrelevant images or limiting their recording to images essential for the mission. These simple activities will assist RPAS operators in meeting privacy expectations, meeting data protection obligations (where they collect personal information) and meeting ethical standards, particularly in combatting public discomfort with RPAS.

3.1.2 Other visual services

Infrastructure inspection is largely focused on an object or piece of property but may collect images of people inadvertently. Other visual services, which use the same payloads and technologies as infrastructure inspection, are being commissioned in situations that are very likely to collect images of people or personal data. These may include services such as real estate showcasing, stock image production and the production of footage for publicity purposes.

An RPAS operator is contracted by a real estate company to make a video showcasing a home for sale. The operator flies about 200m above the house, filming the building, the land included with the sale and the immediate surrounding neighbourhood. The left neighbour's car and toys in their back yard are clearly visible, as is the right-side neighbour walking from her front door to her car. The

RPAS operator transfers the footage to the real estate client and does not keep a copy.

In this scenario, the RPAS operator is in a similar position to the infrastructure inspection scenario whereby the operator is not concerned about the neighbours or capturing footage of individuals on the ground. Instead, the operator is focused on the house that is for sale. However, due to the fact that this operation is occurring in a residential area, and will include footage of neighbours and their property, it raises more significant risks than the infrastructure inspection scenario. As such, the operator has a clear obligation to reduce the risks to privacy and personal data of the people and private properties that may be captured on the footage, and the operator has a clear obligation to meet the data protection requirements associated with the collection and processing of these images. However, the fact that the RPAS operator does not keep a copy of the footage means that the operator is only liable for the risks associated with the collection and processing of the data in question.

The privacy issues associated with this usage of RPAS falls under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

Privacy issue	Risk level	Steps to be taken
Chilling effect Individuals are unsure about whether an RPAS is in operation, or are unsure as to what a visible RPAS can see, whether it is recording and the purpose for which it is being used. This could lead individuals to adjust their behaviour.	Medium	Notification
Dehumanisation of the surveilled The fact that the RPAS operator is not interested in individuals on the ground may lead him/her to discount the potential impact of the RPAS operation on such individuals	High	Impact assessment
Transparency and voyeurism Lack of information could create significant discomfort and public backlash around the use of RPAS for such operations	High	Notification
Function creep There is a risk that the footage could be used to "scope out" neighbourhoods to identify targets for theft.	Medium	Data minimisation (blurring or anonymisation)
Body privacy	Very low	

Privacy of location and space There is a significant intrusion on privacy of location and space in that individuals' private spaces (e.g., yards and gardens) are recorded	High	Data minimisation (blurring or anonymisation)
Privacy of association The footage may indicate the number of adults living in a house (based on the number of vehicles) the relationships between those people (e.g., family groups) and other information about those individuals.	Medium	Data minimisation

In addition to these privacy risks, there are clear risks associated with the protection of the personal data in this scenario. Furthermore, this scenario indicates a situation where *RPAS operators are legally obligated to address the following data protection issues* as they are very likely to collect and process personal data.

Data protection issue	Risk level	Steps to be taken
Transparency It is not clear whether the RPAS operator or the communications company has alerted individuals on the ground that personal data may be collected, or whether the RPAS itself has markings on it to identify the data collector.	Medium	Notification
Data minimisation This scenario clearly involves the collection of images that are extraneous for the purpose of showcasing the property in question, e.g., images of neighbours, their homes and their property. However, the fact that the RPAS operator does not store a copy of the data is a useful data minimisation feature.	High	Data minimisation (blur or anonymise images)
Proportionality It seems clear that a less intrusive technology (e.g., still camera footage from the ground) could be used to collect the data in question.	High	Consider alternative means of data collection
Purpose limitation	Low	
Consent Individuals in the vicinity would not have the opportunity to consent to the collection of their personal data without	High	Notification

adequate notification.		
Accountability Without transparency or obtaining consent from residents and neighbours of the area, it is almost impossible for the RPAS operator to meet his obligations around accountability.	Medium	Notification and company logo on the RPAS
Data security	Low	
Third country transfers	Low	
Rights of access, correction and erasure If individuals are not aware who is operating the RPAS, then it is nearly impossible for them to be able to exercise their rights.	Medium	Notification

Therefore, RPAS operators may potentially breach a number of requirements of the data protection framework by failing to observe a number of the data protection principles. RPAS operators are at a high risk of compromising the principles of data minimisation, proportionality and consent. There is also some risk that RPAS operators may breach the related principles of transparency, accountability and rights of access, correction and erasure, there is less risk of this occurring during this scenario, and even less risk that the principles of data security and third party transfers will be compromised.

In addition to these privacy and data protection issues, ethical issues such as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario. In general, these are low to medium risks, as the operation is not focussed on people. However, the operation could inadvertently jeopardise the safety of property or local residents, but only to the extent that the equipment malfunctions. However, the operation does contribute to a general proliferation of RPAS, which may be viewed negatively by the public, especially as this operation is undertaken in a residential area comprising private properties.

Ethical issue	Risk level	Steps to be taken
Safety Mission in a residential area could raise safety issues in relation to people or property.	Medium	Impact assessment
Public dissatisfaction If residents feel that they are under surveillance (even though they are not), there is a significant risk to public satisfaction.	Medium	Impact assessment Notification
Discriminatory targeting	Low	

Therefore, this scenario does not present any serious ethical risks. Nonetheless, the operators must still inform the residents and surrounding neighbours of the operation. They must also operate with great caution given the close proximity to objects and people, not only so as not to be of nuisance, but to ensure that they do not inflict any damage to the property, objects around the property and neighbouring properties, and importantly, people that may be appear unpredictably.

Overall, the use of RPAS in this situation presents some risks to privacy, data protection and ethical risks. However, these are not serious risks as the operation is focussed on real estate, and the surrounding land, rather than people. Nevertheless, there is a chance that this operation could impact unintentionally or indirectly upon civilian rights and values, especially as individuals are inadvertently captured in the footage, as are their homes and other neighbourhood characteristics that could lead to the identification of residents. However, these risks can be minimised by the real estate agency and the RPAS operator notifying the residents of the intended operation in advance. They could also inform residents of the purpose of the operation, the images to be captured, and the subsequent use of the footage. The agency and the operator could also make the images of individuals unidentifiable by blurring them, and doing the same with any house numbers or car number plates. Alternatively, the RPAS operator could erase the footage of the individuals that was inadvertently captured, as this footage is not imperative to the overall operation. Such steps are significant in reducing the risk to privacy, data protection rights and ethical values. This proactive approach is more favourable than the operator simply relying on an intention not to retain a copy of the footage, as the scenario stipulates.

The organisers of an outdoor concert have contracted a drone operator to fly above the concert taking footage of people in the crowd enjoying themselves. Attendees of the event were informed of the filming via a short notification in the terms and conditions statement when they bought their tickets online.

In this scenario, the RPAS operator is concerned primarily with capturing footage of individuals and as a result raises a number of concerns relating to privacy, data protection and ethical values. Specifically, the footage includes images and location information for identifiable individuals as well as information about their social behaviours and associations. However, due to the fact that this operation is occurring in a public space, and the attendees have been notified prior to their attendance at the concert, these risks are reduced somewhat by the operator discharging some of their obligations and data protection requirements to reduce the risks to privacy and personal data of the people at the concert. However, the extent to which the footage will be used, whether the operator and the organisers intend on keeping a copy of the footage are not presented in this scenario, but if this is the case, then the risks are increased.

The privacy issues associated with this usage of RPAS falls under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

Privacy issue	Risk level	Steps to be taken
Chilling effect	Low	

Dehumanisation of the surveilled The fact that the RPAS operator may discount the potential impact of the RPAS operation on such individuals.	Medium	Impact assessment
Transparency and voyeurism	Low	
Function creep If such footage was made generally available on the Internet, there is a risk that it could be re-used and shared widely	Medium	Data minimisation (blurring or anonymisation) Impact assessment
Body privacy	Very low	
Privacy of location and space	Low	
Privacy of association The footage can directly link individuals to their social preferences, such as type of music and the company they keep whilst in attendance, including their relationships and friendships.	Medium	Data minimisation

In this scenario, there are some risks to privacy, although for the most part, they are medium or low-level risks. The main risk is to privacy of association, although the attendees are made aware of the intended RPAS operation prior to the concert, so they can elect not to attend. Limiting or minimising the detail of images and the duration of images of individuals could significantly reduce any risks. This may include flying at a higher altitude to ensure less focussed data is collected.

In addition to these privacy risks, there are clear risks associated with the protection of the personal data in this scenario. Furthermore, this scenario indicates a situation where *RPAS operators are legally obligated to address the following data protection issues* as they intend to collect and process personal data.

Data protection issue	Risk level	Steps to be taken
Transparency Statement in the terms and conditions represents good practice; however people often ignore these.	Medium	Notification at the site
Data minimisation	Low	

Proportionality The use of the vantage point offered by the RPAS introduces unnecessary risks to the RPAS operator and concert organisers in terms of liability and obligations. However, these risks are reduced due to the fact that the organiser and operator have attempted to notify the attendees of the operation.	Medium	Consider alternative means of data collection
Purpose limitation It is likely that the footage will be posted on the Internet and used for purposes other than the initial purpose of the collection.	High	Impact assessment Data minimisation
Consent Statement in the terms and conditions represents good practice; however people often ignore these.	Medium	Notification at the site
Accountability	Low	
Data security	Low	
Third country transfers	Low	
Rights of access, correction and erasure Individuals were made aware of the information collection, although they likely did not read the statement. Nevertheless, they can approach the concert organisers with any queries.	Medium	Notification at the site

Therefore, the RPAS operator and concert organisers may potentially breach a number of requirements of the data protection framework by failing to observe a number of the data protection principles. RPAS operators are at a medium or high risk of compromising the principles of transparency, proportionality, purpose limitation, third country transfers, consent and the rights of access, correction and erasures respectively. There is less risk of a breach of data security and data minimisation presented by this scenario. However, this depends largely upon the extent of transparency, and consent.

In addition to these privacy and data protection issues, ethical issues such as safety, public dissatisfaction and discriminatory targeting pose a medium or medium to high risk in this scenario. In general, these risks are increased because the RPAS operation is being conducted at a crowded event, and the operation is specifically focussed on people. The operation in this scenario also contribute to a general proliferation of RPAS, which may be viewed negatively by the public, especially as this is a social event, at which attendees are presumably wishing to feel a sense of freedom to enjoy themselves.

Ethical issue	Risk level	Steps to be taken
Safety Mission over a crowd raises high risks in relation to safety.	High	Impact assessment
Public dissatisfaction If concert-goers feel that they are under surveillance (even though they are not), there is a significant risk to public satisfaction.	Medium	Impact assessment and notification
Discriminatory targeting	Low	

Therefore, ethical risks such as safety, public dissatisfaction and discriminatory targeting arise in relation to this situation where the primary aim of the RPAS operation is to capture individuals. However, these risks can be mitigated when the RPAS operator takes steps to reduce any noise or physical disruption caused by the presence of RPAS at the concert.

Overall, the privacy, data protection and ethical risks associated with the use of RPAS in this situation are increased due to the fact that the purpose of the operation is to capture images of individuals, which amounts to personal data under the data protection framework. Although the organiser has taken a valuable step in minimising these risks by purporting to notify attendees of the RPAS operation by including it in the terms and conditions of the tickets, the event organisers and the RPAS operator are required to take additional steps to reduce the threat of privacy and ethical risks and meet their obligations under the data protection framework. Additional steps would be to ensure that attendees are better informed of the intended RPAS operation prior to purchasing the ticket so that they may provide informed consent or assess whether they wish to be captured on the footage. The organiser and RPAS operator could also focus on achieving greater transparency and accountability, as well as minimising other associated risks, by clearly signing the event before the entrance and throughout the grounds. Recommended signage would include detail about the purpose of the collection, the intended use and manner in which the data will be secured, as well as the contact details of the RPAS operator. The attendees must also be given the right to access, correct and erase the personal data collected during this operation. Such steps are significant in reducing the risk to privacy, data protection rights and ethical values.

A commercial RPAS operator flies high over a historical city taking footage of various landmarks. The footage focuses in on the ruins of a castle, a park and the picturesque marina. Because of the height of the RPAS, the images of the people on film appear to be unidentifiable. The RPAS operator sells the image to a stock image database/catalogue, where it is stored indefinitely and made available for purchase by other entities.

This scenario results in the collection of data about individuals living, working, or simply being near the castle, and the marina at the time of filming. However, whether it amounts to personal data is disputable on the basis that the individuals captured in the footage are said to be unidentifiable. Nevertheless, once these images are contextualised by particular

landmarks or other information, or are capable of being zoomed in, individuals may become identifiable. For example, if there is only one other house located near the castle and only one blonde person that frequents that house, or if there is a particularly notable boat moored at the marina that can be connected to a certain individual. In addition, individuals driving through the city may be identifiable if the footage includes images of their number plates, which can be linked to their personal information. Although these images are likely to be blurry, and said to be unidentifiable, it is still important to consider the potential impacts below.

The privacy issues associated with these usages of RPAS fall under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

Privacy issue	Risk level	Steps to be taken
Chilling effect Individuals who live near, travel past or encounter these sights might adjust their behaviour as though they are under surveillance, even when they are not being monitored.	Medium	Notification
Dehumanisation of the surveilled	Low	
Transparency and voyeurism Lack of information could create significant discomfort and public backlash around the use of RPAS for such operations	Medium	Notification
Function creep The fact that that the footage is sold to a stock image database/ catalogue, where it is stored indefinitely and made available for purchase by other entities, without any apparent restriction, can have potential effects on individuals captured in the footage.	High	Data minimisation (blurring or anonymisation) Impact assessment
Body privacy	Very low	
Privacy of location and space	Low	
Privacy of association	Very low	

Overall, in this scenario, personal data may be collected inadvertently through the normal operation of the RPAS when scanning the historical city, the castle ruins and the picturesque marina. While individuals captured in this footage are said to be unidentifiable, those familiar with the area and/or familiar with the individuals who may be in the vicinity may be able to identify them, but this is only likely if they are able to zoom in the images. For example, a yacht club at the marina may be able to able to identify their employees,

but only with great effort. Nevertheless, if persons or vehicles are captured on the footage, the data collected by the RPAS operator and stored by the operator and by the owner of the stock image database/ catalogue should consider the these aspects of the footage to be personal data, that could, however slight a chance, lead, either directly or indirectly, to the identification of those persons. Therefore, in relation to data protection, the scenario is associated the following risk levels:

Data protection issue	Risk level	Steps to be taken
Transparency It is not clear whether the RPAS operator has alerted individuals on the ground that personal data may be collected and stored, or whether the RPAS has markings on it to identify the data collector.	Medium	Notification
Data minimisation The altitude likely makes the images unidentifiable, but the RPAS operator could data additional steps to ensure the images of persons are unidentifiable.	Medium	Data minimisation (delay recording, blur or anonymise images)
Proportionality A less intrusive technology could likely be used to capture the images of the city, the castle ruins and the marina. However, these risks are reduced due to the fact that the RPAS is flying at a great height.	Medium	Consider alternative means of data collection
Purpose limitation	Low	
Consent Individuals in the vicinity may not be aware that RPAS are in operation, and thus would not have the opportunity to consent to the collection of their personal data. However, individuals do not often expect privacy in public space.	Medium	Notification Data minimisation (blur or anonymise images)
Accountability It is unclear whether the RPAS operator informed members of the public that the filming would be taking place. Thus, it would be difficult to hold the operator accountable for his actions.	Medium	Notification Data minimisation (blur or anonymise images)
Data security	High	Improved data security

The purpose of collecting the footage is to sell it to third parties, and it is not clear whether the RPAS operator or the image stock company will store the footage in a secure manner.		measures
Third country transfers It is unclear where the stock image database/ catalogue is located, there is a good chance that it is supported by cloud technology, which presents a high risk of the data being moved around to multiple locations.	Medium	Impact assessment Data minimisation (blur or anonymise images)
Rights of access, correction and erasure If individuals are not aware that their data is being collected and who is operating the RPAS, then it is nearly impossible for them to be able to exercise this right.	Medium	Notification Data minimisation (blur or anonymise images)

The data protection analysis of this scenario indicates that there are some relatively significant risks to data protection when using RPAS to record images of the historical city, the castle ruins and the picturesque marina. This is largely because the RPAS operator, whilst not interested in individuals, has captured individuals. The sale of these images will likely rest on the quality of the images of the city, the castle ruins and the marina. However, the risks that are posed in this scenario can be mitigated by simply meeting the transparency requirement, and anonymising the pictures of the individuals to ensure that they cannot be identified through utilising zoom features.

Finally, in addition to these privacy and data protection issues, ethical issues such as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario. There are various degrees of risk raised by this scenario because the RPAS is operating at a great height, and is not focused on people. However, the operation does contribute to a general proliferation of RPAS, which may be viewed negatively by the public, which presents the highest ethical risk in this scenario.

Ethical issue	Risk level	Steps to be taken
Safety	Low	
Public dissatisfaction If members of the public feel that they are under surveillance (even though they are not), there is a significant risk to public satisfaction.	Medium	Impact assessment and notification

Discriminatory targeting	Low	

The use of RPAS for capturing images of a historical city, castle ruins and a marina, particularly when the individuals inadvertently captured in that footage are unidentifiable due to the height at which the RPAS are operated, is associated with relatively few serious privacy, data protection and ethical risks. These missions are focused on objects, rather than people, and may only collect personal information inadvertently. Nevertheless, great care is still required to ensure that any additional minimisation techniques can be applied to better guarantee that the individuals remain unidentifiable. The transparency requirement can also be met by erecting signage around the city and by notify the managers of the castle ruins so that they can alert visitors to the ruins. Other risks presented by this scenario are related to the sale of the images to the stock image database/ catalogue for what appears to be unrestricted purchase for an indefinite period of time. This use poses more serious risks. It remains important that RPAS operators educate themselves and members of the public about their use of RPAS and the images they collect, and provide specific information about when RPAS are being used and the purpose for which they are being used. RPAS operators should also consider privacy enhancement and data minimisation practices as mentioned above, such as blurring irrelevant images or limiting their recording to images essential for the mission. These simple activities will assist RPAS operators in meeting privacy expectations, meeting data protection obligations (where they collect personal information) and meeting ethical standards, particularly in combatting public discomfort with RPAS.

3.1.3 Novel services

The potential missions for that which RPAS may be used are expected to expand. Some of these new services may involve novel payloads and may include the collection of data about people. A typical scenario for such new services is the following:

> *An energy company uses a commercial RPAS equipped with a GPS sensor and a thermal camera to film houses and other buildings in several residential areas. Using the information collected from the thermal camera, the energy provider identifies a number of homes and businesses with poor insulation. The energy company then uses the GPS coordinates to match the thermal data with individual customers' addresses. This information is used to send out discount offers on roof insulation under the auspices of meeting national carbon reduction targets.*

The privacy, ethical and data protection issues associated with this scenario are unique in that they are using "sophisticated means" such as thermal imaging cameras to conduct the operation. In the USA, at least, such "sophisticated means" when used by police would likely result in the mission being deemed a "search", with specific, associated judicial processes and oversight. In Europe, the use of thermal imaging cameras mounted on a drone would likely be qualified by the ECtHR as "hard surveillance" due to the more privacy-intrusive character of such technology. Accordingly, States shall apply the requirements figuring at Article 8§2 of the European Convention of Human Rights more

strictly. This may occur through the monitoring being deemed necessary for "economic well-being of the country" or through compliance with national carbon reduction targets (i.e., through the protection of health or other national laws).[27] Furthermore, the scenario presents a situation where the non-personal data collected is linked with personal information, and results in RPAS operators possibly having a lot of detailed information about the home and its inhabitants. However, it is worth noting that the operation is not focused on collecting personal information via the thermal images, instead it is focused on the buildings in question. As such, it is only an irresponsible operator that would attempt to review the footage in order to find out information about the specific individuals inside the houses. This section analyses the possible privacy, data protection and ethical risks associated with this particular scenario, with special attention to the thermal imaging and the data linking elements of the mission.

The privacy issues associated with this scenario are primarily focused on transparency and function creep as well as the dehumanisation of the surveilled, privacy of location and space and privacy of association. The risks associated with a chilling effect and body privacy are significantly lower.

Privacy issue	Risk level	Steps to be taken
Chilling effect	Low	
Dehumanisation of the surveilled The energy company undertaking these activities is not interested in what the thermal images reveal about people However, this operation has the potential to make many people uncomfortable with the thermal images collected.	Medium	Notification Impact assessment
Transparency and voyeurism Without some sort of prior notification, individuals would not be aware that an RPAS is collecting thermal images of their homes, and that this information is intended to be linked with their names and addresses.	High	Notification
Function creep This is primarily associated with the use of sophisticated means to achieve the mission in question.	High	Impact assessment
Body privacy	Low	

[27] Council of Europe, European Convention on Human Rights, Rome, .04.11.1950, Article 8.

Privacy of location and space The images collected by the thermal camera may identify the number of people in the home and could indicate the activities in which they are engaged.	Medium	Impact assessment
Privacy of association The thermal images collected could indicate the number of people in the home, and provide clues as to their relationships. For example, thermal images of two people in one upstairs room, with single individuals in adjacent rooms may indicate a family with two children.	Medium	Impact assessment

In addition to these privacy issues, the use of RPAS fitted with thermal imaging cameras, and the linking of that data to occupiers' names and addresses, also raises significant risks in relation to data protection obligations. As above, while the collection of thermal images is not necessarily personal data, the images become personal data once they are linked with the names and addresses. Furthermore, the names and addresses themselves are also personal data. Therefore, the energy company must comply with all of their obligations under the Data Protection Directive.

Data protection issue	Risk level	Steps to be taken
Transparency It is not clear whether the energy company has alerted individuals within the homes and businesses that personal data will be collected, i.e., that thermal images will be attached to their account details. Furthermore, it is not clear whether the RPAS itself has markings on it to identify the data collector.	High	Notification and company logo on the RPAS
Data minimisation It is not clear whether the energy company has taken specific steps to minimise the amount of data collected during the operation, e.g., data about those who are not their customers.	Medium	Data minimisation (selective recording, blur or anonymise images)
Proportionality A less intrusive technology could certainly be used to sell home insulation.	High	Consider alternative means of data collection
Purpose limitation	Low	
Consent Individuals would have to give specific and informed consent	High	Notification Opt-in

for this operation to take place, especially as this scenario raises issues associated with unsolicited marketing.		mechanism
Accountability It is unclear whether the RPAS operator informed members of the public that the filming would be taking place. Thus, it would be difficult to hold the operator accountable for his actions.	Medium	Notification
Data security	Low	
Third country transfers	Low	
Rights of access, correction and erasure If individuals are not aware that their data is being collected and who is operating the RPAS, then it is nearly impossible for them to be able to exercise this right.	Medium	Notification

In this scenario, consent and proportionality emerge as significant data protection risks. The principle of consent is of particular importance as the operation would likely be classed as unsolicited marketing, and prior, informed and explicit consent would be necessary. Furthermore, due to the proportionality principle, a general consent to direct marketing would likely be insufficient to meet the consent obligations. Therefore, the energy company could ensure that it is meeting all of their data protection obligations (including transparency, accountability and data subjects' rights) by writing to customers, informing them of the service being offered, of their rights, and inviting them to opt-in to the thermal imaging data collection.

Finally, in addition to these privacy and data protection impacts, the scenario raises the following ethical risks:

Ethical issue	Risk level	Steps to be taken
Safety The operation is occurring in a populated area with many homes and businesses in the vicinity. Therefore, there is a significant risk that if the RPAS were to crash, it would threaten the safety of people and animals or could damage property.	Medium	Impact assessment
Public dissatisfaction If members of the public feel that they are under surveillance (even though they are not), there is a significant risk to public satisfaction.	Medium	Impact assessment Notification

Discriminatory targeting There is some likelihood that this operation would target homes in economically deprived areas, as occupiers of homes and businesses in these areas are less likely to be able to afford insulation and other home improvement products and services. As such, these operations could be more common in deprived areas.	Medium	Impact assessment Notification Opt-in mechanism

Unlike the infrastructure inspection scenario, the fact that this RPAS operation is occurring in populated areas and is focused on people's homes means that the ethical issues are more significant. There is some danger to public safety, given the fact that the RPAS is operating in a populated area. In addition, there are significant risks to public satisfaction with RPAS, given the linking of the RPAS information with personal data. Finally, it is also more likely that disadvantaged areas and populations would be disproportionately impacted by these information collection and linking processes.

This scenario is occurring in areas with a high population density, it is focused on homes and businesses and it is specifically seeking to link the thermal images collected to the personal data of energy customers. As such it raises significant privacy, data protection and ethical risks. Any company wishing to use an RPAS for such purposes should prioritise the assessment of the risks involved in this operation (including the risks to their business via potential public dissatisfaction with the operation). They may also wish to contact their national data protection authority to seek advice about mitigating these risks. However, in this situation the energy company, as the data controller must meet obligations surrounding privacy (in relation to the use of "sophisticated means"), data protection (specifically, transparency, explicit consent, data minimisation and proportionality) and safety issues surrounding the use of RPAS in populated areas.

This analysis has identified a number of privacy, data protection and ethical impacts associated with typical scenarios for commercial RPAS operators. These potential impacts range from very low to high risks, and are largely depending on two factors. First are characteristics specifically associated with RPAS, including the ability to fly and collect information almost undetectably and the ability to access spaces that are difficult for humans or traditional technologies to access. Second are characteristics associated with the payload and type of data collected by the RPAS, including visual images, thermal images, sounds, location data and others. Given these two factors and the associated heterogeneity of RPAS capabilities and applications, the potential risks associated with RPAS are difficult to pin down and categorise in a comprehensive way. Instead, they vary depending on the purpose for which the RPAS is being used, the types of data collected and the mission undertaken by the operators. Furthermore, as RPAS capabilities and applications proliferate, future risks are difficult to predict.

The next chapter outlines some specific policy recommendations to assist the RPAS industry in reducing their risks and liabilities in terms of privacy, data protection and ethics as well as meeting their obligations in each of these areas. This analysis has, however, indicated some clear directions. First, all RPAS operators should offer members of the public clear and detailed information about the operation of RPAS in their area, the purposes for which it is being used and the identity of the operator. This transparency activity will assist RPAS operators in meeting and addressing many of the potential risks

associated with RPAS, including transparency, a chilling effect, function creep, consent, accountability and enabling members of the public to exercise their rights. Second, RPAS operators should consider the risks posed by their missions on a case-by-case basis, as even missions using similar technologies can raise different risks, depending on the context. One possibility, discussed in detail in the next chapter, is the use of privacy impact assessments to assist in such a risk analysis.

4 GOOD PRACTICE RECOMMENDATIONS

The research project into the potential privacy, data protection and ethical issues associated with remotely piloted aircraft systems culminates in a series of recommendations to assist European policy-makers and industry in ensuring that the civil deployment of RPAS respects these issues. These recommendations also stem from two technical and legal premises. First, technologically speaking, RPAS are complex machines with diverse capabilities and a multitude of potential applications in a dynamic sector. Therefore, an over-arching framework for their regulation by a centralised, European authority would be necessarily inadequate and almost immediately obsolete. Second, the recommendations are built on the finding that definitions of personal data vary between different Member States, between different experts and certainly between different contexts of data collection and processing. Furthermore, the relationship between RPAS and the protection of privacy and personal data is best analysed using notions of risk, rather than applicability. For example, the collection of blurry images in one context may result in a negligible risk to privacy and data protection, while in another context they might represent a medium or high risk. Consider the distinction between the collection of blurry images of a person in their yard in the infrastructure inspection scenario with the collection of blurry images in the image bank scenario. One represents a medium risk to data protection, whilst the other represents a very low risk, but in both cases, data protection laws are applicable. Furthermore, risks to privacy are engendered whether an RPAS is collecting personal data or not, as privacy can be infringed simply by feeling discomfort with the presence of an RPAS. Given this complex interaction, these recommendations are broadly focused on two key ideas – providing recommendations on how the RPAS industry and other stakeholders might minimise these risks and providing tools and expertise to ensure that these risks are identified early and do not represent an additional "cost" to the RPAS industry, regulators or members of the public.

4.1 The recommendations

Overall, the policy recommendations focus on action items and soft law measures, rather than specific changes to European and national legislation, given the issues associated with risk and the need to ensure that any measures are technologically neutral to account for RPAS heterogeneity. In particular, they are organised under five main headings:

- Industry-specific recommendations for reducing risk
- Raising awareness of privacy and data protection requirements in the RPAS industry
- Enacting information and transparency protocols
- Conducting mandatory assessments of privacy and data protection issues for each type of operation (privacy impact assessments)
- Identifying stakeholders to monitor good practice in privacy and data protection.

In this summary report, we focus on the industry-specific recommendations in order to send a concise set of messages to these stakeholders.

First, we identify the following primary recommendation for industry. **RPAS manufacturers and operators need to be proactive in understanding how to minimise the amount of data they collect** in order to reduce their risks in relation to privacy and data protection. In relation to privacy, **it is essential for RPAS operators to enact information sharing practices** to provide members of the public with knowledge about the specific activities being undertaken by the RPAS. In relation to data protection, recommendations for reducing risks in relation primarily require RPAS operations not focused on people to consider the following data minimisation features:

1. Reduce the presence of people and their identifying objects (e.g., vehicles) at the site. Some RPAS operators have enacted this data minimisation feature by flying RPAS missions during workers' lunch breaks, or public holidays, or flying RPAS missions that do not require visual optics at night.

2. Only record images when absolutely necessary. This will ensure that if people do, inadvertently, appear on the footage, it is as infrequent as possible. Specifically, consider not recording the whole flight – only press record once the RPAS is in place and stop recording immediately after the mission aspect of the flight is finished.

3. Enact privacy-by-design features, such as blurring of images, during data collection or immediately afterwards, to make people and their possessions as anonymous as possible.

4. For sites that are visited frequently, inform people who may be captured on the footage what the RPAS is doing and provide relevant contact details to ensure that members of the public can exercise their rights to consent, access, rectification and erasure. Should an individual choose not to consent to their data potentially being collected, find a privacy-by-design feature that solves this problem. Otherwise, the mission may need to be cancelled.

5. Ensure that the data about or including people or their property is only utilised for the purpose for which it was originally collected and processed. For example, if an RPAS collects visual information for mapping a landscape, this footage should not be re-used to assist in a navigation application or for any other purpose not related to landscape mapping.

6. Ensure that the data collected is adequately secured. This may include considering both the types of hardware and software used in data collection, transfer, storage and processing to ensure that the data is not accessible to anyone but authorised persons.

7. Avoid storing unnecessary information about people or their property, and consider transferring such data to the clients without keeping a copy in order to reduce risks to privacy, personal data and ethics.

8. Where possible, RPAS operators should contractually establish whether they, or the client, have control over the "why" and "how" of processing activities, and are acting as the data controller, with all of the associated obligations.

Should an RPAS operator be asked to fly a mission that is focused on people or is very likely to collect personal data, RPAS operators should seek immediate legal advice before conducting the mission.

With specific regard to transparency, we find that a key element of ensuring public acceptance of RPAS is to educate members of the public about the activities RPAS are undertaking in the civil sphere and the types of data they are collecting. Such transparency is a requirement when collecting personal data and represents good practice in allaying concerns around privacy and ethics. Specifically, one of the privacy-invasive aspects of civil RPAS, even those that are not collecting data about people, is that members of the public do not know what the RPAS is being used for and may be concerned that it *is* collecting data about them. Consequently, greater awareness by members of the public about RPAS operators and operations will likely increase public acceptance of RPAS and enable the sector to grow. As such, **civil RPAS operators should be subject to information and transparency protocols**, to provide the public with this information. These transparency protocols could take a number of forms, and each would address obligations related to consent, accountability and rights of access to correction and erasure.

One potential format involves **the development of a national or cross-national information resource to enable citizens to identify the missions and operators associated with individual RPAS**. With the highest functionality, this resource could function similar to the existing Flight Radar 24 system (www.flightradar24.com) and provide real-time information about RPAS flying overhead. This would require RPAS to carry mandatory, unique identifiers that would enable the RPAS to be tracked via GPS using a centralised system.[28] It would require a centralised database of RPAS and their unique identifiers and well as their operators and contact information. Such a system should be a robust transparency tool that would enable citizens to immediately identify the RPAS, the operator and the avenue through which they could find additional information. At a lower end of functionality, RPAS should be marked with mandatory identifiers (e.g., tail numbers or serial numbers), which could be matched to information in a centralised database.[29] The database should contain the contact details of the RPAS operator, and this information should be made available to members of the public on request. However, this second option requires members of the public to undertake significant labour to identify the appropriate CAA contacts as well as RPAS operator contacts. These systems would enable RPAS operators to meet requirements for transparency, accountability, rights of access, correction and erasure as well as foster public confidence in civil RPAS operation. In order to achieve such a system, different RPAS stakeholders would have to work together, and the RPAS industry, in particular would have to participate in the design of common standards for such an identification mechanism, including serial numbers, signals and GPS tracking capabilities.

[28] Such a system was suggested by the International Working Group on Data Protection in Telecommunications, *Working Paper on Privacy and Aerial Surveillance*, 54th Meeting, Berlin, 2-3 September 2013.

[29] Although the tracking of a moving or small drone would be very difficult using binoculars, such identifiers would improve transparency, and are essential in the event that an RPAS crashes.

Finally, we also recommend that industry build on existing tools for impact assessment, including codes of conduct, impact assessments, etc. in order to construct and agree a methodology for conducting a privacy impact assessment. The EC as well as many responsible industry representatives have already agreed that undertaking an assessment of these impacts, on a case-by-case basis, represents good practice in the collection and processing of personal data. Such soft law measures are particularly suited to sectors such as civil RPAS operations, given that RPAS are multi-dimensional tools. The variety of operations, payloads and capabilities of RPAS mean that they must be assessed on a case-by-case basis, rather than using specific, overarching policy requirements. Furthermore, the research has found that the education and enforcement elements of privacy and data protection issues are particularly lacking in the civil RPAS sector. As such, we recommend that **all RPAS operators be required to carry out an impact assessment of the potential privacy, data protection and ethical issues on operations that may raise such issues on a case-by-case basis**. The preferred method of impact assessment is a privacy or data protection impact assessment, as he proposed General Data Protection Regulation includes an article requiring the mandatory impact assessment of any operation involving the collection and processing of personal data. Implementing these practices early will enable the RPAS industry to gain competence and reduce their liability well before they need to comply with this legal instrument.

Considering these eight good practice issues and undertaking a PIA will enable the RPAS industry to construct robust protections for themselves and members of the public in terms of privacy, data protection and ethics. However, the industry cannot work in a vacuum. They need support from the European Commission, national policy-makers, Data Protection Authorities and civil aviation authorities to enable this.

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);

- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries
  (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm)
  or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union
  (http://publications.europa.eu/others/agents/index_en.htm).

NB-07-14-048-EN-N

Publications Office

doi: 10.2769/964439