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,