COMPUTER LAW & SECURITY REVIEW 32 (2016) 577–586

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations

Rachel L. Finn *, *David Wright*

Trilateral Research Ltd, London, UK

Keywords:
Privacy
Data protection
Industry
Regulation

ABSTRACT

This article presents results of a survey of primarily, although not exclusively, European drone industry representatives, regulators and civil society organisations that examined privacy, data protection and ethics with respect to civil drone operations. The article provides snapshot information about the diversity of the drone industry, including information about the types of companies, the types of drones being manufactured and operated, their payloads, capabilities and applications. Using self-reported information from industry representatives, it also demonstrates that these stakeholders do not have a clear understanding of European privacy and data protection law, which can impact their levels of liability and protections for individuals on the ground. With respect to regulators and civil society watchdogs, the results demonstrate that law enforcement, commercial and private (or recreational) drone operators are all thought to be associated with significant privacy, data protection and ethical risks, and that recreational operators are thought to carry the highest risks. However, perceptions of high-risk operators vary among different organisations, raising a potential for regulatory fragmentation. The article concludes with a consideration of the implications of these findings for the regulation of privacy, data protection and ethics for civil drone operations.

1. Introduction

As civil drone use is proliferating rapidly, drones are becoming increasingly integrated with civil practices, including professional, political and recreational practices. Drones are being used by crisis response and humanitarian organisations (Meier, 2015), for conservation activities (Sandbrook, 2015), by police and other authorities (Salter, 2014), by protesters (Martin, 2011) for recreational purposes, including "drone racing" (Moynihan, 2015), and for various commercial purposes. In addition, drones are increasingly being used as "big data" platforms, capturing multiple types of data from a range of sensors, including optical cameras, temperature sensors, GIS sensors as well as others (PrecisionHawk, 2015), and these data are increasingly being integrated with external data sources (Finn and Donovan, 2016).

Yet, despite this integration, there are significant and already well-documented privacy, data protection and ethical issues associated with civil drones. This article analyses the perspectives of different stakeholders within the RPAS ecosystem on these privacy, data protection and ethical issues. It presents survey findings from primarily, although not exclusively, European drone operators and manufacturers (industry), regulators (civil aviation authorities and data protection authorities) and civil society organisations about these issues. For each organisation, it examines their awareness of privacy, data protection and ethical issues associated with civil drones as well

* *Corresponding author.* Crown House, 72 Hammersmith Road, London W14 8TH, UK.
E-mail address: rachel.finn@trilateralresearch.com (R.L. Finn).

http://dx.doi.org/10.1016/j.clsr.2016.05.010

as current practices for addressing these issues. The article demonstrates three key findings. First, the drone industry, including their products and operations, is diverse, making comprehensive regulation difficult. Second, while professional drone manufacturers and operators are undertaking some risk assessment procedures, their knowledge of the specifics of European data protection law is lacking. Third, the research finds that most regulatory organisations view private operators of drones (e.g., hobbyists) as the most risky operators with respect to privacy, data protection and ethics, but that these perceptions vary between different types of organisations. The article concludes by considering the implications of these findings for regulatory oversight over civil drone usage, including examining the extent to which regulation can address both the need for context-specific assessment of issues and provide strong protections for the public.

2. Drones, privacy, data protection and ethics

The specific privacy, data protection and ethical issues associated with the civil use of drones are difficult to pin down, given drones' diverse capabilities and applications. For example, factors such as the purposes for which they are used, the extent and type of (personal) information that may be captured by the drone, the type of operator, the context and location of the drone operation, as well as the type of technology they carry all need to be considered when mapping potential privacy, data protection and ethical impacts. For instance, privacy concerns related to the use of a drone equipped with a facial recognition sensor in the context of a crime investigation are not the same as those occurring when a drone fitted with an optical camera is used to monitor pipelines. Hence, drones raise some key issues in civil contexts.

For example, drones may have significant privacy impacts. Drones equipped with cameras can capture images of persons, intentionally or unintentionally, which can provide information about different aspects of people's privacy, including their location, behaviour, body characteristics and those with whom they associate alongside their loss of control over their image (Finn et al., 2013). In many circumstances, this information can also create a "chilling effect", whereby "to protect themselves from the negative effects of intrusions; individuals must assume they are being observed and attempt to adjust their behaviour accordingly" (ibid., p. 16). Drones fitted with other sensors can also provide information about people's locations (geographical data), their health (temperature data), their behaviour and home lives (Finn et al., 2014). In addition, any use of drones that directly or indirectly collects information about people is subject to function creep, whereby systems expand to include additional functions not originally envisaged by designers, original operators or promoters (Lyon, 2007, p. 52). For example, in commercial contexts, inspecting industry infrastructure might capture information about workers' behaviour, and might be used by management to discipline workers. Drones raise privacy issues no matter for what they are being used, since it is often unclear who is operating the drone, or what capabilities it has and or for what purpose it is being used (Article 29 Data Protection Working Party, 2015).

Drone operations also raise data protection issues. As with related privacy issues, it is difficult to identify and outline each current and potential data protection risk presented by the civil use of drones. Nevertheless, consent, proportionality, data minimisation, transparency, data security, rights of access, correction and erasure and anonymisation all emerge as important issues that need to be addressed by drone manufacturers and operators (Article 29 Data Protection Working Party, 2015). Furthermore, in Europe, the recent Court of Justice of the European Union ruling has clarified the scope of the household exemption in data processing (František Ryneš v Úřad pro ochranu osobních údajů [2014], 2015), including systematic filming of public spaces within the Data Protection Directive (95/46/EC). Thus, the use of drones to record information in public spaces, even when carried out by private individuals for recreational purposes, falls under the scope of the Directive. In addition, the proposed General Data Protection Regulation (GDPR) introduces obligations for manufacturers and operators to include privacy by design features or carry out data protection impact assessments as part of any operation that collects personal data.

Finally, drones raise important ethical issues. For example, pilots operating drones at a distance may be infected by a "Playstation" mentality and violate acceptable ethical practice, especially on particularly dangerous missions (European RPAS Steering Group, 2013). Finn and Wright (2012) note that it is often the "usual suspects" who are targeted by police or authorities' use of drone technology, including migrants, young people and working class people. In conservation operations, drones could aggravate existing political tensions between communities and authorities (Sandbrook, 2015). In journalism, drones may contribute to a greater good, but some drone applications could also undermine public trust (Culver, 2014).

The regulatory framework around these issues is still developing. Many national and regional governments are focused on managing the safety issues associated with the integration of drones into civil air space, although it is clear that much work remains to adequately address these issues (Clarke and Moses, 2014). Regarding safety as well as privacy and data protection, Clarke notes that natural controls, such as technological limitations, economics, reputation risks and industry self-regulation, fail to provide sufficient disincentive for irresponsible, or even illegal, usage (Clarke, 2014). Recently, the US Federal Aviation Administration has accepted recommendations that all drone pilots be registered (Unmanned Aircraft Systems (UAS) Registration Task Force (RTF) Aviation Rulemaking Committee (ARC) (Task Force), 2015). The UK has a similar registration scheme and requires commercial pilots to obtain written authorisation for operations. While this provides some measure for potential accountability, it remains difficult to enforce meaningfully. While the UK and US both recommend that operators consult good practice documentation including privacy and data protection guidance, there is no specific training offered for this beyond high-level advice. In Europe, the police or data protection authorities could investigate drone operations that violate the Data Protection Directive, but in practice, these would be difficult to prosecute, given how time-consuming it would be to build a case. Authorities might regard such issues as a nuisance rather than more serious criminal behaviour.

Heretofore, there has been little information about how well drone manufacturers and operators understand these issues,

their perceptions of these issues and the types of activities they undertake (if any) to address them. There has been minimal empirical research to date about drone operations (Sandbrook, 2015). To remedy this, the European Commission's Directorate General for Growth (formerly DG ENTR) funded Trilateral Research [with Vrije Universiteit Brussel (VUB)] to undertake empirical research into the privacy, data protection and ethical issues associated with the civil use of drones. Trilateral's work included a survey of industry, regulators and civil society organisations' awareness of these issues. This article presents the results of this survey.

3. Methodology

The project designed, distributed and analysed a set of online surveys on privacy, data protection, ethics and the use of drones for civil applications. The surveys were distributed to four different primarily, although not exclusively, European stakeholder categories in Spring 2014.

The researchers had varying levels of success in reaching each of these four groups. Industry representatives were the most highly represented organisations (94 respondents), while civil aviation authorities proved difficult to incentivise to participate, as only nine of the 28 European CAAs responded, with two CAAs each providing two responses (11 total respondents) (Table 1). DPAs and CSOs both had moderate response rates. However, in each case, respondents represented a self-selected sample that is not representative of any of these stakeholder categories. For all organisations, the survey was used to assess their levels of awareness of drone capabilities and applications, as well as the associated threats to privacy, data protection and ethics.

The surveys were distributed online, via a survey software service called SurveyMonkey. The survey was initially distributed via project partners' contact lists that included individual contacts at all of the DPAs and most of the CAAs. Where individual contacts were not available for the CAAs, partners used the generic e-mail address for the organisation. Distribution of surveys to civil society organisations relied on partners' extensive contacts and networks in this area as well as research to build this contact list. Partners identified industry contacts from their own contact lists, from research and via distribution through major European drone organisations, e.g., UVS International, and national industry organisations. In all cases, partners invited respondents to share the survey widely to increase the response rate. The survey was conducted exclusively in English in order to manage the tight research deadlines for the project. However, the researchers recognise that this may have reduced the number of responses across Europe and beyond.

In order to complete the survey, the consortium began the process by sending each individual on the contact list a targeted e-mail advising him or her that the questionnaire will be following shortly. A second e-mail reminder followed this after one week and a third after two weeks. This strategy is known to increase survey response rates as outlined in the survey research literature.[1]

The survey examined different issues in relation to different stakeholder categories. For example, the survey for industry representatives examined the current and future capabilities and applications of drones by asking industry respondents about the devices they design, manufacture and operate, as well as their customers. It also examined the extent to which industry representatives felt that these current and future applications raised privacy and data protection issues, and what, if any, activities they have undertaken to address these issues. Both the DPA and CSO surveys examined what specific aspects of privacy, data protection and ethics might be impacted by visual surveillance by drones (the most common application), including applications undertaken by law enforcement, commercial organisations and private persons. Finally, the CAA questionnaire examined the current regulatory framework, CAAs' knowledge of privacy and data protection legislation and how well they felt that they were positioned to examine privacy and data protection issues alongside their other responsibilities. A full version of the survey results can be found on the EC website; this article discusses two specific findings. First, the drone industry would benefit from further awareness-raising about privacy, data protection and ethical issues. Second, all categories of stakeholders recognised that those using drones for recreational purposes were the most "risky" in terms of privacy, data protection and ethics, and that stakeholders' perceptions of high-risk operators was somewhat fragmented.

Table 1 – Drone survey respondents.

Survey	Respondents
Industry representatives (including drone designers, manufacturers and operators)	94 total respondents European and non-European countries
Data protection authorities	27 total respondents 19 EU Member States
Civil society organisations	17 total respondents 6 European countries plus USA and Australia
Civil aviation authorities	11 total respondents 9 EU Member States

4. Industry findings

Drone manufacturers and operators' responses to the survey provided information about their organisations as well as the capabilities and applications for which their drones could be used. This included information about the payloads their drones could carry, their current and intended customers and any applications of which they were aware. In addition, respondents were asked about their awareness of privacy, data protection and ethical issues, and asked to assess the extent to which their activities raised these issues.

4.1. *Characteristics of the drone industry*

Respondents to the project survey demonstrated the diversity of the drone industry in Europe. Most of the organisations that

[1] See, for example, Aldridge and Levine (2001), De Vaus (1990), and Hoinville and Jowell (1978).

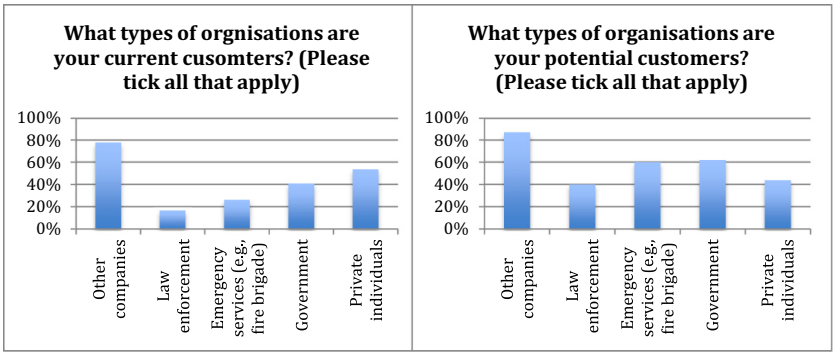

Fig. 1 – Drone current and future customers.

responded to the survey were based in Europe. Many operated in various European countries and had operations in third countries (i.e., outside Europe). Most of the 94 industry respondents to the survey were high-level executives and/or directors; however, many of the companies were small enterprises and, in some cases, sole proprietor enterprises. The survey respondents indicated that their companies undertook a range of drone activities. Eighty-six per cent of respondents indicated that they were drone operators, while 40% and 38% indicated that they were drone designers and manufacturers respectively (respondents were invited to choose more than one option). Seventy-six per cent indicated that they design, manufacture or operate quadcopter type drones, while 51% indicated that they used fixed wing, plane-like drones. A further 18 respondents (20%) indicated that they were also designing, manufacturing and/or operating other types of remotely piloted vehicles, including boats, cars and crawlers. Furthermore, the range of companies that answered the survey is further indicated by their sales figures, where many respondents indicated that they had sold one, two or only a handful of drones the previous year, while others indicated that they sold hundreds of units.

Not only is the industry diverse, the drones produced and used by manufacturers and operators were also diverse. Survey respondents indicated that their drones could carry a range of payloads, including photographic and thermal imaging cameras, GPS location equipment and environmental sensors (Table 2).

The findings indicate that cameras remain the most popular payload to carry on a drone. Thermal imaging and equipment that could be used to enable communication were also increasingly used, raising additional privacy and data protection issues (see Finn and Wright, 2012 for a discussion of privacy and thermal imaging cameras).

Table 2 – Drone payloads.

What types of payloads do(es) your RPAS[a] carry? (Please tick all that apply)	
Answer choices	%
Photographic cameras	98
Thermal imaging cameras	61
Geolocation equipment	51
Communication equipment	34
Environmental sensors (e.g., toxins)	24

[a] The project for which the survey was undertaken used the term "remotely piloted aircraft system (RPAS)", partly because some European policy-makers prefer the term. ICAO also uses the term. Nevertheless, the media have given the term "drones" the greatest currency by far.

Respondents who indicated that they are drone operators reported that their operations are primarily situated in the following sectors: commercial or corporate (94%), emergency services (29%), government (23%), private individuals (21%) and law enforcement (16%) (respondents could tick more than one option). This correlates relatively well with the information provided by drone designers and manufacturers who have indicated that other companies, government and private individuals are currently their primary customers.

This demonstrates that commercial users form the most significant consumer base and most significant use category for drones in Europe. Fig. 1 also indicates that the drone industry in Europe hopes to expand its already significant customer base by building customers in emergency services and government agencies. Respondents also seemed interested in somewhat decreasing their private individual customer base, although with the advent of "drones as toys" marketing, this finding may be already outdated. Finally, in relation to future capabilities, drone designers and manufacturers reported that they would like to develop the capabilities in relation to environmental sensing (67%), video or photography (62%), wide area surveillance (51%), geo-spatial surveying (44%) and telecommunications (24%).

In relation to what types of data they collect, almost all industry representatives (99%) indicated that their drones collected visual or photographic images, while 53% collected geo-spatial data and 44% collected environmental data. One respondent clarified that the type of data collected depends "entirely on what sensors are added" to the drone payloads. Combining all this information indicates that the use of drones for commercial filming is the most widely used application in Europe.

This discussion demonstrates that the drone industry is characterised by a significant diversity within Europe, with companies of different sizes, different business models and selling different types of products. The data also indicate that there are some key aspects of the European drone industry that are worth considering. First, most drone companies that responded to this survey appear to be small organisations with few staff members and relatively small financial turnover. Second, drones are most likely to carry photographic equipment and to sell to commercial organisations. Industry is clearly interested in

expanding both its product capabilities and customer base, both of which will raise additional privacy, data protection and ethical issues beyond those discussed at length in the literature. Finally, it appears that the commercial organisations' use of drones for visual inspection purposes is the most commonly used application in Europe.

4.2. *Industry awareness of privacy, data protection and ethics*

Given the diversity of drone capabilities and their potential applications, drone manufacturers and operators need a clear understanding of privacy, data protection and ethical issues in order to ensure that their products or services do not undermine these. The authors have previously argued that this diversity means that manufacturers and operators should undertake privacy impact assessments to deal with the specificity of their product, operation and context (Finn and Wright, 2012).

The survey used the visual surveillance capabilities of drones as a key example, given the popularity of this payload and associated applications among commercial organisations. Although a significant minority of drone industry representatives who answered this question indicated that their drone did not collect images of members of the public (45%), the majority (55%) stated that their systems either did capture such images or that they did not know. Furthermore, 97% of respondents indicated that the data captured by the drone was recorded, and 71 respondents (76% of those who answered this question) indicated that the data recorded by the drone was stored. Storage times varied from 20 minutes to "indefinitely" and "until it is deleted". However, others indicated that the data and responsibility for storing or deleting it was turned over to the client.

Industry representatives are primarily focused on the technical capabilities of their drones and the skills needed to operate them effectively. As a result, most drone industry representatives are not well informed about European and national privacy and data protection regulations. Sixty-five per cent of respondents characterised their understanding of European privacy and data protection regulations as "basic" or "poor". Half of the respondents characterised their understanding of national privacy and data protection regulations as very good or good, while the other half described them as basic or poor. In total, the most common answer for both questions was that the respondent had a basic understanding. However, drone industry representatives did indicate that they had a comparatively better understanding of national legislation than European legislation.

This is supported by participants' reports on the data protection and privacy issues raised by their use of drones. Although the majority of industry respondents indicated that their drones captured images of members of the public, and that this data was recorded and stored, the majority of respondents also indicated that their use of drones did not raise any privacy or data protection issues. Specifically, 62% of drone manufacturers and operators indicated that their drone did not raise such issues. In conversations with drone industry representatives, many indicated that this finding may be related to the fact that most commercial applications do not focus on people on the ground and that any incidental capture of images of members of the public was often limited to "the tops of their heads".

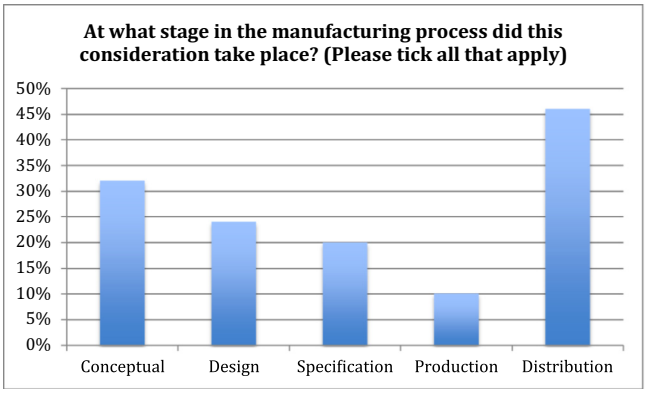

Fig. 2 – Impact assessment in the manufacturing process.

Despite the perceived lack of privacy and data protection issues relevant to the development and deployment of drones, many organisations had undertaken internal procedures to address these issues. Sixty-one per cent of drone manufacturers and 57% of drone operators who answered these questions indicated that they had considered the privacy and data protection issues associated with their drone. For manufacturers, this took place during the conceptual and design phase, with another interesting up-tick in the distribution phase, indicating that some drone manufacturers took responsibility for how the drone may be used once it left their control (Fig. 2).

When asked how this consideration took place, both drone manufacturers and operators indicated that risk assessment and codes of conduct were the most popular instruments used to conduct this assessment (Fig. 2).

Figs. 3 and 4 indicate that some instruments for conducting privacy or data protection assessments are more popular than others. Comparatively, operators appear more likely to conduct such assessments than manufacturers; however, the survey results indicate that for the majority of industry representatives who responded to the survey, such assessments are familiar and could be rolled out to a larger group of drone manufacturers and operators.

Although not widely reported, some of the "fixes" associated with addressing privacy or data protection issues include processes such as scrubbing, anonymisation and pilot training.

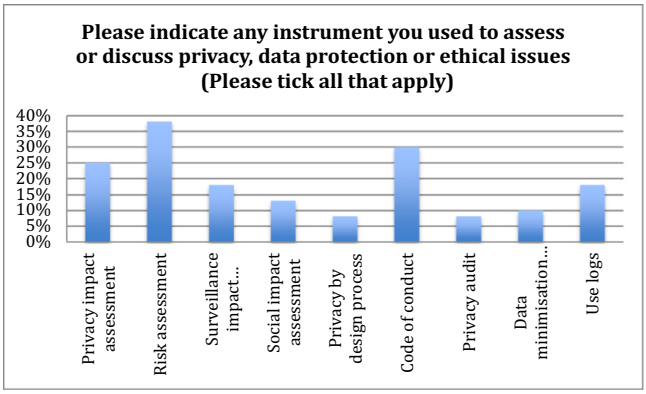

Fig. 3 – Privacy and DP impact assessment by drone manufacturers.

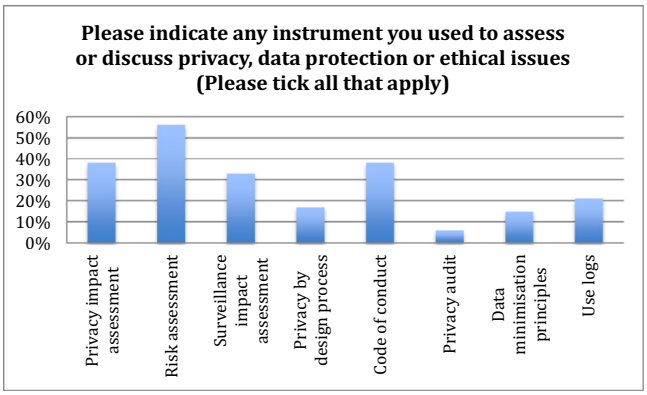

Fig. 4 – Privacy and DP impact assessment by drone operators.

For example, in the comments section of the questionnaire, one UK drone proprietor described how the scrubbing of images of people worked in practice. "Members of public only very rarely captured by accident at small unidentifiable size in background. All images are checked at editing stage and people removed from image." In relation to anonymisation, one Spanish respondent described blurring images of people or vehicles. Another respondent described a pilot operation assessment procedure, which included a "risk assessment that includes data capture and privacy issues. Flight operation considers how to capture enough data to complete the job without excessive data capture." Thus, some organisations are taking measures to deal with privacy, data protection and ethical issues.

Nevertheless, the survey data indicates that true understanding of these issues is lacking. Specifically, reports that operations do not raise privacy or data protection issues despite capturing members of the public on film, recording those images and storing them, sometimes indefinitely, indicate that industry's understanding of these issues could be improved. This is supported by 70% of respondents' indication that clear guidelines on privacy and data protection issues would assist them in their work (Fig. 5).

Thus, there is significant scope for improving the privacy and data protection advice offered to drone industry representatives, particularly in relation to educating those who do not think privacy and data protection issues are relevant to their work. While this would be particularly useful for those who are operating drones professionally, and who take seriously their obligations under current legislation, drone industry representatives also point out that there is a significant minority of operators, in particular, who operate outside, or without consideration of, the law in this area. In these cases, better enforcement of existing regulations would be most beneficial.

In summary, while many industry representatives believe that privacy and data protection issues are not relevant to their work, a significant number of respondents indicated that their drones capture and record images of members of the public and that those images are stored and/or transferred to other organisations. This means that their use of drones is capturing personal information and thus subject to data protection legislation. However, many organisations appear unaware that the information they are collecting introduces obligations related to data protection. While some organisations are evaluating the privacy and data protection impacts of their operations, these practices must be expanded using some form of encouragement or regulation.

5. Risky operators

This section examines other stakeholders' understandings of the privacy, data protection and ethical risks raised by the use of drones in civil applications, specifically the opinions of European data protection authorities and civil aviation authorities, as well as civil society organisations, in Europe and beyond. Despite the risks associated with industry's not understanding the intricacies and specificities of European data protection law, many stakeholders viewed commercial organisations' use of drones as less risky to privacy, data protection and ethics than other stakeholders. CSOs, DPAs and CAAs all situated private, recreational users of drones as the most risky operators;

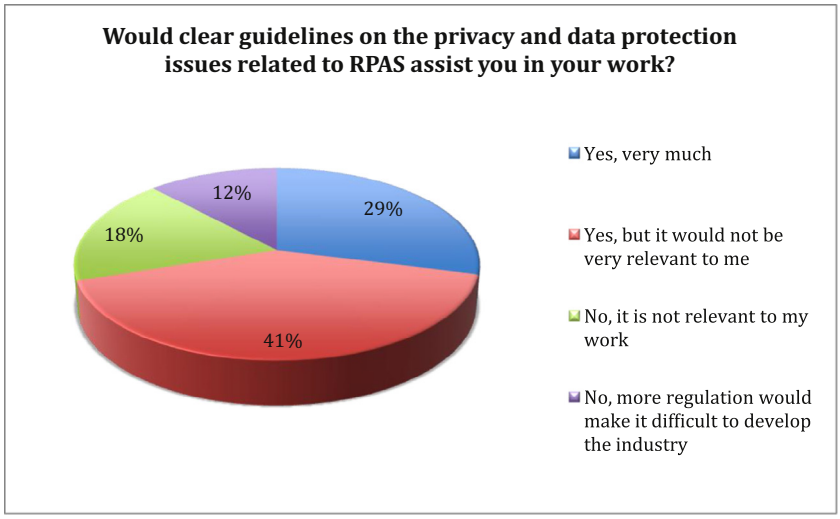

Fig. 5 – RPAS industry interest in guidelines.

however, these relative risk profiles differed between the stakeholder organisations consulted.

This discussion focuses on questions for DPAs, CAAs and CSOs that enquired about potential privacy, data protection and ethical "risks" using the following example scenarios: law enforcement using drones for surveillance, commercial organisations carrying out infrastructure inspection and private individuals using drones for recreational purposes. In each case, privacy was characterised by risks to the following: respect for home and family life and respect for communications (as enshrined by the Charter of Fundamental Rights of the European Union) as well as the right to be let alone, a more common-law understanding of privacy originating in US legal opinions. With respect to data protection, these risks were characterised by issues related to the following data protection principles:

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

The examination of ethical issues focused on various elements that were related to privacy and data protection, but fell outside their specific scope. The surveys examined ethical issues such as discrimination, a chilling effect, a dehumanisation of the surveilled, public dissatisfaction and function creep. DPA and CSO respondents were asked about each of these elements individually, as they were thought to have greater expertise in this area and more in-depth knowledge. CAAs were only asked about privacy, data protection and ethics in general. As such, for the purposes of this article, the DPA and CSO responses for privacy, data protection and ethics have been aggregated within each category to make them comparable to the CAA responses.

Aggregating the data from across all three of the stakeholder categories demonstrates that *all* civil drone operations are thought to carry significant potential privacy, data protection and ethical risks. Few DPA, CAA or CSO respondents thought that the example operations were categorised as "low risk" for privacy, data protection or ethics. Instead, almost every operation was categorised as either medium or high risk, as Fig. 6 demonstrates.

This chart highlights that while law enforcement operations and the use of drones by private individuals are more likely to be identified as "high risk", commercial operations are most likely to be judged "medium risk". Commercial operations are also more likely than other types of operations to be categorised as "low risk", although this characterisation was least frequent across all categories of operations.

Nevertheless, there was nuance to this construction, where different categories of respondent judged the relative risks associated with each category of user slightly differently. Private users were most likely to be deemed high risk rather than medium or low risk by all categories of respondent. However, other categories of drone operator were also located as high risk, depending upon the type of respondent. DPAs were more likely to judge all categories of drone operator as representing a potentially high risk to privacy data protection and ethics, although private users were most likely to be categorised as high risk (Fig. 7).

In contrast, CAA respondents almost exclusively located private users as the only category of drone operator that posed a high risk to privacy, data protection or ethics (Fig. 8).

CAAs seemed to believe that it was unlikely that law enforcement and commercial users would pose a high risk in this area. In contrast, civil society organisations were more likely than any other categories to view law enforcement drone operators as posing a high risk to privacy, data protection and ethics.

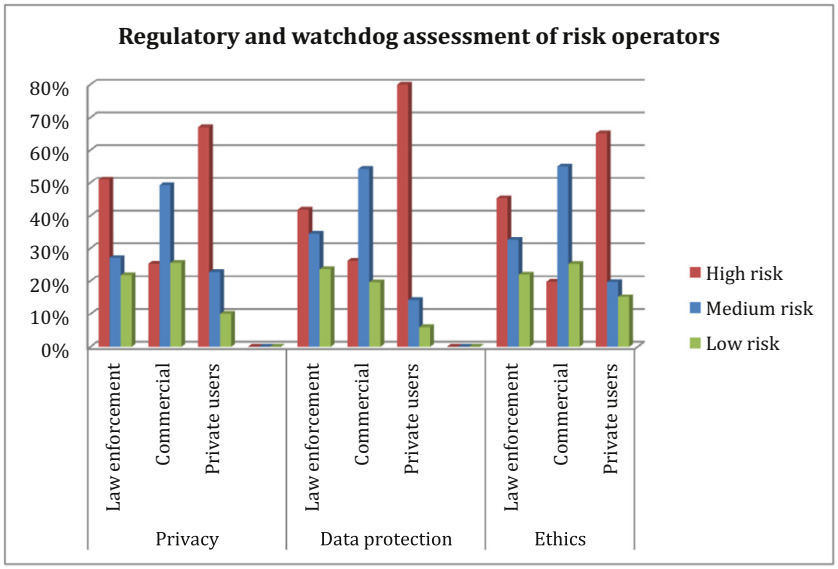

Fig. 6 – Privacy, data protection and ethical risks of civil drone operations.

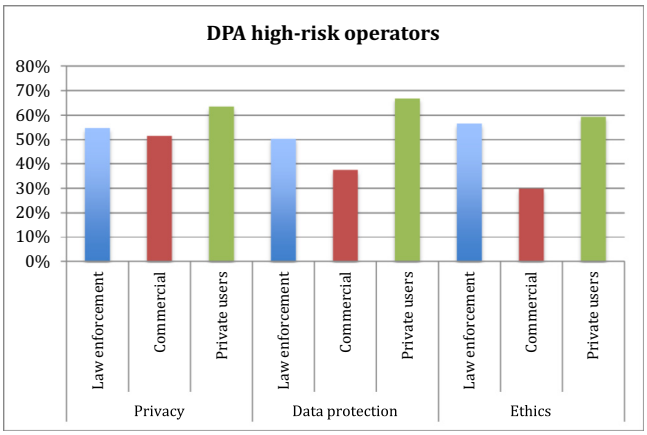

Fig. 7 – DPA high-risk drone operators.

For CSOs, law enforcement operators appear to be more likely than other types of operators to be judged high risk, although commercial operators are also likely (Fig. 9). Across all the respondents, commercial organisations were least likely to be identified as posing a "high risk" to privacy data protection and ethics, although Fig. 6 indicates that they are most likely to be deemed a "medium", and still significant, risk.

This section demonstrates significant concern among regulators and watchdogs about the potential privacy, data protection and ethical risks associated with the civil use of drones. All categories of respondents deemed some operator categories to be high risk, with private, recreational users being most likely to be judged high risk across all respondents. However, the identification of high-risk operators was distributed differently according to which type of organisation was answering the question. DPAs were likely to judge law enforcement, commercial and private operators as being high risk, while CAAs and CSOs were most likely to categorise private individuals and law enforcement operators as being high risk. This suggests a fragmentation in these organisations' perceptions of high-risk operators, which can potentially impact the focus and targets of their regulatory activities or awareness-raising campaigns. It also suggests that all categories of drone operators should be targeted by any awareness-raising or regulatory activity related to privacy, data protection and ethics.

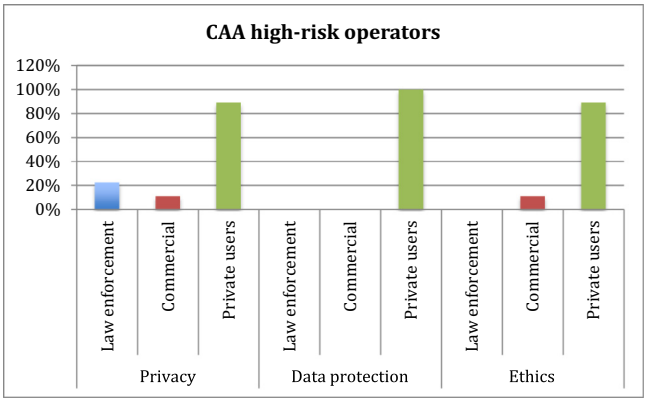

Fig. 8 – CAA high-risk drone operators.

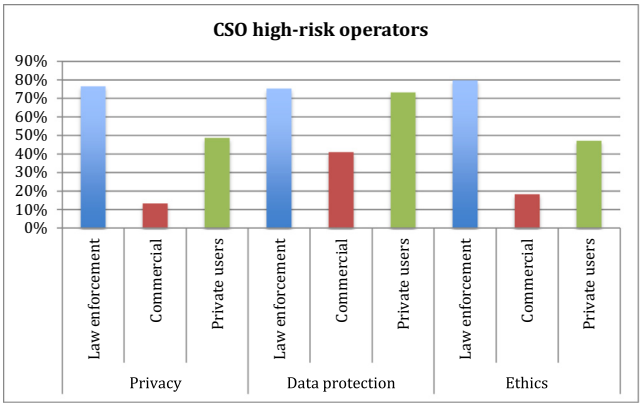

Fig. 9 – CSO high-risk drone operators.

6. Regulatory oversight

The results of this survey have indicated some important insights for the regulation of civil drones with respect to privacy, data protection and ethical issues. They are situated within a tension between what is necessary to address the diversity of drones and their operators and operations, and what is necessary to provide strong protections for members of the public. In particular, while some previous research has argued that soft-law measures such as privacy impact assessments, codes of conduct and others are most appropriate for drone operations, given the diversity with which drone practice is characterised (Finn and Wright, 2012; Wright and Finn, 2016), Clarke (2014) has already noted that such industry self-regulation and soft-law measures are woefully inadequate to provide strong protections for citizens. These survey results exemplify and add important texture to this tension.

The survey results demonstrate that there is a need for awareness-raising and toolkits to assist commercial and recreational drone operators to adequately address privacy, data protection and ethical issues. Commercial drone operators report that they do not have a good understanding of legislation in this area, and it follows that they do not have a good understanding of the principles associated with responsible manufacturing and operation. Their answers to the survey questions indicate that they do not adequately understand the contextual nature of privacy, data protection and ethics, nor the relevant legislative specificities. Instead, they focus on the fact that their operations are not focused on people, that any capture of images of persons are incidental and often limited to the tops of people's heads. However, this incidental capture of images appear to breach some data protection principles, including but not limited to consent, transparency, data minimisation, proportionality and purpose limitation, particularly when these images are recorded and stored. Furthermore, breaches of these data protection principles may result in privacy or ethical breaches. For example, the commercial operators appear to assume that images of the tops of people's heads are anonymous and not subject to data protection regulation, yet when the footage is turned over to the client, those images may be of recognisable employees. This could raise issues related to function creep or privacy of behaviour, privacy of association and others.

In addition, it is clear that private individuals using drones for recreational purposes are in need of easily digestible information about privacy, data protection and ethical issues. All of the categories of respondents judged private operators to be the most "risky" in terms of breaches in these areas. This is also complicated by a somewhat grey area of legislation as a result of the clarification of the household exemption of the Data Protection Directive and proposed changes to European data protection law under the proposed Regulation. In either case, recreational users might find themselves liable for breaches. The survey results demonstrate that professionals do not have a clear understanding of these issues, and it is likely that recreational users do not either. As such, further research in this area should examine the extent to which private, recreational operators understand their obligations and good practice principles. In the meantime, it is imperative to provide private, recreational users with an accessible and comprehensive set of guidelines for using drones that allows them to educate themselves and protect themselves from liability. The US has produced an information portal targeted at different types of users, but the advice offered is very high level (Know before you fly, 2015). The EC is also supporting, via the DroneRules.eu project, the development of a European portal that will have additional functionalities, including scenario-based information and languages other than English.

The survey results also demonstrate a diversity of drone operations, both now and in the immediate future, which underpins the argument that bespoke and contextual assessments of drone operations conducted by operators and manufacturers are the best way to encourage responsible drone use. The results demonstrate that drones come in many shapes and sizes, carry many different payloads and are used by or sold to different types of operators for different purposes and in different contexts. Drones are also expanding beyond flying vehicles, which will likely raise additional privacy, data protection and ethical issues. Furthermore, manufacturers are interested in expanding their capabilities, including making additions to or improvements in the payloads that they carry. A diversity in client contracts means that in some cases, drone operators function as the controller of the data that is collected, while in others they turn the data they collect over to the client. Each of these elements has implications for the privacy, data protection and ethical impacts of the operation of the drone, which would thus require an assessment mechanism that is flexible enough to undertake a multi-dimensional evaluation. Furthermore, those operating the drone would be in the best position to understand and evaluate the context within which they are operating, possibly in partnership with the client where relevant.

The findings also make clear that there is a significant subset of responsible operators who are undertaking assessments of privacy, data protection and ethical issues. In addition to awareness-raising, manufacturers and operators undertaking these assessments need tools to help them understand the issues raised by their devices or operations, particularly given potential misunderstandings of the legal framework. Given the necessity to consider drone operations in context and the dynamic nature of drone development, these assessments must go beyond simple privacy or social impact assessment templates. Instead, they must raise specific questions around key privacy, data protection and ethical principles, and encourage those undertaking the assessment to think like persons on the ground that may be impacted by the operations. This is particularly important as many drone manufacturers and operators are small organisations, including sole proprietorships, and their resources are focused on the core of their business (e.g., drones and their operations), not privacy, data protection and ethics. Expecting small organisations to develop enough expertise in these areas to adequately protect themselves and the public is overly ambitious. The EC portal intends to include tools, including a comprehensive, interactive PIA template that could help such small organisations.

As Clarke (2014) has noted, however, soft-law measures are not enough to provide strong protections for individuals on the ground. Nevertheless, more comprehensive legislation and regulation for the use of drones will be difficult for three reasons. The survey results from regulators and watchdogs suggest a potential strength in that different regulatory and awareness-raising organisations may be focused on issues related to specific types of operators, providing broad coverage when these organisations work simultaneously. For example, CSOs are focused on law enforcement and CAAs are focused on private individuals, while DPAs seem to have a broader focus. The first implication is that no single organisation has authority over the regulation of these issues and no comprehensive legislative framework currently exists to cover all three of the different types of operators examined here (although the proposed GDPR is moving in this direction). As such, any regulatory scheme would be fragmented. CAAs currently only have authority over the air-worthiness aspects of drones, and at best only ask potential operators to certify that they have considered privacy, data protection and ethical issues. DPAs have authority over commercial organisations; however, there are significant gaps with respect to their authority over law enforcement and private users. Additionally, CSOs' role is almost totally restricted to awareness-raising, although some organisations do bring lawsuits related to particular issues. Second, legislation should be technology neutral both to provide a broad coverage and to keep pace with changing technological developments. As such, legislation specific to drones is somewhat problematic; particularly as drones themselves are something of a moving target. Finally, many regulatory organisations and CSOs are under-resourced, making any type of meaningful enforcement of privacy and data protection breaches difficult as these organisations will more likely focus on major targets rather than small organisations or individual drone operators. This is not likely to change with the GDPR as DPAs' role will likely be augmented without an associated budgetary injection.

These regulatory difficulties suggest that the development of good practice principles and support for contextual assessment is more likely to achieve success in supporting responsible practice, albeit with a recognition that these methods will always be dependent upon manufacturers and operators themselves. Some DPAs have moved out in front of this and have included advice about professional and recreational use of drones in specific guidance documents or websites (see, for example, United Kingdom Information Commissioner's Office, 2015). Another possibility is to educate members of the public, particularly through public service messages that can let people know what their rights are with respect to the use of drones in civil air space. In addition, bringing different regulatory and watchdog

organisations together to provide a more comprehensive picture of risky operators and operations would also benefit the overarching regulation and monitoring of privacy, data protection and ethical issues.

7. Conclusions

This article has presented findings from a European survey of drone industry, regulators and civil society organisations to provide information about the drone industry and its potential regulation. The article indicates that the drone industry is significantly fragmented, and that the drones produced by the industry are diverse as is their potential payloads and applications. The article also illustrates that although many responsible professional operators exist, there are significant gaps in the industry's knowledge about their privacy, data protection and ethical obligations under European and national laws. In particular, operators do not appear to be adequately aware of the contextual nature of privacy and data protection issues and, as such, assume that any operations that capture images of members of the public incidentally do not raise privacy and data protection issues.

However, the regulation of such issues is not straightforward. There is no over-arching legislative framework to cover the use of drones by law enforcement, commercial and recreational operators. Furthermore, different regulators and watchdogs construct different risk profiles for different types of operators. As such, different organisations will focus on different types of operators and operations, further exacerbating already existing fragmentation. While it is clear that more comprehensive regulation would offer more robust protections for members of the public, the diverse characteristics of drones, their capabilities and applications make such comprehensive regulation nearly impossible. Instead, the article argues that bringing these regulatory and watchdog organisations together, encouraging greater interaction between them, and simultaneously providing better educational mechanisms for drone operators and members of the public appear to be more viable ways to support a meaningful intervention into the risks associated with civil drone use.

Acknowledgement

The authors gratefully acknowledge funding from the European Commission through the EU programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises (SMEs) (COSME). The views in this paper are those of the authors and are in no way intended to reflect those of the European Commission.

REFERENCES

Aldridge A, Levine J. Surveying the social world: principles and practice in survey research. Buckingham: Open University Press; 2001.

Article 29 Data Protection Working Party. Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones. 01673/15/EN, WP 231, 16 June, 2015.

Clarke R. The regulation of civilian drones' impacts on behavioural privacy. Comput Law Secur Rev 2014;30:286–305.

Clarke R, Moses LB. The regulation of civilian drones' impacts on public safety. Comput Law Secur Rev 2014;30:263–85.

Culver KB. From battlefield to newsroom: ethical implications of drone technology in journalism. J Mass Media Ethics 2014;29(1):52–64.

De Vaus D. Surveys in social research. London: Allen and Unwin; 1990.

European RPAS Steering Group. Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System: ANNEX 1. 2013.

Finn R, Wright D, Friedewald M. Seven types of privacy. In: Gutwirth S, Leenes R, De Hert P, Poullet Y, editors. European data protection: coming of age? Dordrecht: Springer; 2013. p. 3–32.

Finn R, Wright D, Donovan A, Jacques L, De Hert P. Privacy, data protection and ethical risks in civil RPAS operations. European Commission; 2014 <http://ec.europa.eu/DocsRoom/documents/8550>.

Finn RL, Donovan A. Big data, drone data: privacy and ethical impacts of the intersection between big data and civil drone deployments. In: Custers B, editor. The future of drone use. TMC Asser Press; 2016 forthcoming.

Finn RL, Wright D. Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Comput Law Secur Rev 2012;28:184–94. <http://www.sciencedirect.com/science/article/pii/S0267364912000234>.

František Ryneš v Úřad pro ochranu osobních údajů [2014], Case C-212/13. EU:C:2014:2428. 2015.

Hoinville G, Jowell R. Survey research practice. London: Heinemann; 1978.

Know before you fly. Recreational users. 2015. <http://knowbeforeyoufly.org/for-recreational-users/>.

Lyon D. Surveillance studies: an overview. Cambridge: Polity Press; 2007.

Martin A. Occupy Wall Street has a drone: the occucopter. The Wire, 7 Dec, 2011. <http://www.thewire.com/national/2011/12/occupy-wall-street-has-drone-occucopter/45891/>.

Meier P. Developing guidelines for humanitarian UAV missions. iRevolution.net, 21 July, 2015. <http://irevolution.net/2015/07/21/developing-guidelines-for-humanitarian-uav-missions/>.

Moynihan T. The drone racing league will be a spectator sport like no other. Wired.com, 21 Nov, 2015. <http://www.wired.com/2015/11/drone-racing-league-spectator-sports/>.

PrecisionHawk. Better data for smarter business decisions. 2015. <http://PrecisionHawk.com>.

Salter M. Toys for the boys? Drones, pleasure and popular culture in the militarisation of policing. Crit Criminol 2014;22:163–77.

Sandbrook C. The social implications of using drones for biodiversity conservation. Ambio 2015;44(4):636–47.

United Kingdom Information Commissioner's Office. Drones. 2015. <https://ico.org.uk/for-the-public/drones/>.

Unmanned Aircraft Systems (UAS) Registration Task Force (RTF) Aviation Rulemaking Committee (ARC) (Task Force). Task force recommendations final report. 21 November 2015 <https://www.faa.gov/uas/publications/media/RTFARCFinalReport_11-21-15.pdf>.

Wright D, Finn RL. Should drones be subject to privacy impact assessments? In: Custers B, editor. The future of drone use. TMC Asser Press; 2016 forthcoming.