"TOO MANY EYES IN THE SKY:" THE IMPACT OF PRIVATE SECTOR DRONE USE ON THE RIGHT TO PRIVACY AND DATA PROTECTION

Search Words

Drones, RPAS, data protection, privacy, surveillance, emerging technology, European law, European Convention on Human Rights, Data Protection Directive, general data protection regulation, private sector.

Kate O'Malley[1]

ABSTRACT

The once-looming prospect of expanded use of Remotely Piloted Aircraft Systems (RPAS, or colloquially drones) into non-military operations has now become reality. Although not a new phenomenon,[2] the influence of new technology, which has characterised the 21st century, has seen the use of RPAS expanding into the commercial, non-commercial and governmental sectors. This essay will consider how the use of RPAS will impact on a person's right to privacy and data protection, and it will analyse to what extent the legal framework of the European Union on privacy and data protection is applicable and adequate to protect infringement of these rights by RPAS. It will also consider the proposed General Data Protection Regulation in the context of RPAS, before reaching the conclusion that the existing legal regime needs to be updated to ensure that an integration of RPAS into national airspace does not interfere with personal rights.

1 INTRODUCTION

'[P]rogress has never been a bargain. You have to pay for it. Sometimes I think there's a man who sits behind a counter and says, "Alright, you can have a telephone, but you lose privacy and the charm of distance... Mister, you may conquer the air, but the birds will lose their wonder and the clouds will smell of gasoline."' [3]

The current integration of RPAS into more and more aspects of everyday life has been met with mixed reviews. RPAS are unmanned aerial vehicles, with a vast range of sizes, which are

---

1 Junior Sophister, LLB Candidate Trinity College Dublin.

This author wishes to thank and acknowledge the guidance of Jens Kremer, lecturer in the Faculty of Law, University of Helsinki and the editorial team at the Helsinki Law Review. All errors and omissions remain the author's own.

2 Drones have been used by the US military since the 1930s; See Cole 2014.

3 'Inherit the Wind', 1960, motion picture, the United States of America.

controlled by 'pilots' on the ground.[4] For the purpose of this essay, RPAS will be referred to by their more colloquial term, drones.

On the one hand, there are the almost unquantifiable advantages drones can offer to society. The European RPAS Steering Group advocates that emerging drone technology can contribute to boost industrial competitiveness, promote entrepreneurship and create new businesses, which will generate growth and jobs.[5] Drones have the undeniable potential to offer a myriad of benefits across a growing number of sectors – from agriculture to security, from delivery to emergency services, from journalism to scientific research, from advertising to audio-visual film-making.[6] Thus their proliferation into everyday use is unsurprising.

However, on the other hand, when we accept the conveniences of modern drone technology, in the specific context of surveillance, it is argued that it comes at a price; our privacy. It can be said that the point of the legal framework in this context is to ensure a fair transaction, to ensure the scales are balanced when weighing technological advances against the right to privacy. Too rigid an approach would dilute the benefits offered by drones, stifle innovation, and slow down the current competitiveness in the European drone industry, while too broad an approach could result in legitimising gross invasions of an individual's right to privacy.

This essay will examine how commercial and non-commercial use of drones in public places impacts on an individual's right to privacy and data protection rights. It will firstly assess the impact of drone-based surveillance on privacy, comparing it with traditional forms of surveillance and demonstrate how drone-based surveillance has the potential to interfere with an individual's privacy to a greater extent. Secondly, it will analyse the current and projected legal frameworks within the EU, which can offer protection from interference by drones to an individual's privacy and data protection rights. This section will be split into two parts; it will look first at the right to privacy in the sense of privacy as a person's private sphere, and secondly it will look at the legal framework concerning data protection. In this section the scope of applicability of the legal framework to drone-based surveillance will be discussed, as well as an analysis of the adequacy of protection offered. Finally, a conclusion will be drawn emphasising that while the current and

---

4 Australian Certified Operators Inc. - http://www.acuo.org.au/industry-information/terminology/what-do-we-call-them/, accessed 2 January 2015.

5 European Commission, 2013, *http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf*, accessed 2 January 2015; Also, a US industry study forecasts that in the first three years of RPAS integration in the national airspace more than 70,000 jobs will be created with an economic impact of more than $13.6 billion. The number of jobs created through new RPAS activities in the US is estimated to exceed 100,000 by 2025. For Europe, about 150,000 jobs by 2050 are forecasted excluding employment generated through operational services. See, Commission, 'A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner' (Communication) COM (2014) 207 final.

6 Voisin 2013.

projected privacy protecting legal framework can certainly be applied to cases of drone-based surveillance, it is harder to determine the adequacy of the framework when faced with the challenged posed by drones, and much depends on the approach taken by the Court of Justice of the European Union and the European Court of Human Rights. It is submitted that the main task lies in ensuring that any approach taken by legislators or judges should focus on the effects of the surveillance, as opposed to the means of surveillance, because in that way the law has a better chance of keeping up with the rapid technological advancements of the 21st century.

2 HOW DO DRONES CHALLENGE THE RIGHT TO PRIVACY?

Privacy has been a key factor in the critique of drones and 'new-surveillance' technologies alike[7]. Despite this, the concept of privacy is not an uncontested one. The origins of the right to privacy lie in the celebrated article by Warren and Brandeis "The Right to Privacy", which articulates the right to privacy as a "right to be left alone".[8] Years later Whitman describes it as 'an unusually slippery concept'[9] and, more recently still, Solove describes privacy as 'a concept in disarray', and that it is best understood as a family of 'different yet related things'.[10] So although a widely accepted definition of privacy remains elusive, there has been more of a consensus on a recognition that privacy comprises of multiple dimensions[11], and that there exists a 'private sphere' where individuals are entitled to a reasonable expectation of privacy.[12] Roger Clarke defines these dimensions as privacy of the person, privacy of personal data, behavioural privacy, and privacy of personal communication.[13] The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, has favoured a definition of privacy as articulated by Lord Lester and D. Pannick:[14]

"Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with

---

7 Gary Marx characterises new surveillance as data gathered from new forms of technology that has low visibility, and is more likely to be involuntary, automated, and remotely collected. The information is gathered from categories of interest rather than a subject, there is an increase in the amount of data collected, and the data is usually real-time. 'What's New About the "New Surveillance" Classifying for Change and Continuity' (Surveillance and Society, 2002), http://www.surveillance-and-society.org/articles1/whatsnew.pdf, accessed 8 January 2015.

8 Warren and Brandeis 1890, p.193.

9 Whitman 2004, p. 1151.

10 Solove 2008, p. 12.

11 Finn and Wright 2012, p. 184.

12 Stanford Encyclopedia of Technology - http://plato.stanford.edu/entries/privacy/, *accessed 8 January 2015.*

13 Clarke 2013.

14 UN special rapporteur report.

others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[15]

For the purpose of this article, Lester and Pannick's definition of privacy will be preferred. The non-uniform use of the term privacy is, however, potentially problematic; if there remains confusion over the concept, scope and value of privacy,[16] legislation protecting privacy will prove harder to be created and enforced.

3 RPAS AS A SURVEILLANCE TOOL: ANOTHER BRICK IN THE WALL?

This section is addressing how drones operate, and compares drones to traditional forms of surveillance. When so doing, it determines why the use of drones has sparked such a debate on the threat they pose to privacy and data protection.

Drones were primarily developed in the context of military operations, although non-military drones are being increasingly integrated into the civil and commercial sphere. Though the first non-military uses of drones were undertaken by governmental authorities, notably police and intelligence agencies,[17] the focus of this article concerns private sector use. In the commercial sector this includes businesses, corporations or professionals, such as journalists. Retail users are also increasingly interested in the monitoring capabilities of drones, from security measures to recreational activities.[18] Although much literature focuses on the governmental use of drones, the Commission's RPAS Final Privacy Report suggests that it is the anticipated use of drones by the private sector and citizens that will likely pose the greatest threat to privacy, as the use of surveillance by these sectors of society is less regulated.[19] Thus, in order to assess the impact of drone surveillance on privacy it is prudent to address whether the use of drones is "just another tool in the toolbox"[20] of traditional aerial or visual surveillance by helicopters or closed-circuit television (CCTV) respectively, or whether it brings a new dimension to the nature of surveillance.

This author is an advocate of the latter; opining that the complexity of drone technology characterises it as a 'new technology'.[21] A unique feature of a drone is its ability to be equipped with

---

15 Lester and Pannick 2004, para. 4.82.

16 Stanford Encyclopedia of Technology - *http://plato.stanford.edu/entries/privacy/, accessed 08 January 2015.*

17 RPAS report, p. 24.

18 European Commission, 2014, p. 24.

19 Ibid.

20 Nevins 2011.

21 Gary Marx characterises this as surveillance data gathered from new forms of technology, that

a 'payload', which, in the context of this essay, includes advanced sensors to process different types of surveillance i.e. physical surveillance, surveillance of communications, dataveillance, tracking and body surveillance. Mounted with these technologies, drones can engage in, inter alia, facial recognition, license-plate recognition and automated object detection, intercept electronic messages, detect abnormal or 'antisocial' behaviour and use enhanced image resolution to magnify their operator's capacity to observe.[22] It's argued that the greater the advancement in technologies, the greater the drone's ability to invade privacy. Compared to CCTV systems, which are fixed and confined to public places, a drone poses a greater threat to privacy due to its mobile capability. It can offer new angles for visual surveillance, can be deployed without delay to follow an individual or vehicle, and can monitor in locations, which do not require access to the premises. While helicopters can carry out aerial surveillance and have many similar technological enhancements, the noise and mass of alone of such an aircraft prevent the surveillance being carried out in secrecy. The characteristics of drones thus make them a unique tool for covert surveillance.

On this point, the UK Information Commissioner correctly identified that an issue with drones in public spaces is that the data subjects are usually unaware they are being recorded, and the surveillance is often highly intrusive because they can capture images of individuals unnecessarily. Even where individuals may not be directly identifiable by the image captured by the drone, they may be identified by the context they are captured in, or through enhanced resolution zooming technology later applied to the data.[23]

In addition to their technical and physical superiority to other forms of surveillance, drones are becoming increasingly cheaper than any other surveillance system, meaning that any economic barriers, which existed to the proliferation of drone users for aerial surveillance will disappear, and a shift in the actors of surveillance will occur. While military, police and other governmental use of drones will continue to be deployed, the world of drones is becoming more accessible to an increasingly wider variety of organisations and individuals. Due to the affordability of drones and their payloads, drones are contributing to the recent phenomenon of 'privatization of surveillance'[24] Schlag observes that "many privately owned companies already use or have expressed interest in obtaining drones for security, loss prevention" and to "survey property,

---

has low visibility, and is more likely to be involuntary, automated, and remotely collected. The information is gathered from categories of interest rather than a subject, there is an increase in the amount of data collected, and the data is usually real-time - *http://www.surveillance-and-society.org/articles1/whatsnew.pdf,* accessed 8 January 2015.

22 Schlag 2013, p. 1.

23 http://www.out-law.com/en/articles/2014/october/filming-using-drones-must-comply-with-data-protection-laws-says-ico/, accessed 8 January 2015.

24 European Commission, 2014, p. 26.

secure premises or monitor employees".[25]

Thus the evidence above suggests that drones will change the nature of surveillance, and pose a greater threat to privacy. It is submitted that drones, by their nature, present a unique threat to privacy as they "are designed to undertake constant, persistent surveillance to a degree that former methods of surveillance were unable to achieve,"[26] and they could in fact be "transformative in the way they conduct surveillance".[27] An increase in the users of the new surveillance technology only exuberates that threat. That said, however, new users of drones should not be deprived of their freedom to operate them legally, and the duty is on the EU and its Member States to develop laws, which allow the operation of drones while controlling this threat to privacy.

4 THE LEGAL FRAMEWORK OF THE RIGHT TO PRIVACY AND THE RIGHT OF DATA PROTECTION IN EUROPE

4.1 Some introductory remarks on the Legal Framework

It is often said that Europe has a comprehensive legal framework surrounding privacy. This current, extensive regulation of matters concerning privacy in Europe is often justified with reference to continental experiences under extremist governments in the World War II era and Cold War communist regimes, pursuant to which Europeans retain a somewhat suspicious perception of unchecked uses of personal information.[28] With the dawn of the information society European guardedness concerning surveillance and the collection and retention of personal data has intensified, and arguably extended to a distrust of corporate and government databases.[29]

The emergence of drones capable of carrying out such covert surveillance has thus been regarded rather warily by some. However, it is submitted that the extent of the current legal framework on privacy, as well as new privacy regimes due to come into force, are adequate to protect and safeguard citizens' right to privacy in the context of drone-based surveillance.

The following section will analyse the extent of European framework on, firstly, the general concept of privacy and in its sense of a 'private sphere', and secondly, on data protection. It will

---

25 Schlag 2013, p. 1.

26 Epic.org - http://epic.org/privacy/drones/, accessed 8 January 2015.

27 Courtland 2013.

28 Bennett 1992, p. vii.

29 For example, the Court of Justice of the European Union declared Directive 2006/24/EC on the retention of Data to be invalid on 8 April 2014, which provided for the retention of data by providers of publicly available electronic communications services or networks in providing their service, because it was considered to be a disproportionate interference with the fundamental rights to respect for individual privacy and protection of personal data guaranteed by Articles 7 and 8 of the European Charter of Fundamental Rights.

also discuss the extent to which these protections can extend to regulate the use of drones in European airspace.

4.2 Legal framework of the right to privacy

The European Convention on Human Rights (ECHR) is one of Europe's most important legal instruments for the protection of fundamental rights. Article 8 of the ECHR explicitly recognises the right to private life, with the first part enunciating the four aspects protected, privacy, family, home and correspondence, and the second part being providing for the possibility of limiting this right, legitimising interference with it in certain circumstances.[30] While these four aspects do not reflect the meaning of privacy in today's society, the European Court of Human Rights (ECtHR) dealt with this issue by holding that "private life is a broad concept which is incapable of exhaustive definition,"[31] thus the meaning of privacy is capable of being broadened along with the norms of society, and any changing circumstances, which can pose a threat to privacy; such as the emergence of drone-based surveillance.

Article 8 explicitly protects individuals when they are in their personal, intimate sphere, which is considered the private sphere.[32] Physical boundaries delineate this sphere from the public sphere, such as the home, personal relationships, and by select fields of information (such as sensitive or personal information).[33] Thus the use of drone technology, which monitors or captures someone in this private sphere, will undoubtedly be a strong interference of Article 8.

The Venice Commission [34] defines a public space as one 'which can be in principle accessed by anyone freely, indiscriminately, at any time under any circumstance'. [35] It further notes that, in public places, individual privacy is similar to the concept of non-privacy because by entering a public place and remaining there, there is an implication that one is aware they will be seen or recognised, and that one's behaviour may be scrutinised by anyone in that public sphere who may draw inferences from the individual's behaviour.[36] It is acknowledging that 'any human being in a public place may well expect a lesser degree of privacy'. Individuals in the public sphere

30 Article 8 of the European Convention of Human Rights states (1) Everyone shall have the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

31 Costello-Roberts v. the United Kingdom 1993, para. 36.

32 P.G. and J.H. v. the United Kingdom 2001.

33 Nissenbaum 1997, p. 207.

34 The Venice Commission is an advisory body of the Council of Europe created in 1990.

35 Venice Commission 2007, p. 3.

36 Ibid., 5.

can still hold privacy expectations, and should not expect or be subject to a deprivation of their rights, however the degree of expectation is lower than if the individual was in the private sphere. Therefore it can be said that Article 8 does apply in a public space, if the individual can reasonably expect a degree of privacy, as in some circumstances there is a zone of interaction of a person with others or the outside world, even in a public context, which may fall within the scope of "private life". [37] It is interesting to note, however, that the degree of privacy a person can expect in a public space does not seem to apply equally to everyone. While the ECtHR has held that even where a person is known to the general public, in certain circumstances he may rely on a 'legitimate expectation' of protection of and respect for his privacy,[38] the notoriety of a person will be taken into consideration in assessing the degree of privacy so afforded to them, i.e. whether or not they can be regarded as public figures.[39] To determine whether the right to private life has been interfered with in a public place, the ECtHR uses the 'reasonable expectation of privacy' test. In P.J. and J.H. v. UK,[40] the Court found:

'A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example a security guard through a closed-circuit television) is of a similar character.' [41]

In Perry v. the UK, the Court held that 'the recording of data and the systematic or permanent nature of the record may give rise to such considerations' as an interference with Article 8(1).[42]

The decisions are practical ones, and they focus on the effect the surveillance has on the right to privacy, rather than the means of surveillance. Because this approach is not product- or technology-specific, it will be easy to apply it to all forms of surveillance technologies that emerge in the future, including drone-based surveillance. In the abovementioned cases, the ECtHR is drawing a distinction between the monitoring of a public space, and the recording of data from a public space in a permanent way, the conclusion being that while the former does not interfere with the right to private life, the recording of sound or visual images in a public place through surveillance methods may interfere with Article 8(1).

Although the surveillance in the abovementioned cases was undertaken by public authorities, it is submitted that the approach taken by the Court can be applied to surveillance activities carried out by any actor, including commercial or private operators. Similarly, while the reaso-

37 P.G. and J.H. v. the United Kingdom, 2001.

38 Von Hannover v. Germany, 2004.

39 Von Hannover v. Germany (No. 2) 2012, para 110.

40 Ibid.

41 Ibid., para 56.

42 Perry v. the United Kingdom, para. 38.

ning of these cases has not yet been applied to surveillance by drone technology, it is submitted that there are many similarities between the issues considered by the Court, and the scenarios envisaged by the use of drones in public places. Considering the conclusion stipulated from the court, notwithstanding the advanced surveillance capabilities of a drone over a fixed surveillance camera or helicopter, it is opined that, through the application of the case law, a drone is likely to interfere with an individual's right to private life, under Article 8(1) of the ECHR if the payload system records the information captured in a public place, and the operator does not subsequently disclose the footage captured.[43]

In Uzun v Germany,[44] the ECtHR established a graduation in the level of interference of Article 8(1) of the ECHR depending on the type of surveillance technologies used, and made a distinction between 'hard surveillance' (visual surveillance, tapping communications) and 'soft surveillance' (location surveillance).

"GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings." [45]

The Court found that GPS devices are less intrusive than video or voice surveillance, and that a party responsible for an infringing act of location surveillance must prove that it ensured "a general protection against arbitrary interference" in order to justify that interference under Article 8(2). [46]

Based on this case law, it is argued that a drone fitted with a sensor capable of reading location data of an individual is likely to be found to be carrying out 'soft surveillance', based on its similarities with GPS technologies. It follows that an operator carrying out soft surveillance will have a greater chance of justifying that interference under Article 8(2) of the ECHR than if they were conducting hard surveillance. This approach embodies a form of the proportionality principle, in that the surveillance that encroaches rights less (i.e. the soft surveillance) will be easier to justify than the surveillance that causes a more significant encroachment of rights (i.e. the hard surveillance). However, new types of payloads for drones are constantly being developed, and it is submitted that categorising surveillance into either 'hard' surveillance or 'soft' surveillance may be premature, as the line delineating the two may not always be so clear cut.

After the Lisbon Treaty came into force, the Charter of the Fundamental Rights of the EU (Char-

43 RPAS report p. 56; Perry v. the United Kingdom, 2002.

44 Uzun v. Germany, 2010.

45 Uzun v. Germany, 2010, para. 52.

46 European Commission, 2014, p. 59.

ter) has become legally binding on all EU member states, and the provisions of the Charter 'have the same legal value as the Treaties'.[47] This means that the Charter has direct effect in national legal systems, meaning an individual who has had a Charter-right infringed upon by another private individual or corporation can bring a case under the specific article of the Charter before its national court. The Charter is consistent with the ECHR, and when the Charter contains rights that stem from this Convention, their meaning and scope are the same.[48] Article 7 of the Charter recognises the right to private life to all individuals, and contains a copy of the rights guaranteed by Article 8 ECHR, so Article 7 must therefore receive 'the same meaning and the same scope as Article 8(1) ECHR, as interpreted by the European Court of Human Rights'.[49] Thus the scope of Article 7 of the Charter certainly can be applied to privacy concerns raised by drone-based surveillance.

4.3 Legal Framework on Data Protection in Europe

Although data protection and privacy share certain characteristics and interplay, since the emergence of the computer age during the 1960s privacy has no longer been regarded as sufficient to address the issues posed by emerging technologies.[50] While the right to data protection emanated from the rights of privacy, it is said to be more responsive to the specific need to protect citizens from abuses of data processing.[51] In giving practical effect to the overall right to privacy, it can be said that the most prominent aspect of Europe's legal framework is through its regulation of personal data protection through a number of conventions and directives.

An interference with personal data protection occurs if the data that is collected and processed relates to an identified or identifiable person. Applying data protection laws to drones, a distinction arises between data protection and privacy laws, in that data protection legislation will only protect individuals where the drones have collected personal data. The right to privacy is different as it protects people who are monitored by drones in a systematic way or through the means of intrusive payloads, regardless of whether the data is stored.[52]

In M.S. v Sweden,[53] the ECtHR found that "the protection of personal data is fundamental to a

47 Article 6 Treaty of the European Union.

48 Art 53(2) of the Charter of Fundamental Rights of the European Union; however Art 53(2) also enables the European Court of Justice to provide more extensive protection to rights of the European Charter than the rights granted by the ECHR; also, in practice, the interpretations of the two different courts on the same issue have differed in some cases, however this is beyond the scope of this article.

49 O'Neill 2012.

50 De Hert and Papakonstantinou 2009, p. 403.

51 Ibid.

52 European Commission, 2014, p. 61.

53 M.S. v Sweden, 1997.

person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 ECHR."[54] This case highlights the dual functionality of Article 8 ECHR for the purpose of this article, in that it protects both the general right to privacy in its context of a 'private sphere' as well as the protection of personal data. However, the lack of specifics in the provision relating to data processing is problematic. In response to concerns that the wording of Article 8 ECHR was insufficient to protect privacy from all forms of emerging technology, the European Council adopted in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. This included new data protection principles as well as those developed by the ECtHR, and to this day it remains the only binding international legal instrument with a worldwide scope of application in the field of data privacy, open to any country, including those who are not members of the Council of Europe.[55] Although this Convention was formulated well before drones became popular on the private market, because it is both rigorous and adaptive, it is still relevant today to the data collected by drone-based surveillance.

4.3.1 Data Protection Directive

In recognition of a growing need for data protection harmonisation across its member states, the EU adopted the Data Protection Directive[56] (DPD) in 1995. This ensures a balance between a high level of privacy for individuals and the free movement of personal data within the EU.[57]

There is no distinction between public and private life, unlike the right to privacy; the DPD applies to 'the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'.[58] It is submitted that the concept of "automated processing" is a priori broad enough to include payloads fitted to drone technology. [59]

While the DPD applies to both public entities and private companies and parties, data collected by a 'natural person in the course of a purely personal or household activity' does not fall within the scope of the Directive.[60] The meaning of this was explained by the Court of Justice of the European Union in Lindqvist:

"That exception must be interpreted as relating only to activities which are carried out in the

---

54 Ibid., para 41.

55 Council of Europe Privacy Convetion - *https://epic.org/privacy/intl/coeconvention/*, accessed 8 January 2015.

56 Council Directive 95/46/EC.

57 Recital 3 of Council Directive 95/46/EC.

58 Article 3(1) of Council Directive 95/46/EC.

59 European Commission, 2014, p. 63.

60 Art 3(2) of Council Directive 95/46/EC.

course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people." [61]

In Rynes[62], the CJEU ruled that video surveillance by a camera installed in a family home falls outside the scope of this exception, due to the fact that the data collected covers, even partially, a public space, and people walking on the public pathway were identifiable within the meaning of the DPD by the data collected.[63]

The reasoning in these cases can be applied to drone users, and demonstrates that even hobbyists or those using drones for personal security do not fall within the 'household' exemption if the surveillance involved monitors a public space or is capable of processing personal data.

Article 9 of the DPD stipulates that Member States must "provide for exemptions or derogations from some of its provisions where processing is carried out solely for purposes of journalism or the purposes of literary or artistic expression" only if this is necessary to reconcile the right to privacy with rules governing freedom of expression.[64] The wording of this provision is such that it does not give a blanket exemption in every case, but only where 'necessary'. In Satamedia[65], the Court of Justice of the European Union (ECJ) gave a broad interpretation of the phrase 'for purposes of journalism', intending it to cover the disclosure to the public of information, opinions or ideas by any means".[66] Considering civil drones are often used by journalists or in audio-visual fields, this exemption is best applied with caution. If not, there's a risk drones may be used to gather data under the guise of journalistic purpose.

There are also a number of principles encompassed in the DPD, known as the common core principles, to ensure data protection standards when processing data. They are found in Article 6 (data quality) and Article 7 (processing quality). Article 6(1)a provides that data must be collected 'fairly and lawfully', and is only legitimate if one of the conditions in Article 7 is met. If the data subject has not given 'unambiguous consent', a notably high standard reflective of the importance clear consent is regarded as a safeguard against unlawful exercise of surveillance power, the data may still be processed on the condition one of the other conditions in Article 7 are met.

While it is clear that consent is often essential to ensure the lawful operation of surveillance

---

61 Bodil Lindqvist, 2003.

62 František Ryneš, 2014.

63 Ibid., para 33.

64 Article 9 of Council Directive 95/46/EC.

65 Satamedia, 2008.

66 Ibid., para 61.

activities, the weight given to its requirement is uncertain as a result of the other instances. Video-surveillance can be undertaken without the requirement of explicit consent in many cases, because consent is deemed to be implied through the data subject entering public space.[67] Nonetheless, in this situation the data controller still has to comply with the other data protection principles. However these provisions are relatively out-dated to cope with the types of surveillance drones are capable of carrying out. Furthermore, the DPD does not adequately protect the transmission of personal data to outside the EU. This is especially relevant for multi-national companies who operate drones, as data collected in an EU Member State may be transmitted to the headquarters of the company in, for example, the US.

4.3.2 General Data Protection Regulation

The DPD is currently under review, and is due to be replaced by the General Data Protection Regulation (GDPR). The GDPR was formally adopted by the European Parliament in 2014.

Although the GDPR does not contain any drone-specific regulations, some of the new provisions could be relevant in addressing data privacy concerns related to the use of drones, as the aim of the GDPR is to provide for 'a single set of rules technologically neutral – regardless of how technology and the digital environment develop in the future'.[68]

The proposed Article 23 contains two principles, which are likely applicable to the civil use of drones in Europe. Privacy by Design entails adopting privacy-embedding technologies and policies, from design stage and deployment activities, to end use and final disposal. Privacy by Default requires that companies install the strictest possible data privacy settings on a product, so when the data controller receives the product, he or she will have a positive obligation to reduce the privacy setting if they so choose, but the default setting will embody the 'data minimization' principle of having the highest security setting.[69] The Article 29 Working Party commented that the application of these principles to RPAS technology could contribute to better respect for data and privacy and data protection.[70]

A Privacy Impact Assessment system is also included in Article 33 of the draft proposal, and although not defined in the proposal, it makes the controller of the data responsible for the decision as to whether their processing meets the requirements of the GDPR by conducting a Data Protection Impact Assessment prior to dealing with the personal data of their subjects.

As mentioned above, the enforcement of data protection and privacy rules is not easy to achieve,

67 European Commission, 2014, p. 67.

68 European Commission, 2012, accessed 8 January 2015.

69 European Commission, 2014, p. 70.

70 Wong 2011, p. 53.

yet, as David Canton suggests, "if privacy is built into the technology from the beginning, function does not have to be compromised by privacy concerns, and vice versa."[71] Thus it is unsurprising that researchers, lawyers and policy makers have welcomed these new provisions in the context of drones.

5 CONCLUSIONS

The essay presents the privacy and data protection issues that have arisen due to the expansion of drone technology into the non-governmental civilian sector and compares this type of surveillance to traditional aerial, video and audio surveillance. It has clearly demonstrated that drones have the potential to cause greater interference with our right to privacy because of their superiority in surveillance capabilities. This means that concerns surrounding the integration of drones into everyday life are justified. In determining whether there is applicable and adequate legislation in place in Europe to regulate the use of drones from a privacy perspective, it must be acknowledged that the EU has a notable legal framework for both privacy and data protection, of which some were only touched upon within this essay. Article 8 of the ECHR has been the 'historic driver' of the development and expansion of the right to private life in Europe,[72] and if it continues to develop in this way, there is no reason why a sound application of Article 8 will not offer adequate protection from potential privacy infringements by drones. The DPD sets up high-level data protective rules and although it is relatively out-dated and fragmented, there is little room to doubt its provisions can be applicable to drone-based surveillance. However, it is argued that the DPD is unlikely to offer adequate protection of data for citizens because its provisions will not be able to keep pace with the continuously advancing superiority of drone-based surveillance. While much of the current EU framework is not drone-specific, it was found that the majority of the provisions could be applied to such technology. However, due to the potential drones have in infringing on privacy to an extent the EU courts have not previously dealt with, the replacement of the DPD with the GDPR is especially important.

This is a welcome and necessary step to ensuring that privacy is not substituted for the benefits of technological advancements, and vice versa. While the new provisions in the GDPR are in theory likely to provide adequate protection against an interference with personal data because of its technologically-neutral approach, the real effect of the provisions will depend largely on how the CJEU and ECtHR will interpret these provisions in future cases. The GDDPR along with Article 8 ECHR and the numerous other privacy instruments have the potential to be adequate, at least for the time being, to protect the privacy interests of European citizens from drone-based surveillance. However, issues will undoubtedly arise in the future, and when that

71 Canton 2012.

72 Doquir 2008.

time comes perhaps another assessment will be due. To finally conclude, the response to rapid advancements across surveillance technologies lies in ensuring that the legal landscape is a technology-neutral one. Legal guarantees should be in place, which delineates the boundary between acceptable surveillance and surveillance that causes a violation of privacy, data protection or indeed other civil liberties, such as freedom of expression, but which is still flexible enough to cover emerging technologies.

LIST OF REFERENCES

Articles and Books

Bennet Colin J., Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press 1992.

Craig Paul and De Búrca Gráinne, EU Law: Text, Cases and Materials, 5th edn, Oxford University Press 2011.

De Hart Paul and Papakonstantinou Vagelis, The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – A Modest Achievement However Not the Improvement Some Have Hoped For 2009, 25 Computer Law & Security Review 2009.

Doquir Benjamin, Le droit de la vie privée: aperçu général et règles de proportionnalité in B. Docquir and A. Puttemans (Eds.), Actualités du droit de la vie privée, Bruylant Bruxelles 2008 (Doquir 2008).

Finn Rachel and Wright David, Unmanned aerial systems: Surveillance, ethics and privacy in civil applications, 28 Computer Law and Security Review 184 2012.

Lord Lester and Pannick, D. (eds.), Human Rights Law and Practice, Butterworth London 2004.

Nissenbaum Helen, Toward an Approach to Privacy in Public: Challenges of Information Technology, 7 (3) Ethics & Behavior 207 1997.

Schlag Chris, The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights, 13 (2) Journal of Technology Law and Policy 1 2013.

Solove Daniel, Understanding Privacy, Harvard University Press 2008.

Warren Samuel and Brandeis Louis, The Right to Privacy, 4 Harvard Law Review 193 1890.

Whitman James, The two western cultures of privacy: dignity versus liberty, 113 Yale Law Journal 1151 2004.

Wong Rebecca, The Future of Privacy, 27 (1) Computer Law and Security Review 53 2011.

Cases

Costello-Roberts v. the United Kingdom App no. 13134/87 (ECtHR, 25 March 1993).

Uzun v. Germany, App no. 35623/05 (ECtHR, 2 September 2010).

P.G. and J.H. v. the United Kingdom, App no. 44787/98 (ECtHR, 6 February 2001).

Von Hannover v. Germany, App no. 59320/00 (ECtHR, 24 June 2004).

Von Hannover v. Germany (No. 2) App nos. 40660/08 and 60641/08 (ECtHR, Grand Chamber, 7 February 2012).

Perry v. the United Kingdom, App no. 6737/00 (EctHR, 17 July 2002).

M.S. v Sweden, App no. 20837/92 (ECtHR, 27 August 1997).

C-101/01 Bodil Lindqvist [2003].

C-212/13 František Ryneš [2014].

C-73/07 Satamedia [2008].

Official Documents of the European Commission

European Commission, Privacy, data protection and ethical risks in civil RPAS operations - Final Report, 7 November 2014.

European Commission, How will the EU's Reform Adapt Data Protection Rules to New Technological Developments?, Europa, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf, accessed 8 January 2015.

European RPAS Steering Group, Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013, 5, *http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf*, accessed 2 January 2015.

European Commission, A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner (Communication) COM, 2014, 207 final, 8 April 2014.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), 25 January 2012.

Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Other Documents

European RPAS Steering Group, Privacy, data protection and ethical risks in civil RPAS operations – Final Report for the European Commission, 7 November 2014.

Venice Commission, Opinion on Video Surveillance In Public Places by Public Authorities and the Protection of Human Rights, Council of Europe, Strasbourg, March 2007, 3.

Internet Sources

Canton David, Drones Offer Whole New Candid Camera, Harrison Pensa Blog, 2012, http://harrisonpensa.com/drones-offer-candid-camera., accessed 8 January 2015 (Canton 2012).

Clarke Roger, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, 21 October 2013, http://www.rogerclarke.com/DV/Intro.html, accessed 3 January 2015 (Clarke 2013).

Cole Chris, Rise of the Reapers: A Brief History of Drones, Drone Wars UK, 6 November 2014, *http://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones/*, accessed 2 January 2015 (Cole 2014).

Council of Europe Privacy Convention (epic.org), *https://epic.org/privacy/intl/coeconvention/*, accessed 8 January 2015.

Courtland, Erin, Drones in Canada – Will the proliferation of domestic drone use in Canada raise new concerns for privacy?, Officer of the Privacy Commissioner of Canada, March 2013, https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.asp, accessed 8 January 2015 (Courtland 2013).

Domestic Unmanned Aerial Vehicles (UAVs) and Drones epic.org, 2013, *http://epic.org/privacy/drones/*, accessed 8 January 2015.

Marx Gary, What's New About the "New Surveillance? Classifying for Change and Continuity, Surveillance and Society, 2002, *http://www.surveillance-and-society.org/articles1/whatsnew.pdf*, accessed 8 January 2015.

Nevins Joseph, Robocop, Drones at Home, Boston Review, January/February 2011, *http://new.bostonreview.net/BR36.1/nevins.php*, accessed 8 January 2015 (Nevins 2011).

O'Neill Aidan, How the CJEU uses the Charter of Fundamental Rights, Eutopia Law, April 2012,

http://eutopialaw.com/2012/04/03/how-the-cjeu-uses-the-charter-of-fundamental-rights/, accessed 8 January 2015 (O'Neill 2012).

Privacy, Stanford Encyclopedia of Technology, 9 August 2013, *http://plato.stanford.edu/entries/privacy/, accessed 8 January 2015.*

Voisin Gabriel, Drones: Privacy implications across the EU, Bird&Bird, 15 July 2013, http://www.twobirds.com/en/news/articles/2013/global/drones-privacy-implications-across-the-eu, accessed 4 July 2015 (Voisin 2013).

What do we call them: UAV, UAS or RPAS?, Australian Certified Operators Inc, http://www.acuo.org.au/industry-information/terminology/what-do-we-call-them/, accessed 2 January 2015.