Article

International Journal of
Micro Air Vehicles

International Journal of Micro Air Vehicles
2018, Vol. 10(4) 340–351
© The Author(s) 2018
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1756829318794004
journals.sagepub.com/home/mav
SAGE

Ethics for civil indoor drones: A qualitative analysis

María de Miguel Molina[1], Virginia Santamarina Campos[2], Mª Ángeles Carabal Montagud[2] and Blanca de Miguel Molina[1]

Abstract

Drones face two main concerns: safety and security/privacy. Whilst safety has been broadly studied by literature, less research has been carried out into security/privacy. Moreover, current European regulations on drone flights apply to outdoor drones but not always to their indoor counterparts. However, several industrial sectors have started to use drones for indoor tasks such as surveillance, architecture, emergencies, and communication media. A qualitative study has been conducted in order to explore the concerns expressed by civil drone operators over the measures that manufacturers include in their products and information packages. Codes of conduct could also help these parties when there is no legal regulation that can be applied. We used content analysis as the method of analysis for three different sources: secondary data from a literature review and from public European documents, and primary data from focus groups. Results show that safety and security/privacy by design are seen as the best ethical measures, whilst codes of conduct could be used as complimentary information for professional users.

Keywords

Civil drones, safety, security, privacy, European policies, ethics

Received 10 November 2017; accepted 28 June 2018

Introduction

Drones, also known as RPAS (remotely piloted aircraft systems), UAS (unmanned aircraft systems) and UAV (unmanned aerial vehicles), are attracting the attention of many researchers. Over the last few years, the technological advances made in drones have enabled manufacturers to market them to all audiences, not only for professional but also for private use. Drones are used in different sectors such as heritage, topography, inspections, surveillance, security, agriculture, fishing, media, emergencies, transport, communications, and defence.

A search of the keyword "drone" on the Web of Science (Thompson Reuters) has yielded around 3000 results over the last fifteen years, with numbers rising particularly sharply over the last four years. The majority of these results are related to the "Science/Engineering" field.

This shows that drones have become very popular very quickly. However, there is often a legal vacuum when this occurs with a particular product. In addition, there are many different concerns about the use of drones, including their impact on the environment (especially noise)[1] as well as on people (safety) and on people's personal data (security and privacy).[2] Drones can be equipped, for example, with high-resolution cameras, microphones, thermal imaging or the capacity to intercept wireless communications.[3]

Juul,[4] for example, highlights that the current regulatory system in Europe is based on fragmented rules, with many Member States regulating some aspects of civil drones (operating mass of 150 kg or less), and the responsibility for civil drones over 150 kg being left to the European Aviation Safety Agency (EASA).

[1]Department of Management, Universitat Politècnica de València, Valencia, Spain
[2]Department of Conservation and Restoration of Cultural Heritage, Universitat Politècnica de València, Valencia, Spain

Corresponding author:
María de Miguel Molina, Universitat Politecnica de Valencia, Camino de Vera s/n (7D), Valencia 46022, Spain.
Email: mademi@omp.upv.es

Moreover, Fox[5] points out that the EU has recognised that it is not prepared and does not have a suitable framework in place to meet the existing challenges and potential opportunities of this new era of unmanned flight.

The European Council considers the EASA to be the best placed authority to develop technical and safety standards, licences and certificates. Since 2015, the EASA[6] has suggested modifying legal regulations in order to create a European regulation for civil drones. It has proposed several categories and standards, but indoor drones are not included in them, unless we interpret them as being included in an "open" category.[7] Anyway, at present, even if the European Parliament has opened the door to a common European framework and regulation, irrespective of what the drone weighs, the regulation still only applies to outdoor drones as it is based on the "Single European Sky airspace".[8] Therefore, on many occasions, the only solution for drones used indoors, which is considered as a private space, is ethics.

In general terms, measures regarding safety and privacy should take into account the following three main scenarios:

1. Injury to operators due to their constant proximity to RPAS.
2. Injury to the public or invasion of their privacy (personal data). This could refer to an audience of observers, or passers-by who are unaware of drone activity.
3. General damage to property. This includes the indoor surroundings in which the RPAS are flying as well as damage to the actual RPAS.

Moreover, in the case of indoor drones, a flight permit is not always required. In the majority of European countries, this depends solely on the property owner giving permission, for example, in the UK, permission is required when professional work using drones is performed. Nevertheless, although outdoor micro-drones, in general, i.e. those which have less than 500 g maximum take-off mass,[9] and indoor drones do not need special licences, professional operators have to ensure they are covered (insurance for persons/properties).

According to Clarke,[10] there is a risk that manufacturers and operators may neglect safety considerations, especially in the mini-drones segment. Drone costs have fallen sharply, particularly in the case of micro-drones for the consumer market, and competition among producers and operators can result in unethical behaviour, although drone manufacturers have to comply with different standards.[11] For example, all drones have to have an identification number. Requiring operators to be licensed and have insurance can impose standards and ensure safety.[12]

Nevertheless, apart from safety, other regulations regarding privacy, self-image[13] and data protection can affect the use of indoor drones. The European Parliament's Transport and Tourism Committee also emphasises safety, privacy, security and data protection.[4]

The former Article 29 Working Party[14] asked producers to help out by providing advice on their packaging and using codes of conduct in order to self-regulate the industry. Other tools, like impact assessment and the participation of a Data Protection Officer appointed by the data controller, could increase customer trust. It would be positive if industry could react proactively when regulation is not sufficient.

Some associations made up of drone manufacturers and operators have developed codes of conduct and apply ethical rules to their work.[15] What these codes do is provide guidance to regulators of legal standards and practices that are in force.[16] For example, in the European Union, ARPAS-UK has its own code of conduct.[17] As drone technology is changing fast, new organisations' adoption of drone technologies must be paired with clear articulations of their ethical use and full transparency with the public.[18]

Yet critics argue that these codes have the limitations of any industry's attempt to self-regulate: there are no significant consequences when the code is broken. Therefore, some authors add the need for co-regulation in conjunction with government[19] as well as additional training for users.[11]

Consequently, interaction among stakeholders may produce a consensus in terms of a public policy approach in an area where there is considerable uncertainty.[14] In this case, we have focused on the activity of manufacturers when designing indoor drones and the activity of operators and pilots when using them in order to analyse which features and measures will add proactive, safe and secure use for these new unmanned aircraft.

Existing safety technology

According to the literature, safety concerns include disturbance, no direct line of sight, loss of communication, loss of control, loss of positioning system, and low batteries. It normally associates two types of actors, manufacturers and operators, with safety. Technically speaking, these two parties have to take into account very similar safety measures for design and for operations.

Manufacturers

Clarke[10] remarks that the term "airworthiness" is used to refer to an aircraft's suitability for safe flight. For example, an aircraft's altitude represents its orientation around its centre of gravity in three dimensions: roll or bank (rotation around the aircraft's long axis), pitch (rise and fall of the nose of the aircraft), and yaw or heading (port-starboard/left-right swing of the nose of the aircraft).

Safety tests, which should check different key attributes of the product, are necessary before a drone can be marketed.[10] They include:

- Awareness of the drone's location within the operational space, of its altitude and of its direction and speed of movement.
- Sensors and/or remote data-feeds that enable the awareness of location, altitude and movement to be maintained in a sufficiently timely manner.
- A sufficient set of controls over the drone's altitude, direction and speed, to enable flight to be sustained under a wide variety of atmospheric conditions (this does not apply indoors). That is, to have an automated stabiliser in order to prevent crashes.
- Sufficient rapid response of the drone to the controls (manoeuvrability).
- Sufficient power (batteries or whatever source of energy) to maintain movement, to implement the controls, and to operate sensors and data-feeds, for the duration of the flight.
- The ability to navigate to destination locations within the operational space.
- The ability to monitor the operational space (situational awareness, threat detection).
- The ability to navigate with respect to obstacles (collision avoidance).
- Sufficient physical robustness to withstand threatening events, such as wind-shear, turbulence, lightning and bird-strike (this does not apply indoors).

Moreover, existing safety measures on RPAS can be subdivided into active and passive types. Whilst active measures try to detect possible risks to prevent them from happening, passive measures try to mitigate the impact of accidents through the features of RPAS.

Some active measures that can be applied in any environment are:

- A redundant flight control system, which keeps the drone stable even if there is a failure in the primary flight system. Motor propulsion units, a battery and a central unit are critical elements that must be redundant to compensate for a possible failure on a multirotor.
- Failsafe is a pre-programmed behaviour designed to prevent a crash in the event of an unsafe situation. The RPAS either lands automatically or returns to its launch base. Many drones feature this safety device to allow them to abandon a pre-planned mission and return to a landing point directly if they experience any problems.[20]
- Flight stabilisation through an integrated positioning system. A GPS (global positioning system) is the most commonly used positioning system outdoors, but it can also be applied to cellular network positioning to calculate a position via an observed time difference from two different base transceiver stations to a mobile station. In indoor situations, visual positioning systems (VPS) are the most commonly used. However, even though indoor positioning systems have made great progress, most of the new technologies have not been specifically developed for use with RPAS. To date, only a few commercial RPAS, such as Inspire and Phantom by DJI and Rolling Spider by Parrot, claim to incorporate an indoor VPS. Unfortunately, there are several problems with VPS when used in confined spaces, as they are light sensitive, sensitive to different surface textures and also have height limitations. In addition, no extra safety measures (e.g. redundant flight control system, proximity sensors) have been added to these indoor drones.

Furthermore, other active measures that exist for outdoor RPAS, such as geo-fencing (virtual perimeter or no-fly zones, which require a reconstruction of the environment) and flight path programming (automated flights), are currently absent in indoor environments. These measures define a set of vital data and test methods to help machine designers and manufacturers achieve a suitable safety level for the new human-machine collaborative working situation.[21]

Passive measures include rotor protection, reduced weight and an absence of sharp edges.

Operators

The use of an RPAS close to people always involves a certain level of risk. This is generally low as these devices are usually used outdoors. Being pilotless, drones can be more vulnerable to crashing and accidents might injure people on the ground. Rotary wing devices may be more dangerous in cases of engine failure as they tend to fall vertically.[18]

That is, small mistakes could result in crashes that threaten the health, well-being and property of the public[22] and experience is supposed to be the best way to reduce risks. Training is essential to drone operation, and is part of safety.[12]

In addition, the chance of a human piloting error leading to an accident could be eliminated in some cases if there was an auto-pilot function. Training a pilot requires time and dedication and an experienced pilot could input the routes needed during filming or for a photo shoot indoors.

Security and privacy concerns

Fundamental rights such as privacy, self-image and data protection can be affected by drone' operations.[13] Information security deals with measures designed to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.[23] Some security concerns include hacking, hijacking, and cyber-attacks. Therefore, from a manufacturer's point of view, communications between devices need to be encrypted to permit secure computer–RPAS communication and prevent unauthorised access by third parties.

On the other hand, privacy concerns relate to the recording and processing of personal data such as images, geolocalisation and electromagnetic signals, because a drone can attach a camera to record data and subsequently process it.

From the viewpoint of an operator and of companies that could work with them, data protection is guaranteed by the European Union. The Data Protection Law Enforcement Directive[24] (whenever personal data is used by criminal law enforcement authorities) and the General Data Protection Regulation (GDPR),[25] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, guarantee the rights of access, rectification, deletion and blocking. However, in order to correctly apply the standards, the subjects must be informed. There are easier ways to do this indoors, by using tickets, posters and individual authorisations. In addition, the necessary storage measures should be applied when processing this data, according to the GDPR.

Security and privacy by design could also be a solution for more ethical use of drones.[26] For example, data can be made anonymous (such as pixelating images to avoid facial recognition).[27]

Method

To collect the necessary data, we applied a triangulation process,[28] using multiple data sources. Our sources of information included secondary data from our literature review and public documents from the European Union as well as primary data from focus groups with experts.

Scopus literature review

We performed a literature review using the Scopus database to check how the three topics of safety–security–privacy were related. When we searched for the following keywords (RPAs OR drones AND security OR safety OR privacy) an excessive number of documents (564) were returned, therefore we decided to limit the search. As we noticed that privacy was the least studied topic, although all the works were focused on the three topics, we restricted our search as follows:

> TITLE-ABS-KEY (rpas OR drones AND privacy) AND (EXCLUDE (AU-ID, "Undefined" undefined)) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp"))

Through this search, we were able to limit the papers to journals and conference papers. We also removed all the documents without a clear author. After filtering the duplicated results, the results yielded 59 papers that were specifically focused on safety, security and privacy issues with drones.

As Figure 1 shows, the number of papers has increased significantly over the last few years, which demonstrates that this is a trending topic. However, the majority of studies are based in the USA whilst in the European Union, Germany and the United Kingdom are the two most relevant countries working on these topics (Figure 2).

In relation to the field of study, though Computer Science and Engineering cover 76% of the papers (individually or together with other fields), we can observe that 61% are related to Social Sciences plus Business. This means that it is also a relevant topic from the point of view of firms and stakeholders (Figure 3). Anyway, although Scopus is a broader database than others, we have to take into account that not all the journals are included in it, i.e. some Law journals do not appear. However, we preferred to analyse the topic in a homogeneous way using a single database.

Furthermore, we analysed the co-occurrences among the three topics to find out the main areas studied by the literature. To achieve this objective, we used the VOSviewer software,[29] which displays this information with different figures.

In the first one (Figure 4), we can see the co-occurrences between the keywords. "The colour of an item is determined by the cluster to which the item belongs".[29] In this case, four groups were formed: one related to safety, one related to security/data protection, one related to data in general and the last one related to surveillance. The lines indicate the strongest co-occurrence links between words. Safety is mainly related to the design of the drone; security

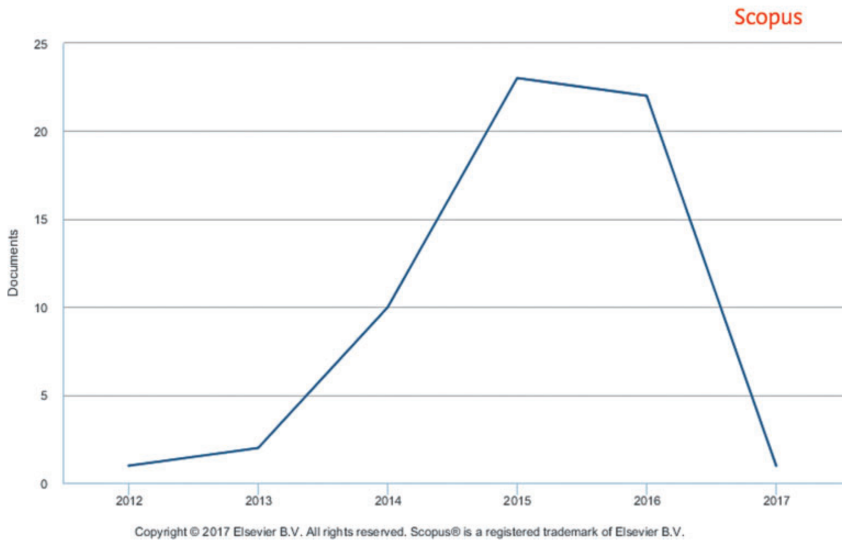

Figure 1. Yearly analysis using the Scopus database (Elsevier).

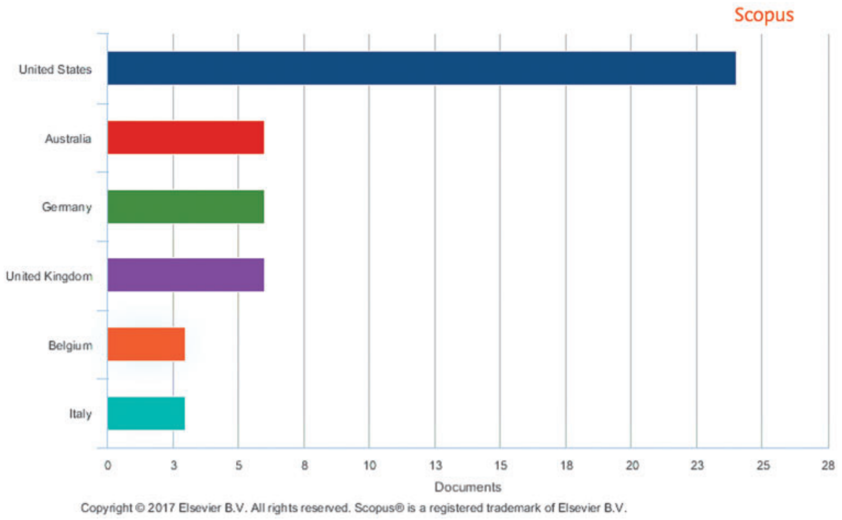

Figure 2. Analysis by countries using the Scopus database (Elsevier).

and data protection are related to the impact on people; surveillance is a specific topic in itself as it is the most closely analysed sector in terms of these topics and generates the greatest concerns about its regulation,[30] whilst data in general is a keyword related to all of them.

An analysis of the density figure (Figure 5) was similar. In this case,

> each point in a map has a colour that depends on the density of items at that point... The larger the number of items in the neighbourhood of a point and the higher the weights of the neighbouring items, the closer the colour of the point is to red.[29]

European documents: Regulations and statistics

As mentioned in Introduction section, the European Union and other related bodies have drawn up a series of documents in order to clarify the regulation of civil drones although no common legislation has yet been approved. Many documents were published in 2015, yet three years later the situation remains the same although it seems a specific regulation could come into force by 2019. The main documents analysed are:

The Riga Declaration on Remotely Piloted Aircraft (drones).[31]
Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones.[14]

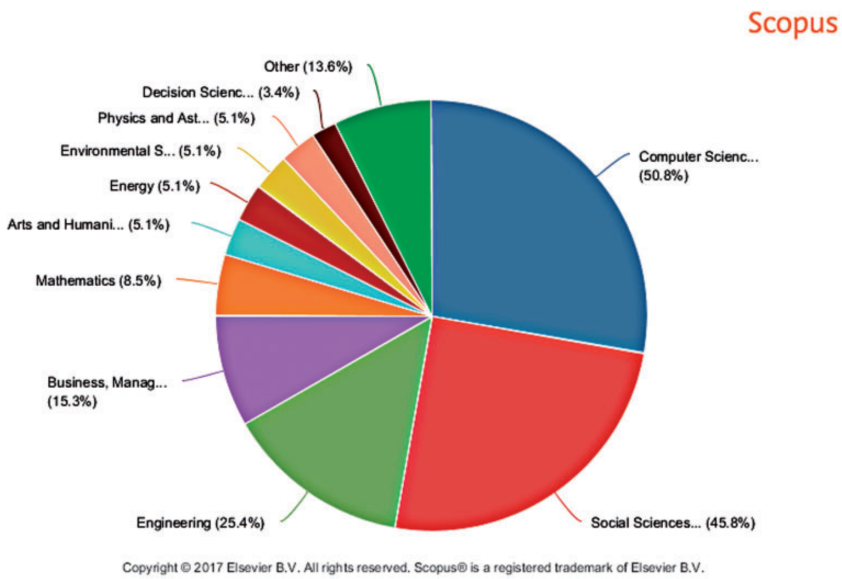

Figure 3. Analysis by field of study using the Scopus database (Elsevier).

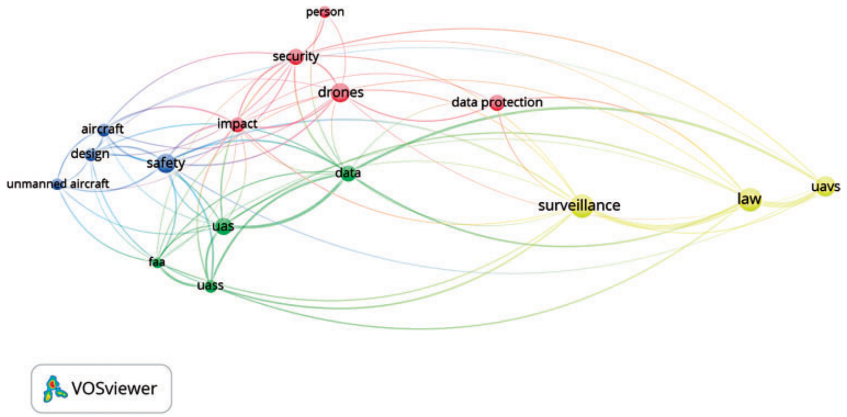

Figure 4. Co-occurrences among keywords with VOSviewer.

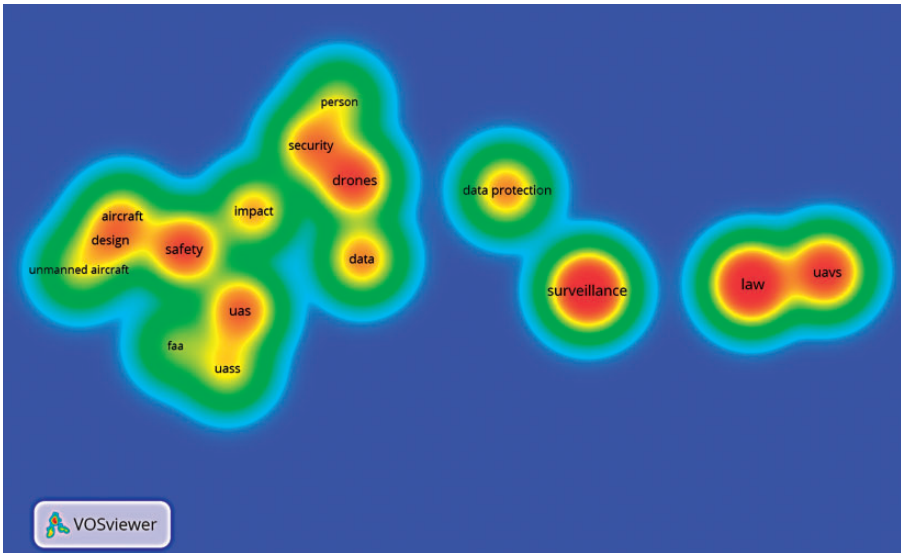

Figure 5. Density among keywords with VOSviewer.

Introduction of a regulatory framework for the operation of drones.[6]
Introduction of a regulatory framework for the operation of UAS in the "open" and "specific" categories.[7]
Civil drones in the European Union.[4]
Common rules in the field of civil aviation and the European Union Aviation Safety Agency.[8]

Moreover, we also analysed new data protection regulations that are set to replace the existing regime:

Directive 2016/680 of the European Parliament and of the Council, of 27 April 2016.[24] From 5 May 2018, this is directly binding for data controllers in all member states therefore the lack of transposition could be a problem for citizens' rights.
Regulation 2016/679 of the European Parliament and of the Council, Of 27 April 2016.[25] This Regulation contains measures that would harmonise data protection procedures and enforcement across the EU and it is applied from 25 May 2018.
The second source of data analysed were statistics from the European Union database Statista. In this database, we found different statistics from the United Kingdom compiled by ComRes in May 2016 (2043 respondents aged 18 and older).

The first one centred on the safety of drones and conventional aircrafts in the United Kingdom (Figure 6). This question was phrased by the source as follows: "To what extent, if at all, do you agree or disagree with each of the following statements? Drones pose more of a safety risk than radio-controlled aircraft which have been around for years." 58 percent of the respondents tended to or strongly agreed that drones posed a greater safety risk than conventional aircrafts.

In the case of privacy, the next statistics show the share of respondents who are concerned about privacy matters because of the use of drones in the United Kingdom (Figure 7). This question was phrased by the source as follows: "Thinking of all the potential uses of drones previously mentioned, to what extent, if at all, are you concerned or otherwise about their usage for any of the following reasons? Privacy (e.g. being spied on at home)". Forty two percent of the respondents stated that they were very concerned about their privacy.

The last one shows the evaluation of the respondents in terms of the commercial sensitivity and private use of drones in the United Kingdom (Figure 8). This question was phrased by the source as follows: "To what extent, if at all, do you agree or disagree with each of the following statements? I am less worried about the commercial sensitivity use of drones than private use of drones." Forty eight percent of the respondents tended to agree that they are less worried about commercial applications of drones than that of private use. An additional 14 percent agreed strongly with this statement. That is, people place greater trust in professionals using drones than in the general public.

In general, the impressions of these citizens regarding safety, security and privacy, are in accordance with the results of Boucher.[32]

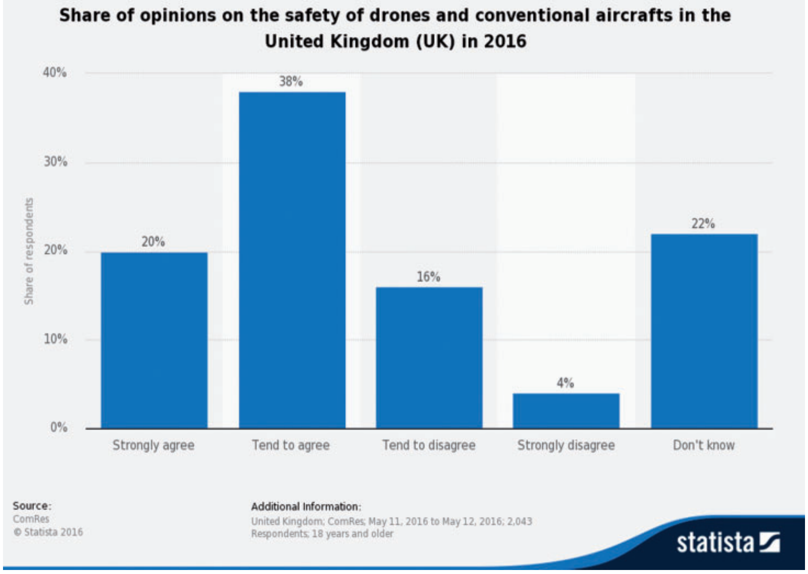

Figure 6. Drones pose more of a safety risk than radio-controlled aircraft which have been around for years?
Source: www.statista.com/statistics/606635/uk-drones-safety-risks/

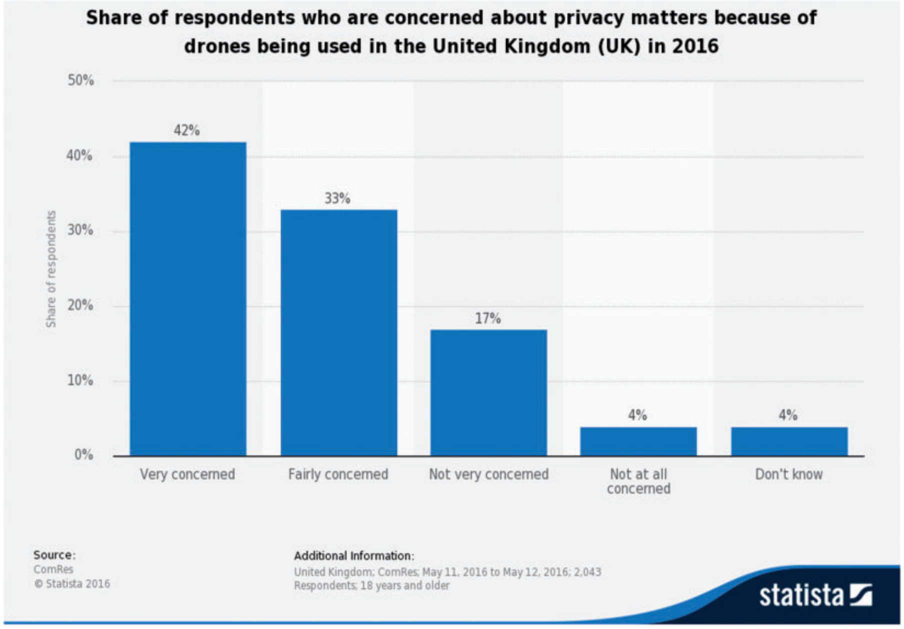

Figure 7. To what extent, if at all, are you concerned or otherwise about their usage for any of the following reasons? Privacy (e.g. being spied on at home).
Source: www.statista.com/statistics/606319/privacy-concerns-and-use-of-drones-uk/

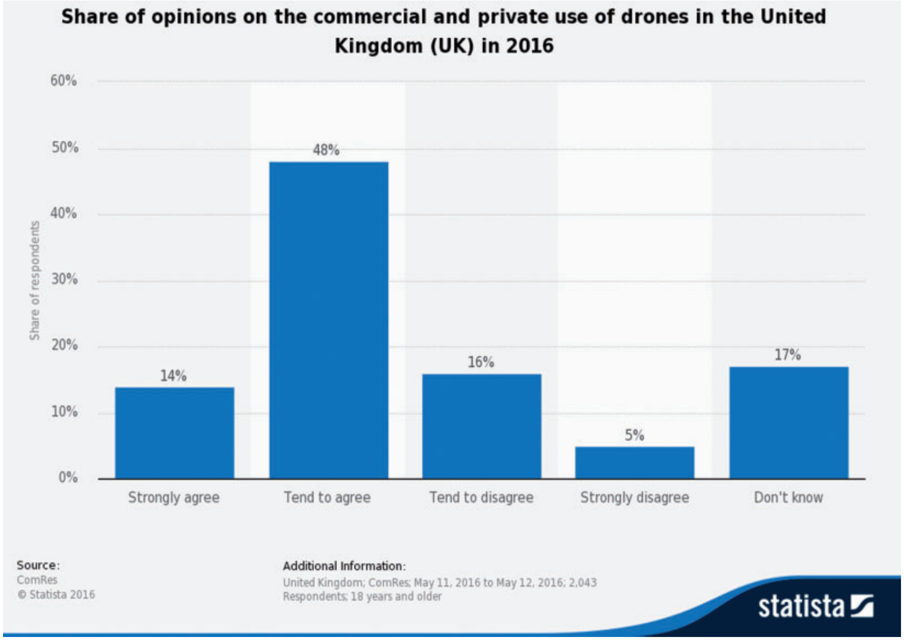

Figure 8. To what extent, if at all, do you agree or disagree with each of the following statements? I am less worried about the commercial sensitivity use of drones than private use of drones.
Source: www.statista.com/statistics/606362/commercial-sensitivity-and-use-of-drones-uk/

Focus groups

In February 2017, we conducted focus groups in three European countries (Belgium, United Kingdom and Spain) in order to explore the concerns of the industry about safety and security related to drones. Each group was formed by six-seven expert informants from different sectors. Half of them had a drone pilot's licence. Based on the literature review, we compiled a guide to conduct the focus groups on the key topics and we acted as facilitators of the dynamics.

First of all, we gave the informants an agreement form to sign so we could record their voice and image, in line with the data protection legislation in force in each country. Their names and affiliation remained anonymous.

Then, in each focus group, we held a two-hour conversation about the following: safety measures (prevention of accidents), security and privacy issues (protection from unauthorised access by third-parties) and ethical issues.

Finally, we transcribed the audio content of the three focus groups from the 20 informants, including 6 hours of recordings, 180 hours of transcription, almost 50,000 words and more than 100 pages to analyse. The main document enabled us to perform a content analysis of the principal issues.

Results from primary data

The information from the focus groups enabled us to explore the possible concerns of operators when flying an indoor drone, even if there is no applicable regulation.

Following the previous analysis, we separated safety and security concerns. However, in general, all the informants agreed that safety by design and security by design are the best solution for all the concerns, because “If it’s very accurate and it works very well then it will be more ethical” (Belgian informant).

> Maybe if there’s a point when, without doubt, the sensors work perfectly, we know there’s no error margin, it’s very easy to use and in case of any problem it lands without crashing on anything… if all of these are thoroughly tested, we could reach a point when anyone could use a drone. (Spanish informant)

Moreover, because indoor drones “do not need a pilot or a licence, anyway it’s always a good idea for the owner to have insurance”, even though “the regulation doesn’t apply”. However, this situation sometimes creates an unsafe environment: “The main problem is always the legal vacuum, depending where you fly you’re afraid of what might happen and sometimes we are stopped when we’re recording something” (Spanish informants).

Safety

We can also separate safety by design (manufacturer) and safety during the flight (operator).

Regarding drone manufacture, informants agreed that safety by design can reduce incidents. As an informant from Belgium said, “something that is ‘uncrashable’ because it detects everything”. In terms of indoor drones, “safety first in this case. And it has to be as easy to use as possible. And small” (Belgian informant).

For example, in the case of outdoor drones, DJI drones shut down when approaching an airport, “that’s built in to the drone by the manufacturer or via a firmware update” (UK informant).

The key elements that an indoor drone should have in its design, according to the informants, are the following:

a. Active elements:
   “Much larger batteries that last longer” (UK informant).
   Speed control: “flying very smoothly, slowly indoors because twitchiness and things like that can be… a pain” (UK informant).
   “Flying home…the drone works… and then returns” (Spanish informant).
   “Not to lose the connection with the pilot…antennas should be fixed to ensure communication is maintained” (Spanish informant).
   Positioning system: sensors (“infrared … and also sound… sonar”) to prevent crashes (Belgian informant). “A safety margin, a safety border, not physical, with sensors, to avoid the drone getting too close to works” (Spanish informant). “Indoors your margin of error is even smaller” (UK informant), so “Safety is a main thing. When you put a camera that has cost €50,000–60,000 in the air you want it to return to the ground in one piece, and that’s the main thing, … you have sensors everywhere” (Belgian informant). “Sensors… would seem to be the most practical and easiest solution in my opinion to prevent indoor collisions. A visual system that you have to look at to see how far away you are distracts you from the position of the drone. You can see that you can’t rely on the valid, sorry inaccurate, indoor positioning system such as the GPS that you use outdoors” (UK informant). “Drone development is also already making more sensors around the drone, in the drone, inside the drone” … “sudden obstacles are still a weak point” (Belgian informant). Other: “then you could fly really, really close to anything and as soon as you touch something with the things they can instantly correct their position and back off a little bit”.
b. Passive elements:
   “Prop guards can be really handy” (UK informant).
   “Weight is also an important factor. The lighter the drone the better, if it crashes on something” (Spanish informant).

From the operators' viewpoint, informants think that for a professional "reputation is everything" and "loyalty is a huge thing" (UK informant), so they avoid taking risks with a wick product or flying a drone without experience. But they worry about the unprepared competition: "Think of all the other people that say they can do it. Probably illegally" (UK informant).

> I think there are lot of people who say 'I am a drone operator' and they may well go with an old one, and they may have read the manual, but actually they don't know fully what they're doing. There are a lot of... a lot of amateurs out there and I worry about the safety of it. (UK informant)

> I think the only thing that doesn't exist is the reliability and the safety of the drone because now the market is like everybody buys a drone but not everybody can fly one so when it is really easy to use that would be a point in its favour. (Belgian informant)

To avoid professional interference, "I will...ask for a licence and total control...you can't take the risk ... a licence and training...You are going to want to ask for the pilot's CV if you are going to out him/her in a special place" (Spanish informant). In addition, "the first thing you would obviously ask for is their licence, proof of insurance, the indemnity insurance they have, etc. Then you would ask... to see the portfolio of the pilot" (UK informant).

Experience brings trust because, even if legal regulations do not require a licence to fly a drone indoors, if you have a

> qualified drone pilot with civil aviation authority...you get your approval or licence ... The other thing is "The course's objective is not to teach you how to fly... The main focus is safety, navigation, rules, regulations, where you can or can't fly, how far you need to be away from... extras, personnel. So, for anyone who's got their licence..., their number one priority ... certainly should be safety." (UK informant)

Professionals pay attention to other things, such as making the operator visible, requests for authorisations and having insurance coverage. "I worry about the insurance side of risks: you know, the equipment getting broken, somebody getting hurt..." (UK informant). If you automate the flight, "Now you don't need two people, ... you only need one person" (Belgian informant). "In an indoor setting, you're far more capable of delivering what your vision is", "someone's always got their eye on the drone while someone else might be monitoring" (UK informant). But... "something else can always happen. You have to anticipate; you have to be able to anticipate. That's when the creativity also kicks in and if everything is too automated, you're limited in those terms" (Belgian informant).

Another comment was that producers could give advice and instructions. For example, "YouTube videos of five minutes each, or some random software, without putting money into it" (UK informant).

Security and privacy

All the informants agreed that security/privacy by design can prevent risks. For example, device authentication can prevent unauthorised connections. A key measure for security is to protect the Wi-Fi connection, as "A big, massive Wi-Fi booster in a big exhibition hall would come across and... that has the potential to knock out your remote-control link" (UK informant).

> The hijacking of drones should be a big focus in the future. Hijacking a drone next to a football stadium, for example, could encourage using the drone to drop something or do something it shouldn't be doing. That's quite a big concern. (UK informant)

In terms of privacy, "if you speak to people who are and aren't familiar with drones... then what's their number one prior...number one worry is their privacy: flying over parks, kids etc." (UK informant). Concerns are related to when a camera is fixed to the drone: "Privacy issues..., are related to the camera you use. Not to the use of the drone. It's just camera use" (Belgian informant). Moreover, because the massive idea is related to bad news, so when people see a drone they say "Stay away from there!... Sometimes you have so many people coming up to tell us" (UK informant). A first measure would be to identify who the drone operator is "especially when they're unethical about it and that's trouble" (UK informant). But, in addition to a camera, other devices such as microphones and thermal imaging can also be used.

Moreover, asking for permission or at least giving the necessary information can prevent trouble or hours of editing. "If there are people in your recording, or they sign to give you permission or you have to delete their faces" (Spanish informant).

Conclusions

This work adds a twofold view to the literature. On one hand, it gives a new perspective to the study of safety and security elements of drones. Traditionally, agencies distinguish between active and passive technical measures. However, we have distinguished between measures according to the actor who is involved.

From our point of view, manufacturers and operators are different actors. Although they both should have the same knowledge on safety risks and measures, manufacturers are key actors as they can actually develop these measures whilst operators can only use them, so they are less involved in the design of the product. However, manufacturers should work together with operators in order to improve these measures. We observed that knowledge of operators' concerns can add considerable value to the product, especially in the case of SMEs that have to compete with powerful firms like DJI.

On the other hand, literature has paid more attention to the safety side of drones rather than to security and privacy concerns. However, this is mainly an ethical issue that policymakers should work on with stakeholders,[33] especially in the case of micro-drones and indoor drones that do not require a flight licence or training to be used.

Participants give importance to the experience of the pilot, and even more so, when dealing with professional jobs. Trust is generated when a pilot has been trained and there is also insurance to cover any eventuality. Protecting the Wi-Fi connection is also a must in all the cases to give information to the subjects when recording.

The results show that, although ethics and codes of conduct can help drone users, co-regulation in which public agencies could provide some kind of certificate would be a beneficial addition to reinforce other kinds of uses where flight licences are not compulsory.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 732433. Project: AiRT, Technology transfer of RPAs for the creative industry, H2020-ICT-2016-2017.

ORCID iD

María de Miguel Molina http://orcid.org/0000-0003-4264-8000

References

1. European Parliament. Annexes III and IX, Common rules in the field of civil aviation and the European Union Aviation Safety Agency, Legislative Resolution of 12 June 2018 on the proposal for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 (P8_TA-PROV(2018) 0245), www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0245+0+DOC+PDF+V0//EN (2018, accessed 12 June 2018).
2. Smith ML. Regulating law enforcement's use of drones: The need for state legislation. *Harv J Legis* 2015; 52: 423–454.
3. Calo MR. The drone as privacy catalyst. *Stanford Law Rev Online* 2011; 64: 29–33.
4. Juul M. Civil drones in the European Union. PE 571.305. Members' Research Service, European Parliamentary Research Service, www.europarl.europa.eu/RegData/etudes/BRIE/2015/571305/EPRS_BRI(2015)571305_EN.pdf (2015, accessed 10 November 2017).
5. Fox SJ. The rise of the drones: Framework and governance. Why risk it! *J Air Law Commerce* 2017; 82: 683–715.
6. EASA (European Aviation Safety Agency). A-NPA 2015-10. Introduction of a regulatory framework for the operation of drones. 31 July 2015.
7. EASA (European Aviation Safety Agency). Opinion No. 01/2018. Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories. 6 February 2018.
8. European Parliament. Common rules in the field of civil aviation and the European Union Aviation Safety Agency, Legislative Resolution of 12 June 2018 on the proposal for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No. 216/2008 (P8_TA-PROV(2018)0245), www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0245+0+DOC+PDF+V0//EN (2018, accessed 12 June 2018).
9. la Cour-Harbo A. Mass threshold for 'harmless' drones. *Int J Micro Air Vehicles* 2017; 9: 77–92.
10. Clarke R. Understanding the drone epidemic. *Comput Law Secur Rev* 2014; 30: 230–246.
11. Clarke R. Appropriate regulatory responses to the drone epidemic. *Comp Law Secur Rev* 2016; 32: 152–155.
12. Luppicini R and So A. A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technol Soc* 2016; 46: 109–119.
13. Sarrión EJ and Benlloch Domènech C. Rights and Science in the drone era. Actual challenges in the civil use of drone technology. *R&S* 2017; 0: 117–133.
14. Article 29 Working Party. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 16 June. 01673/15/EN WP 231, http://ec.europa.eu/justice/article-29/documentation/opinion-recommen

dation/files/2015/wp231_en.pdf (2015, accessed 10 November 2017).

15. Arkin RC. Ethics and autonomous systems: Perils and promises. *Proc IEEE* 2016; 104: 1779–1781.
16. Freeman PK and Freeland RS. Politics & technology: U. S. policies restricting unmanned aerial systems in agriculture. *Food Policy* 2014; 49: 302–311.
17. ARPAS Code of conduct, www.arpas.uk/mem-code-of-conduct/ (2017, accessed 17 October 2017).
18. Culver KB. From battlefield to newsroom: Ethical implications of drone technology in journalism. *J Mass Media Ethics: Explor Quest Media Moral* 2014; 29: 52–64.
19. Clarke R. The regulation of civilian drones' impacts on behavioural privacy. *Comput Law Secur Rev* 2014; 30: 286–305.
20. Sandbrook C. The social implications of using drones for biodiversity conservation. *Ambio* 2015; 44: 636–647.
21. Fonseca A and Pires C. Human robots interactions: Mechanical safety data for physical contacts. In: P Savage-Knepshield and J Chen (eds) *Droning on about drones—Acceptance of and perceived barriers to drones in civil usage contexts. Advances in intelligent systems and computing*, vol.499. Cham: Springer, 2017, pp.305–316.
22. Rao B, Gopi AG and Maione R. The societal impact of commercial drones. *Technol Soc* 2016; 45: 83–90.
23. Braun S, Friedewald M and Valkenburg G. Civilizing drones: Military discourses going civil? *Sci Technol Stud* 2015; 28: 73–87.
24. DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework (Decision 2008/977/JHA).
25. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
26. Coopmans C. Architecture requirements for ethical, accurate, and resilient unmanned aerial personal remote sensing. In: *2014 international conference on unmanned aircraft systems (ICUAS)*, Orlando, FL, 27–30 May 2014, pp.1–8. Orlando: IEEE.
27. Ruchaud N and Dugelay JL. Privacy protection filter using StegoScrambling in video surveillance. In: *CEUR workshop proceedings*, Wurzen, Germany, 14–15 September 2015, vol. 1436, p. 62. Germany: CEUR-WS.org.
28. Berg BL and Lune H. *Qualitative research methods for the social sciences*. New Jersey: Pearson Education, 2012.
29. Van Eck NJ and Waltman L. *Manual for VOSviewer version 1.6.5*. The Netherlands: CWTS, Universiteit Leiden, 2016.
30. Kaminski ME. Regulating real-world surveillance. *Washington Law Rev* 2015; 90: 1113–1165.
31. European Commission. Riga declaration on remotely piloted aircraft (drones) 'Framing the Future of Aviation'. *Riga*, 6 March 2015.
32. Boucher P. "You wouldn't have your granny using them": Drawing boundaries between acceptable and unacceptable applications of civil drones. *Sci Eng Ethics* 2016; 22: 1391–1418.
33. Finn RL and Wright D. Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Comput Law Secur Rev* 2016; 32: 577–586.