

The processing of personal information using remotely piloted aircraft systems in South Africa

Nomalanga Mashinini

LLB LLM (UP)

Lecturer, Faculty of Law, Rhodes University

SUMMARY

Remotely piloted aircraft systems are becoming a commodity all over the world. Typically known as “drones”, remotely piloted aircraft systems allow pilots to record videos and take photographs without being physically present. Such systems are used in both private and commercial ways that vary from service delivery to surveillance. As such, the protection of the right to privacy faces new challenges under South African law. This paper is concerned with the irresponsible use of remotely piloted aircraft systems, that results in privacy infringement. The article also includes a discussion of the obstacles that come with identifying users of remotely piloted aircraft systems, and the burden that such constraints place on people who seek to enforce their right to privacy. Therefore, the paper is a critical analysis of whether the existing data protection and civil aviation laws can withstand the invasion of remotely piloted aircraft systems in South Africa.

1 Introduction

No one knows how many RPAS exist in South Africa. Not all RPAS are registered.¹ In 2017, the South African Civil Aviation Authority (SACAA) reported that the number of registered remotely piloted aircraft systems (RPAS) has increased from 216 to 468 in total. By the end of 2018, this number had further grown to a total of 663 RPAS.² People often use RPAS for private purposes, either as a toy or to take photographs;³ but RPAS can provide commercial or essential benefits such as service

1 McKinley “New terrains of privacy in South Africa: Biometrics/smart identification systems, CCTV/ALPR, drones, mandatory sim card registration and Fica” 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

2 IT Web Daily (2017-02-09) <http://www.itweb.co.za/mobilesite/news/159283> accessed on 13 February 2017; “State of RPAS report in South Africa” available at <https://www.rocketmine.com/wp-content/uploads/2019/07/ROC-008-STATE-OF-RPAS-REPORT-2018-email.pdf> (accessed 2019-11-21).

3 Clarke “The regulation of civilian drones’ impact on behavioural privacy” 2014 *Computer & Security Law Review* 287.

delivery.⁴ Since an RPAS has a camera,⁵ it can be used to collect photographic data remotely without obtaining permission from anyone.⁶ An RPAS provides real-time feedback to the pilot; giving them the uncontrolled ability to store other people's photographs and videos. Given how people interact on social media, a pilot may share the data on their social media account as well. As a result, the right to privacy withers when people use their RPAS negligently.

In general, privacy is under threat because of the irresponsible use of technology such as RPAS.⁷ Besides, RPAS are becoming more accessible and inexpensive to purchase.⁸ The cheapest RPAS costs R1 999 and has a camera that takes 5-megapixel images and records high definition videos while the pilot views a live feed.⁹ Such RPAS can also be used to track people, animals and objects without the need for a tracking bracelet. Therefore, it may allow a remote pilot to track a person and keep stored records about the latter without their consent.¹⁰ Personal data generates money and helps to predict people's preferences and hobbies. As such, the law must be concerned about the implications of people and businesses acquiring data-collecting RPAS.

This paper involves an analysis of the enforceability of the right to privacy in civil aviation. The relevant laws to consider in South Africa are the Civil Aviation Act 13 of 2009 (CAA), read along with the Civil Aviation Regulations, 2015 (CARs).¹¹ The existing regulations for the recreational use of RPAS prohibit certain forms of irresponsible use. Whether these laws are sufficient to protect individuals from unlawful infringement of their right to privacy will be discussed throughout this paper. Furthermore, the protection of privacy also entails protection against unlawful processing of personal information, which may include photographic data of individuals. Therefore, a critical analysis of the

-
- 4 Cash "Droning on and on: A tort approach to regulating hobbyist drones" 2016 *University of Memphis Law Review* 696; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 11; Washington "Survey of drone use for socially relevant problems: Lessons from Africa" 2018 *Afr. J. Comp. & ICT* 2.
 - 5 Cash 2016 *University of Memphis Law Review* 696.
 - 6 Cash 2016 *University of Memphis Law Review* 696; Huneberg "The rise of the drone: Privacy concerns" 2018 *THRHR* 267.
 - 7 Cash 2016 *University of Memphis Law Review* 697 and 704; Loubser and Midgley *The Law of Delict* (2017) 327; Huneberg 2018 *THRHR* 264 & 267; Washington 2018 *Afr. J. Comp. & ICT* 6.
 - 8 Cash 2016 *University of Memphis Law Review* 696; Washington 2018 *Afr. J. Comp. & ICT* 5.
 - 9 See https://broadcasthub.co.za/product_details/ryze-tech-tello-quadcopter-iron-man-edition for an example of the cheap model described in this paper (accessed on 2020-04-05).
 - 10 Clarke 2014 *Computer & Security Law Review* 287.
 - 11 S 155(g)-(i) of the Civil Aviation Act 13 of 2009 empowers the minister of transport to make regulations for purposes of recreational activities specified in the regulations and establish regulatory bodies for such purposes; Civil Aviation Regulations, 2011 published in GG 38830 of 2015-05-27.

Protection of Personal Information Act 4 of 2013 (POPI Act) is included in this study to determine whether RPAS users are bound to the principles aimed at protecting the right to privacy in the POPI Act.

2 Regulation of RPAS in South Africa

RPAS, commonly known as drones, are aircraft operated from a remote pilot station, excluding a model aircraft and toy aircraft.¹² The pilot of an RPAS manages the flight thereof from a remote pilot station.¹³ Part 101 of the CARs applies to RPAS used for private and commercial flight operations.¹⁴ Commercial operations involve the use of RPAS in farming, mining, media, journalism, film and entertainment.¹⁵ Private operations refer to the use of an RPAS for personal purposes where there is no commercial outcome, gain or interest.¹⁶ Subparts 101.01 and 101.05 of the CARs regulate such private use.¹⁷ The regulations have three main parts: (a) rules relating to the requirements for operating RPAS and the required distance between the pilot and the RPAS; (b) restrictions that limit the distance between the RPAS and other aircraft, other people and their property and (c) exemptions from liability.

2.1 License and distance requirements for RPAS pilots

A pilot who uses an RPAS for private operations is not required to have a license.¹⁸ However, pilots using RPAS for personal reasons must have a certificate of registration for each RPAS they own.¹⁹ As opposed to private RPAS pilots, commercial RPAS pilots must undergo training and require a license to operate RPAS lawfully.²⁰ The CARs require the pilot using RPAS for commercial operations to have an operations license which specifies the kind of operation the pilot may participate in, hence training is required.²¹ Furthermore, the holder of an RPAS operational license for commercial use is required to have insurance against third-party liability.²² Whether insurers satisfy violation of privacy claims will depend on the contractual arrangements between parties.

12 R 2(k) Civil Aviation Regulations, 2011.

13 *Supra*.

14 Part 101.01.1(1) read with subpart 101.01.1(2)(d) Civil Aviation Regulations, 2011; McKinley 2018 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

15 McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 13.

16 R 2(i) Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

17 Part 101.01.2(1) Civil Aviation Regulations, 2011.

18 Part 101.01.2(2) Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12-13.

19 Part 101.05.10(1)(c) Civil Aviation Regulations, 2011.

20 Part 101.04 Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 13.

21 Part 101.04.1 Civil Aviation Regulations, 2011.

22 Part 101.04.12 Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 13.

All pilots must fly RPAS within a visual-line-of-sight (VLOS),²³ 400 feet above ground level while maintaining direct and unaided visual contact with the RPAS at a distance not exceeding 500 metres.²⁴ Although, commercial RPAS can also be operated beyond the visual-line-of-sight (B-VLOS) if they have the approval to fly B-VLOS.²⁵ The CARs aim to ensure that the pilot actively and continually monitors the RPAS while it is in flight, not allowing it to move outside of their VLOS. Therefore, the mentioned regulations deal with the distance required between the pilot and the RPAS. Additionally, the CARs also provide restrictions that must be observed by RPAS pilots concerning other people affected by RPAS operations.

2.2 Restrictions on private and commercial RPAS operations

The CARs prohibit RPAS operations directly above any person or a group of persons within a lateral distance of 50 metres unless such persons are under the direction of the RPAS pilot.²⁶ These provisions apply to both private and commercial operations. RPAS may not be operated within a lateral distance of 50 metres from any structure or building without permission from the owner thereof.²⁷

The cumulative effect of these regulations makes it unlawful to fly RPAS less than 50 metres away from a person, above a person or someone's property while the remote pilot of the RPAS is, at most, 500 metres away from the RPAS. Not complying with CARs can amount to an offence and may result in a fine of up to R50 000 or a period of imprisonment not exceeding ten years or both.²⁸

Moreover, all RPAS pilots are prohibited from engaging in negligent or reckless RPAS operations that endanger the safety of people, property or any other aircraft.²⁹ This provision relates explicitly to the safety of other people concerning the use of RPAS. SACAA issued a notice on their website explaining that the dangers of the negligent operation of an RPAS may result in "legal liability for breaking privacy laws and other laws enforceable by other authorities".³⁰ However, the CARs do not

23 R 3(l) read with 101.05.11(1) and (2) Civil Aviation Regulations, 2011.

24 R 2(n) Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

25 Part 101.05.11 Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 14.

26 Part 101.05.13 Civil Aviation Regulations, 2011; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

27 Part 101.05.14(1)(b).

28 S 112(b) of the Civil Aviation Act 13 of 2009.

29 Part 101.05.9(2) Civil Aviation Regulations, 2011.

30 South African Civil Aviation Authority "Remotely Piloted Aircraft Systems – General Information" <http://www.caa.co.za/Pages/RPAS/Remotely%20Piloted%20Aircraft%20Systems.aspx> accessed on 27 May 2017.

explicitly prohibit the invasion of privacy through RPAS.³¹

Although the CARs do not place a specific duty on RPAS pilots to refrain from violating the right to privacy of others, such a duty can be inferred based on the communication of SACAA's expectations of RPAS users, in conjunction with the wording of the regulatory rules that bind RPAS pilots. Therefore, the regulations are all indirectly aimed at protecting the right to privacy, but they fail to provide enforcement of this right effectively.³²

2.3 Exemptions and limitations on liability

The CAA explicitly states that no action for trespassing can arise merely because an aircraft passes at a reasonable height over private property at a reasonable distance.³³ The CAA does not stipulate what the term 'reasonable' means in this context. One can assume that a reasonable height to fly over one's property would be one that does not exceed the restrictions under the CARs. A reasonable height may also include an operation that exceeds the CARs restrictions only as far as it is necessary to do so, based on the surrounding facts and circumstances. The provision seems to take the form of a rule of reason, tested against the standard of a reasonable man in the same position as the RPAS pilot. As a result, owners of RPAS may enjoy a statutory exclusion from claims if their conduct is proved reasonable under the circumstances.

Nonetheless, the SACAA urges all RPAS users to observe and avoid the possibility of infringing on other people's right to privacy, but there are no remedies or penalties prescribed for non-compliance or failure to observe the CARs in a way that violates the right to privacy. On the contrary, both the CARs and CAA omit the invasion of the right to privacy under the listed types of offences which can be committed by an RPAS pilot. This omission leaves an aggrieved party seeking other means to protect their rights in terms of either the common law of delict or legislation that regulates privacy if such legislation applies to their circumstances. As such, an analysis of the regulatory framework for the protection of privacy is essential for this paper.

3 The right to privacy under the Constitution

The right to privacy finds protected under section 14 of the Constitution, the common law and various statutory laws.³⁴ Everyone in South Africa has the right to privacy, but certain limitations of this right can be

31 McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 12.

32 Huneberg 2018 *THRHR* 271-272.

33 S 8 of the Civil Aviation Act 13 of 2009.

34 Papadopoulos and Snail *Cyberlaw@SA III: The law of the internet in South Africa* (2012) 277.

justified in terms of section 36 of the Constitution.³⁵ The right to privacy includes the claim not to have one's person, home and property searched or possessions seized.³⁶ However, the right to privacy is not limited to searches, seizures and communications only.³⁷

3 1 The scope of the right to privacy

The right to privacy is the right to be left alone;³⁸ the scope of which becomes narrower, the more a person interrelates with the world.³⁹ It relates to an individual's family life, sexual preference and home environment, which should be shielded from erosion through conflicting rights in the community. The right strongly relates to the individual's way of life as characterised by seclusion from the public and publicity.⁴⁰ Despite this, the right to privacy also extends beyond the inner sanctum of the home.⁴¹ Therefore, even in public places, such as a hotel room, private business or public bathroom, an individual can still expect their right to privacy to be protected.

3 2 Protection and enforcement

Section 38 of the Constitution provides that anyone acting in own interest or acting in the public's interest can approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened.⁴² A court hearing the matter may grant appropriate relief

35 S 36(1) of the Constitution of the Republic of South Africa, 1996 is known as the limitations clause. In terms of the limitations clause, a general law of application may limit any right under the Bill of Rights if that limitation is justifiable and reasonable in an open and democratic society based on human dignity, equality and freedom. To test whether a limitation of constitutional rights passes the constitutional muster, the following factors are considered: (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and the less restrictive means to achieve the purpose. See further s 16 of the Constitution of the Republic of South Africa, 1996 for a layout of the right to freedom of expression.

36 S 14 of the Constitution of the Republic of South Africa, 1996; Papadopoulos and Snail 277; Freedman and Robinson *LAWSA* (edJoubert) 5(4) (2012) para 91; Huneberg 2018 *THRHR* 266.

37 Currie and De Waal *The Bill of Rights Handbook* (2013) 295; De Vos and Freedman *South African Constitutional Law in Context* (2015) 462.

38 *Investigating Directorate: Serious Economic Offences and Others; Curtis v Minister of Safety and Security and Others* 2000 (10) BCLR 1079 (CC) para 16; Loubser and Midgley 326.

39 *Bernstein v Bester* 1996 (4) BCLR 449 (CC) para 77; Papadopoulos and Snail 281.

40 *Bernstein v Bester supra* para 67; Neethling, Potgieter and Visser *Neethling's Law of Personality* (2005) 30; De Vos and Freedman 322.

41 *Investigating Directorate: Serious Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 (1) SA 545 (CC) para 16; *Magajane v Chairperson, North West Gambling Board and Others* 2006 (10) BCLR 1133 (CC) para 42.

42 S 38(a) and (d) of the Constitution of the Republic of South Africa, 1996; Currie and De Waal 177-178.

and must promote the values that underlie an open and democratic society based on human dignity, equality and freedom.⁴³ However, if the court finds that there is legislation that regulates RPAS concerning the right to privacy, it will determine the matter based on such a statute first.⁴⁴ without legislative or common law remedies, constitutional litigation may arise when a person claims that there has been a violation of their right to privacy through an RPAS.

The plaintiff would have to establish that they were entitled to enjoy the right to privacy under the circumstances.⁴⁵ This investigation involves finding out whether the alleged infringer is bound to the duties imposed by the constitutional right to privacy of the plaintiff. The scope of the right to privacy under the facts and circumstances must be determined.⁴⁶ If it appears that the infringer violated the right to privacy of the plaintiff, the question arises whether such infringement was a justifiable infringement of the right. If the violation of the right to privacy is proven to be unjustifiable, the court may grant appropriate relief.⁴⁷ The court can be flexible with the relief that it grants to the plaintiff and adapt to the damaging effects of new technologies.

Nevertheless, constitutional litigation is expensive for persons who cannot afford legal counsel in South Africa.⁴⁸ More so, a claim is almost impossible to prove when the alleged infringement happens through an RPAS. The burden is on the plaintiff to identify the wrongdoer who used an RPAS to invade their privacy. All South African-registered RPAS must be marked with identification numbers that are engraved, etched or stamped and affixed conspicuously on the exterior.⁴⁹ However, the make of an RPAS is not easy to identify while it is in flight, making it even more difficult for anyone to identify a wrongdoer who conceals their identity using an RPAS. Such considerations increase the burden on individuals to enforce the right to privacy against violations committed through an RPAS.

When applying the right to privacy as contained in the Bill of Rights, a court must give effect to that right by either applying enabling legislation or developing the common law to the extent that legislation does not give effect to that right.⁵⁰ Therefore, in subsequent paragraphs, an analysis of the common law protection of the right to privacy in the context of RPAS follows. After that, the POPI Act is also discussed to determine the

43 S 38 read with s 39(1)(a) of the Constitution of the Republic of South Africa, 1996.

44 De Vos and Freedman 338.

45 Freedman and Robinson *LAWSA* 5(4) para 93; De Vos and Freedman 322.

46 *Supra*.

47 S 38 of the Constitution of the Republic of South Africa, 1996; Currie and De Waal 180; De Vos and Freedman 685.

48 Fowkes "Constitutional Review in South Africa: Features, changes and controversies" in Fombad *Constitutional adjudication in Africa* (2017) 170.

49 South African Civil Aviation Technical Standards part 101.02.4.

50 S 8(3) and s 39(2) and (3) of the Constitution of the Republic of South Africa, 1996; Currie and De Waal 45; De Vos and Freedman 685.

effectiveness of the regulatory framework relating to the right to privacy, in the context of RPAS.

4 Common law protection

The courts have recognised that the right to privacy is an independent personality right under the common law of delict.⁵¹ The courts perceive privacy claims as related to the infringement of the right to human dignity,⁵² although they maintain that dignity and privacy claims are different.⁵³ When a person acquaints themselves with private facts,⁵⁴ against the will or permission of the owner of those private facts, their conduct may amount to a violation of the right to privacy.⁵⁵ A claim based on the invasion of privacy will only succeed if the alleged violation is proved to be intentional and unlawful, without a valid ground of justification.⁵⁶ In order for the invasion to be deemed unlawful, the plaintiff must have a legitimate expectation of privacy. Additionally, the invasion of privacy must be objectively unreasonable when viewed through the eyes of the community and in light of constitutional values and norms.⁵⁷

4 1 Requirements for liability

In order to incur liability, the wrongdoer must have manifested an intention to acquire personal information by invading others' privacy using an RPAS.⁵⁸ South African courts have not yet had an opportunity to test whether the common law protection is sufficient to hold that an RPAS pilot acted with the necessary intention when an RPAS had been used to capture images and videos during flight, whether the pilot intended to capture such images or not.⁵⁹ It also remains to be seen whether the common law may be sufficient to protect an individual from the infringement of their right to privacy, to the extent that their personal information is merely collected using an RPAS, but not perused or published without their consent.⁶⁰

51 Neethling, Potgieter and Visser 29; Huneberg 2018 *THRHR* 266.

52 Often when the right to privacy is violated, they are not treated with respect, thus violating their human dignity, see De Vos and Freedman 463; Loubser and Midgley 325.

53 Neethling, Potgieter and Visser 218; Loubser and Midgley 325.

54 Neethling, Potgieter and Visser 222; Huneberg 2018 *THRHR* 265.

55 Currie and De Waal 296; Huneberg 2018 *THRHR* 265.

56 Currie and De Waal 296; Grounds of justification that can operate against the infringement of the right to privacy include necessity, private defence, public interest in information relating to a public figure or a newsworthy event, and consent – see Neethling, Potgieter and Visser 240-251.

57 Neethling, Potgieter and Visser 55; Currie and De Waal 298; De Vos and Freedman 462.

58 Neethling, Potgieter and Visser 292 and 221.

59 McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 14.

60 Roos "Data protection: Explaining the international backdrop and evaluating the current South African position" 2007 *SALJ* 423.

4 2 Requirements for the *actio iniuriarum*

The *actio iniuriarum* allows recourse for the violation of the right to privacy. Specific forms of infringements of the right to privacy include setting up bugging and listening devices;⁶¹ unauthorised use of photos;⁶² unauthorised entry into a private residence;⁶³ listening to private conversations and disclosing private facts acquired through an unlawful act of intrusion;⁶⁴ shadowing of a person;⁶⁵ publishing someone's photograph without their consent;⁶⁶ and peeping through the window to see a person undressing.⁶⁷ All these forms of infringement can also be committed using an RPAS. For instance, one can look into a window to see a person undressing using an RPAS without them having to be physically present outside that window.⁶⁸ Therefore, the courts must decide on a case-by-case basis, whether a claim for the infringement may succeed if the acts mentioned above could not have been committed without using an RPAS.⁶⁹

The *actio iniuriarum* can never be used against negligent actions because is aimed at satisfaction for non-patrimonial loss caused by intentional, wrongful conduct.⁷⁰ When the courts assess satisfaction in a privacy claim, the facts and circumstances of the case determine the outcome.⁷¹ The court considers the plaintiff's social standing, the seriousness of the violation, and the defendant's attitude at the time of the infringement and afterwards. The courts further consider the nature of the infringement and its effects on the plaintiff.⁷² Therefore, the *actio iniuriarum* provides a restricted approach in protecting the right to privacy. It does not sufficiently protect an individual from the negligent collection of their personal information using an RPAS camera;⁷³ let alone an RPAS operated contrary to the CARs. Whether the *actio iniuriarum* requires development to remedy negligent acts was previously raised in the Constitutional Court.⁷⁴ However, the court found it unnecessary to deal with this question because it held that the matter related to the intentional infringement of the right to privacy.⁷⁵

61 Loubser and Midgley 326.

62 Loubser and Midgley 327.

63 *S v Boshoff* 1981 (1) SA 393 (T) 394H.

64 *Financial Mail v Sage Holdings* 1993 (2) SA 451 (A) 469G.

65 *Epstein v Epstein* 1906 TH 87 at 88.

66 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 248H-249A.

67 *Rex v Holliday* 1927 CPD 395 at 401.

68 Clarke 2014 *Computer & Security Law Review* 287; McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 13.

69 *Supra*.

70 *NM v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC) para 55; Neethling *LAWSA* (ed Joubert) 20(1) (2009) para 399; Currie and De Waal 297; Loubser and Midgley 326 and 329-331.

71 Loubser and Midgley 429.

72 *Supra*.

73 Currie and De Waal 297.

74 *NM v Smith supra* para 21; Currie and De Waal 297.

75 *NM v Smith supra* para 57; Currie and De Waal 297.

A pilot should not be allowed to circumvent the law by using an RPAS to violate people's privacy. An RPAS flown in VLOS may indirectly violate the privacy of anyone around it. Arguably, the RPAS under these conditions assists the pilot to invade the right to privacy negligently. The common law is not sufficient to protect the right to privacy from RPAS.⁷⁶ Consequently, the POPI Act regulates the collection and processing of personal information in South Africa, to protect the right to privacy, cognisant of the right to freedom of expression and the impact of technological advancements that threaten the right to privacy.⁷⁷

5 Protection of Personal Information Act 4 of 2013

According to section 2 read with section 3(1)(a) of the POPI Act, this legislation aims to protect the right to privacy by regulating the processing of personal information that forms part of a filing system or intended to form part thereof.⁷⁸ It specifically deals with personal information that is entered into a record by or for a responsible party, by making use of automated or non-automated means.⁷⁹ The words used in the POPI Act to define its scope of application have specific meanings. For instance, a person to whom the information regulated under the POPI Act relates is a data subject.⁸⁰ It is the processing of personal information that belongs to such data subjects that the provisions of the POPI Act refers. As such, in subsequent paragraphs, the definitions of the words "processing"; "personal information"; "record"; "responsible party"; "automated" and "filing system" are explained in order to test whether the use of RPAS can be subject to the POPI Act.

5.1 Meaning of "processing"

The meaning of the word "processing" is cast broadly in the POPI Act.⁸¹ The term processing means:⁸²

"... any operation or activity or set of any operations, whether or not by automatic means, concerning personal information, including -

- a collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- b dissemination by means of transmission, distribution or making available in any other form; or
- c merging, linking, as well as restriction, degradation, erasure or destruction of information".

76 Huneberg 2018 *THRHR* 267.

77 Preamble of the Protection of Personal Information Act 4 of 2013.

78 S 2 of the Protection of Personal Information Act 4 of 2013.

79 S 3(1)(a) of the Protection of Personal Information Act 4 of 2013.

80 S 1 of the Protection of Personal Information Act 4 of 2013.

81 Van der Merwe *Information and communications technology law* (2016) 435.

82 S 1 of the Protection of Personal Information Act 4 of 2013.

The primary rule of statutory interpretation is to determine the intention of the legislature, by giving the words in the provision their ordinary grammatical meaning unless to do so would lead to absurdity that the legislature could not have contemplated.⁸³ A literal interpretation of the words used in the above definition may render the use of an RPAS as processing under the POPI Act. For example, the most apparent forms of processing using an RPAS involve collecting and storing photographs.⁸⁴ On the one hand, the ordinary meaning of “collection” refers to the action or process of gathering together or seeking to acquire items of a particular kind as a hobby. On the other hand, the word “storage” means to retain for future electronic retrieval.⁸⁵ Consequently, any photographic data captured with an RPAS camera would have been collected and stored by the RPAS pilot. However, such collection and storage would have to relate to personal information as defined in the POPI Act.

5 2 Definition of “personal information”

Section 1 of the POPI Act provides the following definition for personal information:⁸⁶

“‘personal information’ means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

- a information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person;
- b information relating to the education or the medical, financial, criminal or employment history of the person;
- c any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- d the biometric information of the person;
- e the personal opinions, views or preferences of the person;
- f correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g the views or opinions of another individual about the person; and
- h the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person”

The POPI Act does not provide an exhaustive list of items that can be personal information. The term “reveal” is used more than once in this provision to illustrate that personal information may include data that an

83 Du Plessis *LAWSA* (edJoubert) 25(1) (2011) para 349; *Ngweyama v Mayelane* [2012] 3 All SA 408 (SCA) 409.

84 Clarke 2014 *Computer & Security Law Review* 287.

85 Oxford University Press *Oxford Dictionary of English* (2016).

86 S 1 of the Protection of Personal Information Act 4 of 2013.

individual does not want to disclose to the public. The right to privacy associates with one's ability to decide what they want to disclose to the public and such an expectation is reasonable.⁸⁷ Such information could be a person's presence at a particular location, which may be disclosed by an RPAS pilot if they post a photo of that person on the internet.

For example, location falls under the definition of personal information in the POPI Act.⁸⁸ It may be argued that photographic data collected by an RPAS pilot can reveal the location of a person while the individual does not wish for such a location revealed to others. Therefore, depending on the photographic data collected using RPAS, the use of an RPAS may be the processing of personal information.⁸⁹

A purposive approach to interpreting the definition of personal information requires a broad construction to apply its provisions to achieve the purpose of the legislation.⁹⁰ It would be absurd for the legislature to attempt regulating the processing of personal information, with the effect that photographic data that reveals personal information, such as location, falls outside of its ambit. This outcome would inevitably allow RPAS pilots to circumvent the purpose of the POPI Act, even though their actions might be a violation of the right to privacy using technological means. The right to privacy would erode if a purposive approach is not applied, and any conflicting interpretation would thwart the spirit, purport and values of the Constitution. Nevertheless, the legislature has included a list of activities excluded from the meaning of personal information to curb the far-reaching effects of the purposive approach.

5 2 1 General exclusions from the definition of "personal information"

Section 6(1)(a) of the POPI Act excludes purely household activities or personal activities from the scope of personal information. The term purely "household or personal activities" is not defined in the Act. This exclusion creates a gap in the scope of the POPI Act for instances where an RPAS is used to look through the window of a person's private home. Unfavourable outcomes may arise if the videos that remote pilots record about people's day-to-day household activities do not amount to processing personal information within the meaning of the Act.⁹¹

The scope of personal activities may range from everything a data subject does with their life, save for activities undertaken in the workplace, or at a public event. Considering what may be viewed

87 *Investigating Directorate: Serious Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit supra* 16; Neethling, Potgieter and Visser 226; Currie and De Waal 302-303.

88 S 1(c) of the Protection of Personal Information Act 4 of 2013.

89 Clarke 2014 *Computer & Security Law Review* 287.

90 Du Plessis *LAWSA* (2011) para 327.

91 Clarke 2014 *Computer & Security Law Review* 289.

subjectively as “personal activities”, it appears that the meaning of “personal activities” is broad or unfairly limited. However, the meaning must be viewed objectively and reasonably in line with the legal convictions of the community.⁹² One person may consider a day spent at the park as a personal activity which they would prefer to enjoy without an RPAS hovering above them. Another person may restrict personal activities to their home, and thus considering activities carried outside their yard as not forming part of personal activities.

Notably, what is “personal” may differ from person to person, as everyone has the right to “determine what they would like to keep private”.⁹³ Drawing a line between what is and what is not purely personal household activity may be difficult in some instances. Therefore, the exclusion of purely household activities remains to be tested in court or addressed by the Information Regulator when determining the margins of personal information under the POPI Act.⁹⁴

5 2 2 Exclusions for journalistic, literary or artistic purposes

The legislature aimed to balance the right to privacy with freedom of expression in circumstances where it is in the public’s interests to reconcile the two.⁹⁵ Accordingly, the processing of information for journalistic, literary and artistic expressions is not subject to the POPI Act.⁹⁶ However, the meaning and extent of “journalistic, literary and artistic expressions” is not provided. The ordinary meaning of these words applies, given the context and purpose of the statute.⁹⁷ As such, using RPAS to collect news for reporting or public comment and expressions of photography and videography may fall under this provision and exempt from the conditions set out in the POPI Act. The exemption must account for the importance of the right to freedom of expression, seeing that the legislature cleared tried to balance with privacy in this context.⁹⁸

Based on the abovementioned exclusions for certain types of information, it is evident that photographs are neither included nor excluded explicitly in the ambit of the word personal information.

92 Neethling, Potgieter and Visser 55. Determining the legal convictions of the community requires a constitutionally transformative approach because the Constitution applies to all law. Therefore, the meaning of “personal activities” must be informed by the norms and values that underpin the Constitution of the Republic of South Africa, 1996.

93 Loubser and Midgley 326.

94 The Information Regulator is the office empowered to ensure the administration and enforcement of the Protection of Personal Information Act 4 of 2013 in terms of s 39 thereof.

95 S 2(a) read with s 7(1) and (3) of the Protection of Personal Information Act 4 of 2013.

96 S 7 of the Protection of Personal Information Act 4 of 2013.

97 Du Plessis *LAWSA* (2011) para 349; *Ngweyama v Mayelane supra* 409.

98 S 7(3) of the Protection of Personal Information Act 4 of 2013; Duhnkrack “The art of regulating arts – artistic street photography and the limits of EU regulation” 2020 *JiPLP* 69.

Therefore, this provision would call for a case-by-case determination of whether photographic data falls under personal information because the legislature has left room for discretion to determine what constitutes personal information under the POPI Act. Since photographic data is personal information, it follows that it must be entered into a record by or for a responsible party, by making use of automated or non-automated means.⁹⁹

5 3 Meaning of “record”

The POPI Act refers to a record as:¹⁰⁰

- “... any recorded information –
- a regardless of form or medium, including any of the following:
 - (i) writing on any material;
 - (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
 - (iii) label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
 - (iv) book, map, plan or drawing;
 - (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
 - b in the possession of or under the control of a responsible party;
 - c whether or not it was created by a responsible party; and
 - d regardless of when it comes into existence”.

The POPI Act provides that information produced or recorded using computer equipment, whether hardware or software, refers to a record, regardless of form or medium.¹⁰¹ A photograph is defined as a record,¹⁰² even when produced by an RPAS because the latter is computer equipment.¹⁰³ It is not a requirement for the responsible party to have created the record and the time of its creation is irrelevant. Nonetheless, a responsible person must ensure that the processing of personal information stored in a record follows the POPI Act.

5 4 Meaning of “responsible party”

The responsible party referred to in the POPI Act is a juristic person in the form of a private or public body which determines the purpose of processing personal information.¹⁰⁴ The statutory provisions expressly restrict its jurisdiction to organisations and do not extend to private persons. This definition immediately excludes private operations of

99 S 3(1)(a) of the Protection of Personal Information Act 4 of 2013.

100 S 1 of the Protection of Personal Information Act 4 of 2013.

101 S 1 of the Protection of Personal Information Act 4 of 2013.

102 S 1(a)(v) of the Protection of Personal Information Act 4 of 2013.

103 S 1(a)(ii) of the Protection of Personal Information Act 4 of 2013; Van der Merwe 435.

104 S 1 of the Protection of Personal Information Act 4 of 2013.

RPAS from the scope of the POPI Act, which is somewhat understandable because the penalties provided for contravening the POPI Act may be too harsh for a private individual to bear for flying an RPAS.¹⁰⁵ Nevertheless, juristic persons who use RPAS for private and commercial operations still fall within the scope of the meaning of a responsible party, provided that they are processing personal information as defined in the POPI Act, using either automated or non-automated means.

5 5 “Automated” means versus “non-automated” means

The POPI Act applies to the processing of information using both “automated” and “non-automated” means. The term “automated” refers to any equipment that can operate automatically in response to instructions given for processing information.¹⁰⁶ It seems that the legislature intended to include any possible means that could be employed to process personal information, in response to instructions, but without human intervention. Therefore, collecting data using RPAS amounts to processing using automated means. If found to be non-automated means, the use of RPAS would still be within the scope of the POPI Act, provided that the responsible party stores the collected photographic data in a filing system.

5 6 Meaning of “filing system”

A filing system refers to a structured set of information. The information can be stored on a database, server or network, as the data can be centralised, decentralised or dispersed on a functional and geographical basis.¹⁰⁷ An RPAS has a filing system that it uses to record and store all the data it collects while it is in flight because it connects to a computer that provides a live feed to the pilot.¹⁰⁸ Such information is stored on a chip or server while the RPAS communicates with the computer.¹⁰⁹

Based on the terms stipulated above, RPAS operations may fall within the POPI Act when used by a responsible party to collect and store photographic data containing personal information. It is therefore necessary to establish whether the POPI Act would provide sufficient remedy for private and commercial RPAS operations that intentionally or negligently infringe on the right to privacy. A look at the findings about the constitutional protection, the common law *actio iniuriarum* and the civil aviation hurdles also follows.

105 S 107 read with s 109 of the Protection of Personal Information Act 4 of 2013 provides penalties in the form of imprisonment or a fine not exceeding R10 million.

106 S 3(4) of the Protection of Personal Information Act 4 of 2013.

107 S 1 of the Protection of Personal Information Act 4 of 2013.

108 Clarke 2014 *Computer & Security Law Review* 287; Washington 2018 *Afr. J. Comp. ICT* 3.

109 Cash 2016 *University of Memphis Law Review* 705.

6 Findings and recommendations

6 1 Accessibility of the Constitution

South African law subscribes to the principle that where there is a right, there is a remedy.¹¹⁰ As discussed throughout this paper, a data subject can legitimately expect protection from unauthorised collection and storage of photographic data about their person using RPAS, subject to justifiable limitations. Conversely, the common law and statutory protection avenues for enforcing the right to privacy seem flawed.

6 2 Limited common law protection

Under the common law of delict, the *actio iniuriarum* is available for those who want to litigate on the matter in a traditional court, instead of pursuing the POPI Act. An aggrieved person can also rely on the common law to pursue a claim against natural and juristic persons who invade their privacy using RPAS to collect information relating to purely household or personal activities and literary, artistic and journalistic activities. However, the *actio iniuriarum* can only protect the right to privacy against intentional acts of violation. It is impossible to prove intent when a pilot threatens the right to privacy without directing their will to that effect.

The common law remedy fails to accommodate the automated nature of new technologies such as RPAS and thus proves to be insufficient to protect the right to privacy in this context. This position is disappointing, especially given the fact that privacy infringement may also result in the violation of the right to human dignity. The *actio iniuriarum* must develop to include negligence as a requirement for this remedy to apply to the use of RPAS.¹¹¹ Then again, as mentioned earlier, the development of the common law mainly rests with our courts if and when the relevant issue comes before the court.¹¹²

Perhaps relying on the POPI Act for protection may prove to be less burdensome, and more flexible than the common law because the dispute process involves laying a complaint with the Information Regulator who then investigates both negligent and intentional conduct.

110 Currie and De Waal 23.

111 Neethling, Potgieter and Visser 58-59.

112 S 8(3) read with s 39(2) and (3) of the Constitution of the Republic of South Africa, 1996.

6 3 Legislative barriers

6 3 1 *Challenges in regulating the processing of personal information using RPAS*

The purpose of the POPI Act is to provide remedies to protect personal information against processing that is contrary to its provisions.¹¹³ However, the POPI Act is too restrictive regarding its scope of application. Natural persons who operate RPAS privately are left with too much discretion to use their RPAS without licenses, and they do not even fall under the regulation of the POPI Act.¹¹⁴ RPAS hobbyists are probably the most concerning group of pilots because they may share live streams of their flight operations on social networks. The risk that comes with unauthorised disclosure is that photographs can be misinterpreted and result in a false representation of a person.¹¹⁵

At least the POPI Act finds some application to juristic commercial pilots or natural persons who use RPAS under the instructions of juristic persons, making them subject to the principles of processing personal information in terms of the POPI Act.¹¹⁶ However, the open-ended definition of personal information, which does not explicitly include or exclude photographs leaves a gap in our law. As a result, privacy infringement will be determined on a case-by-case basis when an RPAS pilot is accused of violating the right to privacy in terms of the POPI Act.

It seems that the POPI Act does not afford adequate protection from private and commercial operations of RPAS. A data subject who wishes to object to their personal information being processed using an RPAS will have to file their objection by submitting a form to the responsible party, using a data message, registered post or personal delivery.¹¹⁷ However, the method of reporting is ineffective and potentially costly for the plaintiff to pursue because it is nearly impossible to identify the RPAS pilot when the RPAS is in flight or unlicensed.

Furthermore, the option to object to processing information is only operational against those who are processing information that is within from the ambit of the legislation. The POPI Act cannot provide a remedy against pilots who use RPAS to collect personal data during private operations. The listed exclusions of information collected for literary, artistic and journalistic purposes could also prohibit the application of the POPI Act to the collection of personal information through RPAS.

113 S 2(c) of the Protection of Personal Information Act 4 of 2013.

114 Part 101.01.2(2) Civil Aviation Regulations, 2011; s 1(a)(v) of the Protection of Personal Information Act 4 of 2013.

115 Clarke 2014 *Computer & Security Law Review* 287.

116 McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 14.

117 R 2(1) of the Regulations Relating to the Protection of Personal Information GN R 1383 in GG 42110 of 2018-12-14.

6 3 2 *Obstacles in civil aviation rules*

Additionally, a pilot may take images of others and process such without incurring any statutory liability under the CAA because the CARs allow the private use of RPAS for up to 50 metres away from any person, aircraft or building without permission. Considering that people are inclined to purchase RPAS, combined with the fact that RPAS are becoming relatively inexpensive,¹¹⁸ lack of direct protection of the right to privacy against exploitation through RPAS creates the need for development in the law of privacy in information technology and civil aviation.¹¹⁹

A specific provision in the CARs that regulates the invasion of privacy through RPAS is vital in ensuring that there is some form of regulation directed at the irresponsible use of RPAS. The CAA and the CARs must also incorporate a specific remedy for the violation of privacy using RPAS because the POPI Act cannot apply to private operations as defined in the CARs. This incorporation can take the form of referring to the POPI Act in the CAA to address the privacy concerns that come up in civil aviation.¹²⁰ However, the legislature should not create arbitrary rules that unnecessarily restrict the right to freedom of expression, innovation and development, since civil aviation is mainly concerned with operational and safety requirements, rather than privacy regulation.¹²¹ The rights of South Africans must be balanced carefully in order to ensure that RPAS users can freely enjoy their hobbies without violating the privacy of others. At the moment, it seems that private users are self-regulated.¹²²

An analysis of existing legislation suggests that amending the POPI Act or the CARs is best to deal with the insufficiency of protection against the invasive use of RPAS. However, if the POPI Act were to be amended to regulate how private individuals handle personal information, the consequences of the contravention of the POPI Act would have to be tailored to suit the relevant contravention. The penalties imposed under the POPI Act would be too exorbitant for the kind of infringement that an RPAS pilot commits.

Nonetheless, the Constitution remains available to all South Africans to protect them from unjustifiable limitations of their right to privacy. However, as discussed earlier, the direct enforcement of this right under the Constitution can prove to be burdensome,¹²³ and can only be

118 Cash 2016 *University of Memphis Law Review* 696; Washington 2018 *Afr. J. Comp. & ICT* 5.

119 McKinley 2016 *Right to Know Campaign and the Media Policy & Democracy Project* 14.

120 Clarke 2014 *Computer & Security Law Review* 300.

121 *Supra*.

122 *Supra*.

123 Fowkes 170.

accessed after attempting to rely on applicable legislation, such as the POPI Act.¹²⁴

7 Conclusion

Amending the statutory rules that regulate RPAS operations is the best option for South Africa. The proposed amendments would have to deal with all operations of RPAS, whether commercial or private purposes. Seeing that the use of RPAS increases annually, the more we become a nation that uses RPAS for entertainment, economic growth and service delivery, the more such uses will threaten the right to privacy. The legislature must guard, protect and preserve the right to privacy against the rise of RPAS in South Africa.

124 Du Plessis *LAWSA* 25(1) para 327; De Vos and Freedman 338.