

**DRONES, PRIVACY AND INFORMATION PRIVACY: A  
DUE DILIGENCE HUMAN RIGHTS ANALYSIS  
WITH REFERENCE TO SOUTH AFRICAN AND  
NAMIBIAN LEGISLATION**

by

**LOIDE ANBELINA SHAPARARA**

**Student No. 58541241**

**submitted in partial fulfillment  
of the requirements for the degree of**

**MASTER OF LAWS  
with specialisation in Information Communications Technology Law**

at the

**UNIVERSITY OF SOUTH AFRICA**

**SUPERVISOR**

**PROFESSOR ANNELIESE ROOS**

**2022**

**Keywords:** Protection of Personal Information Act, Information Privacy, Data Protection, GDPR, Namibia Data Protection Law, Data Protection Principles, Privacy by Design, Data Protection Impact Assessment, Posthumous Data Protection, Drone Law, Civilian Drones, Chicago Convention, ICAO, Drone Regulations, Remote Aerial Vehicle, Drone industry, Emerging Technologies, Unmanned aircraft systems, Unmanned aerial vehicles

## DECLARATION

**Name:** Loide Anbelina Shaparara

**Student number:** 58541241

**Degree:** MASTER OF LAWS with specialisation in Information Communications Technology Law

Exact wording of the title of the dissertation as appearing on the electronic copy submitted for examination:

**Drones, Privacy and Information Privacy: a due diligence Human Rights analysis with reference to South African and Namibian Legislation**

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality-checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

*(The dissertation will not be examined unless this statement has been submitted.)*

---

**SIGNATURE**

---

**DATE**

## Contents

Dedication .....	6
Acknowledgements .....	7
List of Abbreviations .....	8
Table of Columns .....	11
Table of Figures .....	11
Chapter 1 .....	12
General Introduction.....	12
<b>1. Introduction</b> .....	<b>12</b>
<b>2. Background</b> .....	<b>14</b>
<b>3. Drones and Information Privacy</b> .....	<b>18</b>
<b>4. The Privacy-Intruding potential of Drones</b> .....	<b>20</b>
<b>5. Problem Statement</b> .....	<b>23</b>
<b>6. Purpose</b> .....	<b>25</b>
<b>7. Scope of the Study</b> .....	<b>27</b>
<b>8. Limitations of the Study</b> .....	<b>28</b>
<b>9. Research Methodology</b> .....	<b>29</b>
<b>10. Point of Departure</b> .....	<b>29</b>
<b>11. Hypothesis</b> .....	<b>30</b>
<b>12. Synopsis of Chapters</b> .....	<b>30</b>
Chapter Two .....	33
Selected Literature Review .....	33
<b>1.Introduction</b> .....	<b>33</b>
<b>2. History of Information Privacy</b> .....	<b>34</b>
<b>3.Foundational Legal Framework on Information Privacy</b> .....	<b>39</b>
3.1. International Legal Framework.....	39
3.2. National Legal Framework .....	41
<b>4. Parameters and Significance of Privacy</b> .....	<b>45</b>
4.1. Significance and Delineation of Privacy .....	46
4.2. Academic Theories on Information Privacy .....	47
<b>5. Information privacy protection as an Enabler of the right to Privacy</b> .....	<b>49</b>
5.1. Parameters and Purpose of Information Privacy Protection.....	49
5.2. Nexus between Privacy and Information Privacy .....	51
5.3. Regulatory Approaches.....	52
5.4. Stakeholders .....	52
5.5. Possible Expansion of Scope: Post-Mortem (Posthumous) Data Protection .....	52
<b>6. Current appraisal of Information Privacy Protection and Drones</b> .....	<b>55</b>
Chapter Three .....	58
Information Privacy Laws in RSA and Namibia .....	58
<b>1. Introduction</b> .....	<b>58</b>
<b>2. Generations of Information Privacy Laws</b> .....	<b>59</b>
<b>3.Yardsticks of a sound Information Privacy Legal Framework</b> .....	<b>61</b>

<b>4. Republic of South Africa</b> .....	<b>63</b>
4.1. Protection of Personal Information Act (POPIA) .....	63
4.1.1. Scope and Application .....	64
4.1.2. Exclusions.....	65
4.1.3. Information Privacy Protection Principles.....	66
4.1.4. Oversight and Enforcement .....	69
4.1.5. Enforcement and Implementation .....	70
4.1.6. Administrative Fines, Offenses and Penalties.....	70
4.1.8. Parallel Civil Claim(s).....	71
4.1.9. Collaboration and Sectoral Governance .....	71
4.1.10. Data Export.....	72
4.1.11 Cooperation Initiatives.....	72
<b>5. The Republic of Namibia</b> .....	<b>73</b>
<b>5.1 Governance Institutions</b> .....	<b>74</b>
5.2 Data Protection Bill .....	77
5.2.1. Terminology and Scope .....	77
5.2.2. Exemptions .....	78
5.2.3. Basic Principles for Lawful Processing.....	78
5.2.4. Technical.....	79
5.2.5. Data Subject Rights .....	79
5.2.6. Institutional Arrangements .....	81
5.2.7. Enforcements, Administrative Fines and Penalties .....	82
5.2.8 Data Export.....	82
5.2.9. International Cooperation.....	82
<b>6. Chapter Conclusion</b> .....	<b>82</b>
<b>Chapter Four</b> .....	<b>85</b>
<b>Applying Information Privacy Protection Principles to Drone Laws in RSA and Namibia</b> .....	<b>85</b>
<b>1. Introduction</b> .....	<b>85</b>
<b>2. Policy, Legal and Institutional Framework</b> .....	<b>86</b>
2.1. RSA.....	86
2.2. Namibia .....	88
<b>3. Selected Substantive CARS with Information Privacy Implications</b> .....	<b>88</b>
<b>3.1 Design and Manufacture</b> .....	<b>89</b>
<b>3.2. Import and Export</b> .....	<b>92</b>
<b>3.3. Sale and Labelling</b> .....	<b>93</b>
<b>3.4. Technical Classifications of Drones</b> .....	<b>94</b>
<b>3.5. Private (Recreational) Drone Operations</b> .....	<b>96</b>
<b>3.6 Approval and Registration</b> .....	<b>100</b>
<b>3.7. Personnel Licensing</b> .....	<b>101</b>
<b>3.8. Drone Operators Certificate (ROC)</b> .....	<b>103</b>
<b>3.9. Safety Management</b> .....	<b>105</b>
<b>3.10. Security</b> .....	<b>105</b>
<b>4. Selected General Drone Operation Limitations</b> .....	<b>106</b>

5.	Liability .....	110
5	Insurance .....	110
6.	Enforcement of the SACARs.....	111
<b>CHAPTER FIVE</b> .....		117
<b>The European Union Legal Framework on Drones</b> .....		117
1.	Introduction .....	117
2.	Key Institutions.....	118
2.1	EU Aviation Safety Agency .....	118
2.2.	European Organisation for Civil Aviation Equipment .....	119
2.3.	Joint Authorities for Rulemaking on Unmanned Systems .....	119
2.4.	National Aviation Authority (NAA).....	119
2.5.	European Organisation for the Safety of Air Navigation .....	120
3.	Overview of the EU Legal Framework on Drones .....	120
4.	Substantive Information Privacy Provisions .....	123
5.	Classification .....	124
4.	Manufacturing .....	129
	Technical Specifications .....	129
5.	Sale, Labelling and Market Surveillance .....	131
6.	Registration .....	134
7.	Pilot Training .....	135
8.	Cross-Border and Third-Party Drone Operations .....	137
9.	Enforcement .....	139
10.	Safety, Security and Maintenance .....	142
11.	Insurance .....	144
12.	Evaluation of the EU Legal Framework on Drones .....	145
13.	Chapter Conclusion .....	149
<b>Chapter Six</b> .....		151
<b>Information Privacy within the Global Drone Civil Aviation Regulatory Regime</b> .....		151
1.	Introduction .....	151
2.	Institutional Framework.....	152
3.	General Overview of the ICAO Regulatory Framework on Drones.....	154
4.	ICAO's approach to Information Privacy .....	158
5.	Chapter Summary and Evaluation.....	160
<b>Chapter Seven</b> .....		165
<b>Conclusion</b> .....		165
1.	Introduction .....	165
2.	Synopsis of the Research .....	165
3.	Main Conclusions .....	173
4.	Recommendations .....	174
5.	Suggestions for Future Research.....	177

## **Dedication**

**All glory to God for being there every step of the way and for all that is to come.**

## Acknowledgments

Now that we are here, drawing a close on a journey born from a casual debate on the interplay of information privacy and drone technologies, at the first-ever civil aviation legal advisors forum a sheer curiosity and a conviction that there is a greater duty to preserve privacy within the drone industry.

My heart is overwhelmed with gratitude because I realise that I am a woman mightily helped by God and his people...

I want to thank my supervisor Professor Anneliese Roos, for the privilege to quench my curiosity under her able guidance. Moreover, for her boundless generosity, support encouragement, and most particularly that I could borrow from her calm and sturdiness in my moments of alarm and despondency. Thank you, Prof, for keeping me sane throughout the whole process. Only now do I truly understand the value of a head and heart thesis supervisor.

I'd like to offer thanks to my mother Nora, thank you for the example of your tenacity and valour, being your daughter remains a lifetime privilege.

Loving thanks to Mr. C Kamerika for your warm companionship and practical and emotional support.

My appreciation also goes to everyone who understands in the words of John Updike:

*'To be a human being is to be in a state of tension between your appetites and your dreams, and the social realities around you and your obligations to your fellow man.'*

Loide Anbelina Shaparara, the audacity! May the odds be in your favour.

## List of Abbreviations

AC's	Advisory Circulars
AI	Artificial Intelligence
AICs	Aeronautical Information Circulars
AMC	Acceptable Means of Compliance
ANS	Air Navigation Services
ATC	Air Traffic Controllers
ATM	Air Traffic Management
AU	African Union
BR	Basic Regulation
CAEP	Committee on International Aviation Environmental Protection
CARs	RSA and Namibia Civil Aviation Regulations
CE	Conformité Européenne
Civil Aviation Authorities	SACAA
CoE	Council of Europe
DNA	Deoxyribonucleic acid
DRI	Direct Remote Identification
EASA	EU Aviation Safety Agency
EC	European Commission (),
EEA	European Economic Area
EU-	European Union
EUROCAE	European Organisation for Civil Aviation Equipment () and
GDPR	General Data Protection Regulation
GM	Guidance Material
GPA	Global Privacy Assembly
GPS	Global Positioning System
ICASA	Independent Communications Regulatory Authority of South Africa



IAPP	International Association of Privacy Protection Professionals
ICAO	Civil Aviation Organisation
ICCPR	International Convention on Civil and Political Rights
ICDPPC	Conference of Data Protection and Privacy Commissioners
ICJ	Statute of the International Court of Justice
IEWG	International Enforcement Working Group
IR	Implementing Regulation
JARUS	Joint Authorities for Rulemaking on Unmanned Systems ()
LUC	Light UAS Operator Certificates
NACAA	Namibia Civil Aviation Authority
NACAA	Namibia Civil Aviation Authority
NADPA	Network of African Data Protection Authorities
NAMCARs	Civil Aviation Regulations: Part 101 Rules of the Air and General Operating Rules Operation of Remotely Piloted Aircrafts
NCAA	Namibian Civil Aviation Act
NCCA	Namibia Civil Aviation Authority
PET's	Privacy-enhancing technologies
POPIA	Protection of Personal Information Act
RADPA	Round Table of African Data Protection Authorities
RPAS	Remotely Piloted Aircrafts
RPASP	Remotely Piloted Aircraft Systems Panel
SACAA	South African Civil Aviation Authority
SACARs	South African Civil Aviation Regulations

SA-CATS	South Africa Civil Aviation Technical Standards
SADC	Southern African Development Community
SARP	Standards and Recommended Practices
SCAA	South African Civil Aviation Authority
SES	Single European Market Strategy
STS	Standard Scenarios
UAS	Unmanned Aircraft Systems
UASSG	Unmanned Aircraft Systems Study Group
UDHR	Universal Declaration of Human Rights
UNCLOS	United Nations Convention on the Law of the Sea
USOAP	Universal Safety Oversight Audit Programme
E-VLOS	Extended Visual Line of Sight
B-VLOS	Beyond Visual Line of Sight
PETs	Privacy Enhancing Technology
GDPR	General Data Protection Regulation
Wi-Fi	Wireless Fidelity

## Table of Columns

<b>Column 1</b>	Summary of the scope of personal data amassed by drones
-----------------	---

## Table of Figures

<b>Figure 1</b>	NACC website disclaimer to privacy queries
-----------------	--

# Chapter 1

## General Introduction

---

*This chapter sets out the general introduction to the thesis. It contains inter alia the background to the research problem, the objectives of the study and the methodology followed throughout the research process. To offer a signpost to readers, it also sets out a summary of the chapters that make out the thesis.*

### 1. Introduction

Drones technologies are pronounced as one of the most disruptive technologies of the twenty-first century.<sup>1</sup> The drone industry is hailed as one of the most dynamic industries and is estimated to generate 6.6 billion Namibian Dollars (N\$) per annum; this figure is expected to double over the next decade.<sup>3</sup>

It is reported that civilian drones are dominantly employed within the aviation, health, and agricultural fields and have also gained prominence for recreation use.<sup>5</sup> Drones are inter alia used for search and rescue operations, tracking and monitoring wild animals and property, geo-spatial mapping, law and regulatory enforcement, journalism leisure, and several other snowballing usages across multifaceted disciplines.<sup>6</sup>

There is immense enthusiasm for the budding capabilities and economic viability of drones.<sup>7</sup> Drones are keenly marketed, and their use is supported by the compelling

---

<sup>1</sup> S Watkins and Others, 'Ten questions concerning the use of drones in urban environments' 2(2020) 167 *Building and Environment Journal* 1064558.

<sup>3</sup> Nigel McKelvey, Cathal Diver C and Kevin Curran, 'Drones and Privacy' (2015) 6 *International Journal of Handheld Computing Research* 44,46; UNCTAD, *Technology and Innovation Report* (United Nations Publications 2021); See also Alistair Barr and Reed Albergotti, 'Google to buy Titan as Web Giants battle for Air Superiority' (*Wall Street Journal*, 14 April 2014) <<https://www.wsj.com/articles/SB10001424052702304117904579501701702936522>> accessed 19 January 2021; Fortune Business Insights 'Unmanned Systems /Commercial Drone Market' (Report ID: FBI102171), (Fortune Business Insights, no date supplied) <<https://www.fortunebusinessinsights.com/commercial-drone-market-102171>> accessed 15 November 2022.

<sup>5</sup> Matthew Ayamga, Selorm Akaba and Albert Apotele Nyaaba, 'Multifaceted applicability of drones: A review' (2021) 167 *Technological Forecasting and Social Change Journal* 120677.

<sup>6</sup> Marzocchi Ottavio, *Privacy and Data Protection Implications of the Civil Use of Drones: In-depth Analysis* (4th ed, European Parliament Publications, 2015) <<http://www.europarl.edu.studies>> accessed 30 March 2020; K Kirthan Shenoy and Divya Tyagi, 'Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky' (2022) 9(1) *International Journal of Aviation, Aeronautics, and Aerospace* <<https://doi.org/10.15394/ijaaa.2022.1669>> accessed 1 November 2022;

<sup>7</sup> Fact.MR, 'Drone Market' (Fact.MR, no date supplied) <[https://www.DroneMarketfactmr.com/report/62/dronemarket?utm\\_source=adwords&utm\\_medium=ppc&gclid=Cj0KCQiA0eOPBhCGARIsAFIwTs7gTEKInh1udDTznkg4qr](https://www.DroneMarketfactmr.com/report/62/dronemarket?utm_source=adwords&utm_medium=ppc&gclid=Cj0KCQiA0eOPBhCGARIsAFIwTs7gTEKInh1udDTznkg4qr)> accessed 1 Jan 2021; Research and Markets, 'Commercial Drones Report 2016 Global Strategic Analysis 2014-2020' (Globes

expediency it offers to various industries. The magnitude of this multiplicity is neatly summarised by Micheal Calvo<sup>8</sup> in the following words:

[D]rones can be found in several civilian sectors such as journalism, scientific research, agriculture, and surveillance. Because of how they are designed, their variations in size, and their almost limitless capabilities, drone technology has virtually presented this generation with a twenty-first-century new-age equivalent of the Swiss Army Knife.

The research established that the exponential accessibility, growth and expanding usefulness of drones constitutes a threat to the right to privacy.<sup>9</sup>

Embedded with the ability to among others capture photographs and videos in first person view from remote locations surreptitiously, cause public outcry to regulate drones to protect the human right to privacy in instances where such is 'assumed wanted or justified'.<sup>10</sup>

In response to this phenomenon, there is an international call to adopt policy and legal interventions to ensure that the privacy qualms brought about by developments in civilian drone technologies are addressed.<sup>11</sup>

---

Newswire, 26 Feb, 2016)<<https://www.persistencemarketresearch.com/market-research/uav-drones-market.asp>> accessed 21 March 2020; Global Industry Analysts Inc, 'New Analysis from Global Industry Analysts Reveals Steady Growth for UAV Drones, with the Market to Reach \$58.5 Billion Worldwide by 2026' (Cision PR Newswire, 16 November 2021)<<https://www.prnewswire.com/news-releases/new-analysis-from-global-industry-analysts-reveals-steady-growth-for-uav-drones-with-the-market-to-reach-58-5-billion-worldwide-by-2026--301423829.html>> accessed 1 Jan 2021.

<sup>8</sup> Michael Calvo, 'Uncertainty and Innovation: The Need for Effective Regulations to Foster Successful Integration of Personal and Commercial Drones' (2016) 22 *Southwestern Journal of International* 189,193–94.

<sup>9</sup> Nils Melezer, *Human Rights implications of the usage of Drones and Unmanned Robots in Warfare* (European Union, 2013) 15; Rachel L Finn and David Wright, 'Privacy, Data Protection and Ethics for Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organisations' (2016) 32 *Computer Law & Security Review* 577, 586; Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 1 *Monash University Law Review* 44; See also Miriam McNabb, 'Are Drones Ready to Take Off in Africa?' (*Dronelife*, 19 June 2018)<<https://dronelife.com/2018/06/19/are-drones-ready-to-take-off-in-africa-the-african-union-report/>> accessed 28 February 2020; Abishek Mishra, 'Ushering Drones for Development Technology in Africa' (*Observer Research Foundation*, 16 June 2019)<<https://www.orfonline.org/expert-speak/ushering-drones-for-development-technology-in-africa-51920/>> accessed 12 June 2020; Edwin Ashimwe, 'Rwanda hosts Africa's first Drone flying competition next month' (*Observer Research Foundation*, 30 Jan 2020)<<https://www.newtimes.co.rw/news/rwanda-hosts-africasfirst-drone-flying-competition-next-month>> accessed 30 January 2020.

<sup>10</sup> S Watkins and Others, 'Ten questions concerning the use of drones in Urban environments' 2020 (167) *Building and Environment Journal* 1064558,106461.

<sup>11</sup> Timothy Takahashi, 'Drones and Privacy' [2012] *Columbia Science and Technology Law Review* <10.2139/ssrn.2035575> accessed 27 July 2021; Saby Ghoshray, 'Domestic Surveillance via Drones: Looking through the Lens of the Fourth Amendment' (2013) 33 *Northern Illinois University Law Review* 579; David C. Gray and Danielle Keats Citron, 'The Right to Quantitative

Noting the caution extended by Rodger Clarke<sup>12</sup> which advises that, existing laws and regulations should be examined and applied to the optimal and new laws should only be introduced, in instances where it is necessary.

This dissertation will scrutinise the policies and laws governing privacy and drones, in order to assess whether the right to privacy is satisfactorily protected within the Republic of South Africa (RSA) and the Republic of Namibia (Namibia) within the context of civilian drones.<sup>13</sup>

Moreover, the findings will be contrasted against the laws, policies, and practices applied in respect of civilian drones within the European Union (EU) and by the International Civil Aviation Organisation (ICAO), with the view of recommending policy and legal responses, to ensure that the right to privacy is protected, in the course of the deployment of civilian drones, in the aforementioned jurisdictions.

## 2. Background

Initially, dubbed flying bombs, guided missiles, or aircrafts without a pilot. Drones evolved from the military radio control flying applications and rapidly changed into more sophisticated flying systems with a lot of commercial and recreational expediency.

Today, an assortment of terms such as unmanned aircraft, unmanned aerial vehicles (UAV), unmanned aircraft (UA), unmanned aerial systems (UAS)<sup>14</sup>, and remote piloted aircraft systems (RPAS) are used to refer to drones.<sup>15</sup> The reference UAV is generally the umbrella term employed to refer to both RPAS and UA.

---

Privacy' [2013] Minnesota Law Review 62, 65; Sarah Jane Fox, 'The Rise of the Drones: Framework and Governance –Why Risk It!' (2017) 82 Journal of Air Law and Commerce 683; Sarah Jane Fox, 'Policing: Monitoring, Investigating and Prosecuting: Drones' (2019) 6(1) European Journal of Comparative Law and Governance 78,126; Sarah Jane Fox, 'Policing the Technological Revolution: Opportunities and Challenges!' [2019] Journal of the American Society for Information Science and Technology 56; Mark Burdon, *Digital Data Collection and Information Privacy Law 2* (Cambridge University Press 2020); Sarah Jane Fox, 'Past Attacks, Future Risks: Where Are We 20-years After 9/11?' (2021) 14 (3) Journal of Strategic Security 112,157.

<sup>12</sup> Roger Clarke, 'Appropriate Regulatory Responses to the Drone Epidemic' (2016) 32 (1) Computer Law & Security Review 152.

<sup>13</sup> In this thesis reference to commercial should be construed to include recreational drones as well.

<sup>14</sup> An unmanned aircraft system (UAS) is the unmanned aircraft and its associated elements (including communications links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

<sup>15</sup> Rebecca L Scharf, 'Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy' (2019) 94 (3) Indiana Law Journal <<https://www.repository.law.indiana.edu/ilj/vol94/iss3/6/>> accessed 28 April 2021.

Notwithstanding the aforesaid since the 1990s, the application is largely identified by the imitative term drone, which connotes the 'Queen Bee'<sup>16</sup>, an early military unmanned aircraft programme.<sup>17</sup> The term drone is a popular, casual, and generic substitute for an RPA or UAS and is the preferred term for this paper.

Drones are internationally considered an aircraft.<sup>18</sup> The International Civil Aviation Organisation (ICAO) defines a drone as,

[a] pilotless aircraft, in the sense of Article 8 of the Convention on International Civil Aviation, which is flown without a pilot-in-command onboard and is either remotely and fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous.<sup>19</sup>

Being considered an aircraft, the regulation of drones vests in ICAO on an international front and the Civil Aviation Authorities at a national.

Traditionally, the civil aviation industry is exclusively preoccupied with safety and security.<sup>20</sup> This pre-occupation is apparent from the reading of the ICAO, Unmanned Aircraft Systems (UAS) Circular which states that 'the principal objective of the aviation regulatory framework on drones is to achieve and maintain the highest possible uniform level of safety of persons and property on the ground'.<sup>21</sup>

---

<sup>16</sup> DH.82 Queen Bee was the first Remotely Piloted, Multiuse Unmanned Aircraft flown by the British Army.

<sup>17</sup> Rodger Clarke, 'Understanding the Drone Pandemic' (2014) 30 Computer Law & Security Review 240, 246; See also Dhananga Pathirana, 'Towards better Regulation of Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of selected National Regulations' (LLM Thesis, McGill University, 2018).

<sup>18</sup> Article 15 of the Convention Relating to the Regulation of Aerial Navigation as modified by 1929 Protocol, signed on 13 October 1919. (commonly referred to as the Paris Convention 1919); Article 8 of the Convention on International Civil Aviation adopted 7 December 1944, entered into force 4 April 1947 (15 UNTS 295) (commonly Chicago Convention); ICAO Curriculum 328/AN/190 'Unmanned Aircraft Systems' (ICAO 2011); See also Stefan A. Kaiser, 'UAVs and their Integration into Non-segregated Airspace' (2011) 36 (2) Air & Space Law Journal 161, 172; Anton Maneschijn, 'A Framework and criteria for the Operability of Unmanned Aircraft Systems' (DPhil Thesis, Stellenbosch University 2010); Manana Wanyonyi and Edison Rodgers, 'Integration of Unmanned Aircraft Systems into Civil Aviation : A study of the U.S., South Africa and Kenya' (DPhil Thesis, University of South Africa 2020).

<sup>19</sup> ICAO, *Global Air Traffic Management Operational Concept*, Doc 9854 / AN 458, (1<sup>st</sup> ed, ICAO 2005); ICAO, *Manual on Remotely Piloted Aircraft Systems*, Doc 10019 AN/507, (ICAO 2015).

<sup>20</sup> Michael Calvo, 'Uncertainty and Innovation: The Need for Effective Regulations to Foster Successful Integration of Personal and Commercial Drones' (2016) 22 Southwestern Journal of International 189, 193–94; Dhananga Pathirana, 'Towards better Regulation of Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of selected National Regulations' (Master of Laws Thesis, Institute of Air and Space Law, McGill University, Montreal 2018).

<sup>21</sup> ICAO, *Unmanned Aircraft Systems (UAS) CIR 328, AN/190* (ICAO, 2011)  
<[https://www.icao.int/meetings/uas/documents/circular%20328\\_en.pdf](https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf)> accessed 21 March 2020.

Mindful of this preoccupation with safety and security, I am of the opinion that the evolution in drone technologies necessitates, considerations beyond safety and security within the civil aviation industry.

Recalling the observation by Merchant, who postulates that, existing regulatory agencies lack the legal authority, expertise, and resources to regulate any of the emerging technologies comprehensively, even if they wanted to [...] traditional regulation may be inadvisable [...].<sup>22</sup> Marchant also highlights the fact that the risks and concerns posed by emerging technologies more often than not fall outside the ordinary jurisdiction of regulatory agencies, as an additional challenge to the effective governance thereof.<sup>23</sup>

Pathirana validates Merchant's assertions and maintains that drones have generated a host of inimitable issues indicating an urgent need for governmental response in a manner unlike any other, in the history of aviation.<sup>24</sup> He believes that the best way of dealing with drones is to adopt a co-regulatory approach. Co-regulation calls for partnerships and shared regulatory responsibilities between the government and relevant independent regulatory agencies.<sup>25</sup>

Moreover, according to a report by the Canadian Office of the Privacy Commissioner;<sup>26</sup>

---

<sup>22</sup> Gary Merchant, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 *Vanderbilt Law Review* 1861,1864.

<sup>23</sup> Gary Merchant, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 *Vanderbilt Law Review* 1861,1864.

<sup>24</sup> Dhananga Pathirana, 'Towards better Regulation of Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of selected National Regulations' (Master of Laws Thesis, Institute of Air and Space Law, McGill University, Montreal 2018) ,38.

<sup>25</sup> Christopher T. Marsden, *Internet, Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press 2011); Christopher T. Marsden, 'Internet Privacy and Data Protection' (New Perspectives on Regulation, Governance and Learning 2012 Conference Panels and Papers) (ECPR Standing Group on Regulatory Governance, 2012) <Governance and Legitimacy in Cyberspace by Christopher T. Marsden' (2012) 71(2) *The Cambridge Law Journal* 71.

<sup>26</sup> Ann Cavoukian, *Privacy and Drones: Unmanned Aerial Vehicles* (Office of the Information and Privacy Commissioner Canada, 2012)<<https://www.ipc.on.ca/wp-content/uploads/resources/pbd-drones.pdf>> accessed 26 August 2020; See also Office of the Privacy Commissioner of Canada, *Drones in Canada Report :Will the Proliferation of Domestic Drone use in Canada raise new concerns for Privacy* (Office of the Privacy Commissioner of Canada March 2013)<[https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/drones\\_201303/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/drones_201303/)> accessed 03 March 2020; Ciara Bracken-Roche et al, *Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada* (Office of the Privacy Commissioner of Canada, April 30, 2014)<[https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance\\_Drones\\_Report.pdf](https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance_Drones_Report.pdf)> accessed 1 April 2021.



[D]rones operate remotely and are increasingly autonomous, invisible (they are not always seen or heard like aircraft) and is endowed with capabilities, applications and technological payloads which enable the collection of a massive amount of personal data and a wealth of ambient information across a wide scope of terrestrial environments.<sup>27</sup>

For this reason, Calo asserts that drones hold the ability to portend the art of surveillance and undermine the right to information privacy.<sup>28</sup>

Mindful of the above, it is my considered view that there is want and a due diligence human rights duty on State(s), as well as civil aviation authorities to weave in information privacy considerations into the regulation of civilian drones in order to avert or minimise the privacy intruding potential of drone technologies.<sup>2930</sup>

This thesis, therefore, advocates that the forecasted raise in the civilian use of civilian drones<sup>31</sup> demands policy and regulatory interventions, which incorporate information privacy protection mechanisms to address the information privacy infringements likely to ensue from the use of civilian drones, in addition to the traditional safety and security issues, as is the case in respect of conventional aircrafts.<sup>32</sup>

---

<sup>27</sup>Ryan Calo, 'The Drone as Privacy Catalyst' [2011] *Stanford Law Review* 64.

<sup>28</sup>Rachel Finn et al, *Study on Privacy, Data Protection and Ethical Risks in Civil RPAS Operations* (Luxembourg: Publications Office of the European Union 2014) <<https://www.politico.eu/wp-content/uploads/2019/08/Study-on-privacy-data-protection-and-ethical-risks-in-civil-RPAS-operations-1.pdf>> accessed 28 April 2020.

<sup>29</sup>Konstantinos Dalamagkidis, K Valavanis, and Les A Pieggl, *Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations* (Spinger 2012); Ryan Calo, 'The Drone as Privacy Catalyst' [2011] *Stanford Law Review* 64; Rebeccah M Scarf 'Game of Drones: Rolling the Dice with Unmanned Aerial Vehicles and Privacy' (2017) *Scholarly Works University of Nevada, Las Vegas-William S. Boyd School of Law 1006*< [https://scholars.law.unlv.edu/facpub/1006/.](https://scholars.law.unlv.edu/facpub/1006/)> accessed 30 June 2020; See also N J Warren, 'Private Drone Use causing many to Worry, Chubb Survey Finds'( Chubb Group of Insurance Companies, 8 September 2014) <[www.prenewswire.com-releases](http://www.prenewswire.com-releases)> accessed 28 April 2021; Peter Finn, 'Domestic use of Aerial Drones by Law Enforcement likely to prompt Privacy debate' (Washington Post, 22 January 2011)<[https://www.washingtonpost.com/national/domestic-use-of-aerial-drones-by-law-enforcement-likely-to-prompt-privacy-debate/2011/01/22/ABLD0MR\\_story.html](https://www.washingtonpost.com/national/domestic-use-of-aerial-drones-by-law-enforcement-likely-to-prompt-privacy-debate/2011/01/22/ABLD0MR_story.html)> accessed 04 August 2020; Jay Stanley and Catherine Crump, *Protecting Privacy from Aerial Surveillance: Recommendations for Government use of Drone Aircraft* (American Civil Liberties Union, December 2011) <<http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>> accessed 28 April 2020.

<sup>30</sup>David Banisar and Simon Davies, 'Global Internet Liability Campaign, Report on Privacy and Human rights: An International Survey of Privacy Laws and Practice' (Privacy International, no date supplied) <<http://gilc.org/privacy/survey/intro.html#defining>> accessed 21 March 2020.

<sup>31</sup>Rico Merket and James Bushell, 'Managing the Drone evolution: A Systematic Literature Review into the Current Use of Airborne Drones and Future Strategic Directions for their Effective Control' (2020) 89 *Journal of Air Transport Management* 101929.

<sup>32</sup>Richard M Thompson, *Domestic Drones and Privacy: A Primer* (Congressional Research Service 30 March 2015) <<https://sgp.fas.org/crs/misc/R43965.pdf>> accessed 11 March 2021; Kristen Thomasen, 'Personal Drones, AI and our Privacy' (Policy, Options & Politiques, 20 February, 2018)<<https://policyoptions.irpp.org/magazines/february-2018/personal-drones-ai-and-our-privacy/>> accessed 30 March 2020; See also ; Dhananga Pathirana, 'Towards better Regulation of

### 3. Drones and Information Privacy

It is a foregone conclusion that owing to the proficiencies and applications drones are endowed with, may advertently or inadvertently infringe the right to (information) privacy.<sup>33</sup>

The scope of the confrontation between privacy and drones is neatly captured in various literature, which elaborately sets out the privacy and information privacy risks associated with the use of drones, alongside other adverse legal and ethical implications.<sup>34</sup>

It is postulated that the unabated civilian use of drones is tantamount to approving 'trespass' and thus constitutes a serious violation of the right to information privacy.

The right to privacy is widely hailed as a first generational fundamental human right.<sup>35</sup> It is protected *inter alia* under Article 12 of the Universal Declaration of Human Rights (UDHR), Article 16 of the United Nations Convention on the Rights of the Child (CRC), Article 17 of the United Nations Convention on Civil and Political Rights (ICCPR), the African Union Convention on Cyber Security and Personal Data Protection (hereinafter referred to as the Malabo Convention).<sup>36</sup>

Similarly, the RSA<sup>37</sup> and Namibian Constitutions extend protection to the privacy of all persons (natural and juristic persons) under section 14 and article 13, respectively.

Section 8(1)-(2) of the RSA Constitution and article 5 of the Namibian Constitution enjoin the respective States, as well as all-natural and juristic persons, to protect

---

Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of selected National Regulations' (LLM Thesis, McGill University, 2018).

<sup>33</sup> See Table1 of this Chapter.

<sup>34</sup> Rachel Finn et al, 'Study on Privacy, Data Protection and Ethical Risks in Civil RPAS operations' (Luxembourg:Publications Office of the European Union 2014) <<https://www.politico.eu/wp-content/uploads/2019/08/Study-on-privacy-data-protection-and-ethical-risks-in-civil-RPAS-operations-1.pdf>> accessed 28 April 2020.

<sup>35</sup> Caroline B Ncube, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems' (2004) (2) 4 Journal of Information, Law and Technology 1, 24, 27; Yayanta Gosh, 'Data Protection: A Different Dimension under Human Rights and Intellectual Property Law' (2015) (1) International Journal of Justice and Legal Studies 39.

<sup>37</sup> South Africa Act 108 of 1996 (hereinafter referred to as the RSA Constitution).

and uphold the fundamental rights and freedoms guaranteed under their Constitutions, which includes the right to privacy.

These Constitutions also stipulate that this right to privacy can only be restricted if legislation to that effect was promulgated, and the restrictions so imposed are reasonable and justifiable to foster public interest, provided that the essential content of the rights are not negated.

In order to give expression to the constitutional right to privacy, the RSA promulgated the Protection of Personal Information Act<sup>38</sup> (POPIA), which became fully operational on 1 July 2020.<sup>39</sup>

The short title of the POPIA provides that, the objective of the Act is *inter alia* 'to set minimum standards for the lawful processing of personal information and to promote the protection of the right to privacy by public and private bodies, as a means to safeguard the right to privacy under the RSA Constitution'.

The POPIA prescribes compliance with eight minimum standards as an appropriate measure to protect the constitutional right to privacy. In summary, the POPIA requires that personal information must be:

- obtained fairly and lawfully;
- used only for the originally specified purpose;
- adequate, relevant, and not excessive for the purpose for which it was obtained;
- accurate and up-to-date at all relevant times;
- destroyed after completion of the purpose for which it was obtained
- accountability; and
- data subject participation.

At present Namibia does not have legislation dedicated to addressing information privacy and is in the process of developing a Data Protection Law. The Data Protection

---

<sup>38</sup> Act 4 of 2013.

<sup>39</sup> Proclamation 14 of 2014; See also Hunton Andrews Kurts, 'Privacy and Cybersecurity: South Africa's Protection and Personal Information Act, 2013 goes into effect July 1' (The National Review: 29 June 2020) <<https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1>> accessed 26 Jan 2021.

Bill was considered by the Namibian Cabinet Committee on Legislation (CCL) on 07 October 2021, but regrettably, it is not cleared for onward transmission to Parliament.<sup>40</sup> Several public consultations on the Bill took place for the major part of 2022 on recommendation by the CCL.<sup>41</sup>

#### 4. The Privacy-Intruding potential of Drones

The nexus between the use of drones and information privacy protection infringements depends on the scope of data that a drone can amass, as elicited by the information communication technologies it is endowed with, which may comprise of any of the following or a combination of the following:<sup>42</sup>

TECHNOLOGY	USE/PURPOSE
<b>Facial recognition or other biometric recognition technology</b>	Detecting biographic identification attributes such as height, age, gender, and skin colour
<b>High-power zoom lenses</b>	Enabling real-time video capabilities at imperceptible distances
<b>Night vision, infrared, ultraviolet Forward-Looking Infrared Radar (FLIR) / thermal imaging, and Light Detection and Ranging (LIDAR) technology</b>	Enabling the capturing of information such as heat emanations

<sup>40</sup> See discussion on the Namibian Data Protection Bill in Chapter two hereof.

<sup>41</sup> Paul Hartman, 'Stakeholders meet on data protection bill' The Namibian (Windhoek, 29 November, 2022) <<https://www.namibian.com.na/6226193/archive-read/Stakeholders-meet-on-data-protection-bill>> accessed 1 December 2022.

<sup>42</sup> Table compiled from information the following sources: Office of the Privacy Commissioner of Canada, 'Drones in Canada: Report prepared by the Research Group of the Office of the Privacy Commission of Canada' (Privacy Commissioner of Canada: March 2013) <[https://www.priv.gc.ca/media/1760/drones\\_201303\\_e.pdf](https://www.priv.gc.ca/media/1760/drones_201303_e.pdf)> accessed: 03 March 2020; Jay Stanley and Catherine Crump, 'Protecting Privacy from Aerial Surveillance: Recommendations for Government use of Drone Aircraft' (American Civil Liberties Union, December 2011) <<http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>> accessed 28 April 2020; Timothy Takahashi, 'Drones and Privacy' [2012] Columbia Science and Technology Law Review <10.2139/ssrn.2035575> accessed 27 July 2021; Saby Ghoshray, 'Domestic Surveillance via Drones: Looking through the Lens of the Fourth Amendment' (2013) 33 Northern Illinois University Law Review 579.

<b>Radar Technology</b>	Collecting information by penetrating various surfaces including walls, all types of weather conditions, and even foliage, detecting chemical and magnetic composition of objects
<b>Video analytics</b>	Algorithmically flag deviations from normal processes
<b>Wifi Information Communication Technology</b>	Transmitting communication signals
<b>Automated license plate recognition technology</b>	Recognising images and reading license plates
<b>Distributed network surveillance technology</b>	Offering a wide scope of intelligence analysis when integrated with surveillance networks or digital technologies
<b>Modular Cyber-attack hardware</b>	Enabling interception, corruption, hacking, decryption, and jamming of data

<p><b>Audio recordings and GPS recording technology</b></p>	<p>Capturing sound and location information</p>
---	---

**Column 1: Table summarising the information that can be captured by Drones.**

Whereas the civilian use of drones presents a wide range of benefits, it holds the potential to produce various impairments, as well. <sup>43</sup> Owing to the above-summarised capabilities of drones, there is a great probability that the unabated use of civilian drones may eviscerate the human right to privacy.

Kindly bear in mind that this thesis is overtly dedicated to investigating the information privacy consequences of civilian drones, as distinguished from physical bodily privacy.

From a preliminary analysis, the deployment of drones offends the following minimum standards under POPIA:<sup>44</sup>

- **Lack of transparency:** owing to their size and distance from the remote pilot, drones operations are clandestine, data subjects will invariably be unconscious that their personal information is captured or will find it grim to determine the scope of the personal information that has been apprehended; as well as the identity and scope of personal data being processed.

---

<sup>43</sup>Thomas P Hughes, *American Genesis; A Century of Innovation and Technological Enthusiasm* (Edward Elgar Publishing 2006) 188; See also Ciara Braken-Roche, 'Surveillance Drones Privacy Implications of the Spread of Unmanned Aerial Vehicles in Canada' (Surveillance Study Centre Queen's University: 30 April, 2014)<[https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance\\_Drones\\_Report.pdf](https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance_Drones_Report.pdf)> accessed 21 March 2020; Shayna Gersher, 'Eyes in the Sky: The Domestic Deployment of Drone Technology & Aerial Surveillance in Canada'(Master's Thesis Carleton University 2014); Rocci Luppicini and Arthur So, 'A Techno Ethical Review of Commercial Drone use in the context of Governance, Ethics and Privacy' (2016) 46 *Technology in Society* 109,119 < DOI: 10.1016/j.techsoc.2016.03.003>accessed 30 November 2021

- **Unauthorised processing and over-collection:** the deployment of drones may result in the inapt processing of personal information or processing void of legitimate or for unspecified purposes;
- **Accountability:** being remotely controlled and inconspicuous owing to its size, those who process personal information using drones can escape the duty to observe the information privacy protection principles or be held accountable for failing to implement information privacy safeguards imposed by law;
- **Function creep (Secondary use);** moreover, save if data subjects are accorded active control of their personal information, personal information processed by drones may be further utilised for unrelated and or illicit purposes.<sup>45</sup>

## 5. Problem Statement

In line with the general academic opinion, my preliminary examination of the drone regulatory framework in the jurisdictions under discussion indicates that drones are still exclusively regulated, in relation to safety, security and to a limited degree environmental protection only<sup>46</sup> and that limited to no consideration is afforded to the impact of drone technologies on the right to privacy in regulating the drones.<sup>47</sup>

Civil aviation regulators are engrossed with safety and security and consider it imperious to be required to focus on the privacy implications of drones.<sup>48</sup> Moreover, they are often

---

<sup>45</sup>Thomas P Hughes, *American Genesis; A Century of Innovation and Technological Enthusiasm* (Edward Elgar Publishing 2006) 188.

<sup>46</sup> Section 10 of the Namibian Civil Aviation Act 6 of 2016. The long title of provides *inter alia* that, the SCAA is established to exercise aviation safety and security within RSA.

<sup>47</sup> Thomas Lawrenson and Ricardo De Oliveira, 'South Africa: without Drone-ing On: Legal Overview of Drones in South Africa' (Clyde & Co, 17 October 2018) <<https://www.mondaq.com/southafrica/aviation/746350/without-drone-ing-on-a-legal-overview-of-drones-in-south-africa>> accessed 7Jan 2021; See also Siyabulela Matanzima and Vilimile Gumede, 'Drones and Delict: Robot Usage and Damage in South African Law' (Snail Attorneys @ Law Inc, 2019) < <http://www.lex-informatica.org/wp-content/uploads/2020/08/DRONES-AND-DELICT-Artificial-Intelligence-Robot-Usage-and-Damage-in-South-African-Law.pdf>>accessed 20 July 2020; Sharlene Naidoo, 'Drone Laws South African Commercial Regulations' (Drone Laws, February 2020)<[http://www.durban.gov.za/City\\_Services/engineering%20unit/Surveying\\_Land\\_Information/Documents/DroneLawsSouthAfricanCommercialRegulations.pdf](http://www.durban.gov.za/City_Services/engineering%20unit/Surveying_Land_Information/Documents/DroneLawsSouthAfricanCommercialRegulations.pdf)> accessed 21 March 2021 L A, Ingham, 'Considerations for the Roadmap of Unmanned Aerial Vehicles (UAV) in the South African Airspace' (PHD Dissertation, Stellenbosch University 2008) 209; Roger Clarke and Lyria Bennett Moses 'The Regulation of Civilian Drones' Impacts on Public Safety' (2014) 30 (3) Computer Law & Security Review 263, 285.

<sup>48</sup>Rodger Clarcke, 'The Regulation of Civilian Drones' Impacts on Behavioural Privacy' (2014) 30 (3) Computer Law & Security Review 286-305; Riaan Stopforth, 'Drone Licenses-Necessities and Requirements' (2017) 73 (1) International Journal of Sciences and Research 149,159; See also

endowed with limited personnel with exclusive civil aviation-specific technical skills and inadequate financial resources to take on the gigantic responsibility of protecting the right to privacy, alongside ensuring aviation safety and security, and environmental protection.<sup>49</sup>

Based on the common law understanding of privacy, this preoccupation is often in my opinion erroneously justified by the assumption that there is sufficient redress under civil and criminal law to vindicate infringement(s) to the right to privacy.

This fixation is evident from the public notice on the Namibian Civil Aviation Authorities (NACAA) website<sup>50</sup>. The NACAA website contains a disclaimer that all privacy queries fall outside the scope of the NACAA and that the Ministry of Home Affairs, Immigration, Safety, and Security; the ministry responsible for NAMPOL should be consulted instead, for any privacy-related queries. The website contains a statement that unequivocally refutes any responsibility of NACAA in respect of privacy issues.

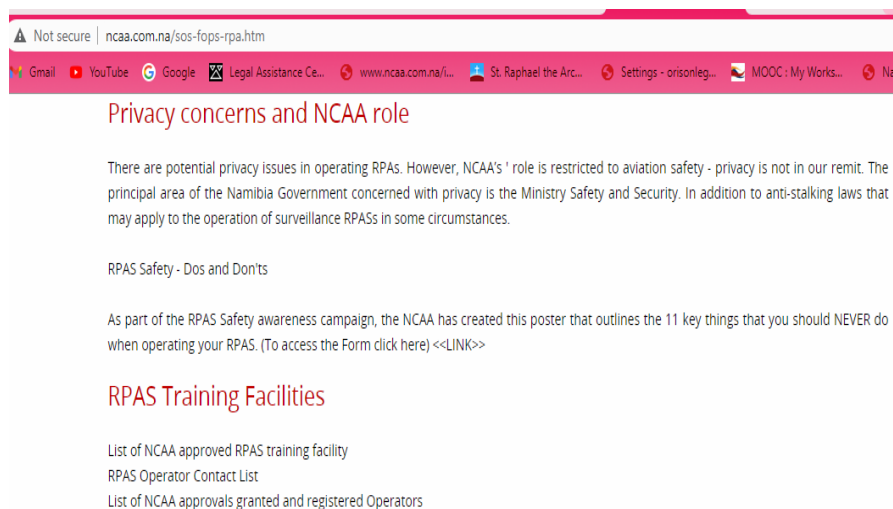


Figure 2: Screenshot from Namibian Civil Aviation Authorities Website<sup>51</sup>

---

Sonet Kock 'An Overview of South African RPAS Regulations' (EE Publishers, 13 February 2015) <<https://www.ee.co.za/wp-content/uploads/2015/08/Sonet-Kock.pdf>> accessed 21 June 2020.

<sup>49</sup>Marzocchi Ottavio, *Privacy and Data Protection Implications of the Civil use of Drones: In-depth Analysis* (4th ed, European Parliament Publications, 2015) < <http://www.europarl.edu.studies>> accessed 30 March 2020; L A, Ingham, 'Considerations for the Roadmap of Unmanned Aerial Vehicles (UAV) in the South African Airspace' (PHD Dissertation, Stellenbosch University 2008) 209.

<sup>50</sup>See figure 2 below.

<sup>51</sup> Screenshot from Civil Aviation Authority of Namibia Website (NACCA 15 December 2020) <<http://www.ncaa.com.na/>> accessed 15 December 2020.



However, this author supports the proposition advanced by many prominent writers, who postulate that some of the threats imposed on the right to privacy by drones are indictable under criminal and or civil law.<sup>52</sup> The remedies available under the above-mentioned branches of law can only be invoked *post-ante* following more often than not, irreparable harm to the fragile right to information privacy.<sup>53</sup>

Aggrieved persons will invariably only obtain redress after being subjected to a protracted and costly court process. Consequent to this, inappropriate restorative remedies, which are only available to those who enjoy the privilege of being able to afford legal counsel, will regrettably be imposed by courts.<sup>54</sup>

Bearing in mind the above, it is my conviction that the current legal framework applicable to drones in the RSA and Namibia lacks information privacy considerations and to that end, undermines the constitutional guarantee of the right to privacy.

Resultantly, I advance that the Civil Aviation Authorities within these respective countries are constitutionally bound to take steps to avert the potential threats to the right to privacy posed by the use of drone technologies, by adopting a proactive due diligence human rights risk-based regulatory approach, to ensure that the regulatory framework on drones in these jurisdictions promotes and protects the constitutional guarantee to privacy, as enshrined under section 8 and article 5 of the RSA and Namibian Constitutions, within the limits permitted by law.

## **6. Purpose**

The key purpose of this paper is to appraise the legal framework governing information privacy and drones within the RSA and Namibia, in order to determine the degree to which information privacy considerations are incorporated in the course of regulating and deploying civilian drones.

---

<sup>53</sup> Alex B Makulilo, 'Protection of Personal Data in Sub-Saharan Africa' (PhD Thesis, University of Bremen 2012); Anneliese Roos, 'Core Principles of Data Protection Law' (2006) 36 Comparative and International Law Journal of South Africa 102; Anneliese Roos, 'Personal Data Protection: explaining the International backdrop and Evaluating the current South African position' (2007) 124 South African Law Journal 400; Anneliese Roos 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) (4) Potchefstroom Electronic Law Journal 62; Anneliese Roos, 'Data Privacy Law': In Dana Van der Merwe et al, Information and Communication Technology Law (3rd ed, LexisNexis Durban 2021).

<sup>54</sup>See also Nomalanga Mashinini, 'The processing of Personal Information using Remotely Piloted Aircraft Systems in South Africa' [2020] De Jure Law Journal 140.

The question to be addressed in this thesis is: **whether or not the right to privacy is sufficiently promoted and protected in the regulation of civilian drones in the Republic of South Africa and Namibia?**

To answer this research question, I will;

1. scrutinise Part 101: Remotely Piloted Aircraft Systems of the Civil Aviation Regulations, 2011 issued under the South African Civil Aviation Act,<sup>55</sup> as well as Part 101 of the draft Civil Aviation Regulations<sup>56</sup> passed in terms of section 236 (2) of the Namibian Civil Aviation Act,<sup>57</sup> as amended, which governs the use of drones in the jurisdictions under discussion;
2. evaluate the POPIA and the Data Protection Bill of Namibia,<sup>58</sup> to determine the information privacy principles, safeguards, and mechanisms extended to data subjects within these jurisdictions, which must be adhered to in the course of regulating and deploying civilian drones;
3. undertake a comparative analysis of the principles, laws, administrative mechanisms and guidelines applied to safeguard the right to information privacy as it relates to drones, in the EU, as well as within the ICAO against that in the RSA and Namibia, in order to draw lessons from these more accomplished jurisdictions on how to bolster the information privacy responsiveness of the RSA and Namibian drone regulations.

To this end, I will endeavour to provide recommendations for policy and legal interventions, to ensure that the right to privacy is promoted across the civilian drone regulatory spectrum.

---

<sup>55</sup> 13 of 2009.

<sup>56</sup> NAMCARs Part 101; RPAS (Drones and other Remotely Piloted Aircrafts), as published in Government Gazette No. 7157 of 27 March 2020. Available at <<http://www.ncaa.com.na/index.php/documents/secondary-legislation/regulations-namcars>> accessed 16 June 2021.

<sup>57</sup> Act 16 of 2006.

<sup>58</sup> Version workshopped 24-26 February 2020 GLACY+ Stakeholders Consultation Workshop and submitted to the Cabinet Committee on Legislation on 07 October 2021 <<https://mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25>> accessed 26 August 2020.

## 7. Scope of the Study

This thesis is limited to the protection of the right to information privacy within the context of civilian (commercial and recreational) drones, to the exclusion of drones employed for purposes of maintaining law and order, or national security and military drones.

Scant consideration will be given to the technical historical development of drone technologies and the security and technical aspects thereof. The thesis similarly does not address issues of freedom of expression and other justifiable public interest limitations to the right to privacy, the same being exempted in terms of the respective Constitutions, POPIA, and the envisaged Namibian Data Protection law.

This academic enquiry also excludes discussions on the comprehensive right to privacy and its development under common law, save as is expedient to contextualise the discussions herein and will focus exclusively on information privacy, as an enabler of the comprehensive right to privacy.

The EU is hailed as the World's Tech Police Man<sup>59</sup> and information privacy is a fundamental right under Article 7 of the EU Charter of Fundamental Rights (EU Charter) and is the foremost continent to adopt a binding international treaty on information privacy,<sup>60</sup> which is hailed as the mother of information privacy and complemented by an additional Protocol thereto.<sup>61</sup>

Moreover, considering that the EU's information privacy rules are among the toughest in the world and that following the operationalisation of the General Data Protection Regulation(GDPR)<sup>62</sup>, it became the prime exporter of its information privacy rules.<sup>63</sup> This paper benchmarked the policies, laws, and regulations governing the information

---

<sup>59</sup> Mark Scott, 'Europe's Tech Ambition: To be the World's Digital Policeman'(Politico 20 August 2017)<<https://www.politico.eu/article/europe-tech-ambition-to-be-world-digital-policeman/>>accessed 15 January 2021.

<sup>60</sup>Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data (adopted 28 January 1981, entered into force 1 October 1985) CETS 108 (Convention 108).

<sup>61</sup> Council of Europe, Additional Protocol to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, 2001, (adopted, entered into force 28 November 2001 and updated in 2018),CETS 181+ (Convention 108+);

<sup>62</sup> EU General Data Protection Regulation 2016/679 of 27 April 2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.GDPR [has been described as the new golden standard for data protection].

<sup>63</sup> Alessandro Mantelero, 'The future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 Computer Law & Security Review 105500.

privacy implications of drones within the Republic of Namibia, RSA against that of the EU.

Additionally, this paper further assesses the regulation(s) in question against the framework advanced by the International Civil Aviation Organisation (ICAO). The ICAO is the world's leading agency in aircraft and airspace regulation. On 23 June 2020, ICAO issued Model UAS (Unmanned Aircraft Systems) Regulations, as well as various Advisory Circulars (ACs) which represent the contemporary consensus on the best practices in respect of regulating drones on the international level.<sup>64</sup>

## **8. Limitations of the Study**

In the course of the research process, the researcher anticipates encountering challenges, owing to the following:

Firstly, privacy and information privacy are vast, multi-dimensional subjects, with a notable lack of clarity and parameters in the current law and jurisprudence.

Additionally, bearing in mind that the POPIA only became fully operational recently, there has not been sufficient room for the development of jurisprudence elucidating the application of information privacy principles, therefore a lot of reliance will be placed on secondary sources.

Moreover, there is a dearth of literature investigating drones with reference to their information privacy implications and how the information privacy challenges posed by drone technologies must be addressed.

There appears to be no consensus outside the EU on how to address the privacy concerns of drone technologies.

Owing to the above it was challenging to offer an all-encompassing synopsis of the thesis topic.

---

<sup>64</sup>ICAO Model UAS Regulations titled Parts 101, 102 and 149. Available at <<https://www.icao.int/safety/UA/UAID/Pages/Model-UAS-Regulations.aspx>>accessed: September 2020.

## **9. Research Methodology**

This paper employed the qualitative legal research approach through the analysis of primary and secondary sources of law relevant to the subject matter of this thesis.<sup>65</sup>

The literature study primarily includes legislation, case law, textbooks, reports, journal articles, as well as electronic resources. This paper critically examines and undertakes a textual examination of applicable sources.

In applying this methodology, legal scholarly works were predominantly studied to propose a legal reform on how and to what extent the existing legal framework on information privacy and civilian drones offer protection for the right to information privacy.

This work will set out a comparative analysis of the principles, laws, administrative mechanisms and guidelines applied to safeguard the right to information privacy in the EU, as well as within ICAO against those applicable in the RSA and Namibia, which will abet the author to formulate recommendations for policy and legal interventions to ensure that information privacy is promoted within the drone industry.

## **10. Point of Departure**

Whenever the international and domestic regulatory framework applicable to drones will be discussed, the focus was limited to the provisions which have privacy implications.

Owing to the historical contingency of the Namibian and RSA legal systems, to the extent that it is feasible, save in instances where there are glaring disparities in the legal position(s) in the RSA and Namibia, a single discussion is advanced as a representation of both jurisdictions. Separate discussions were resorted to only in instances where there are manifest differences in the legal positions on a matter within these two jurisdictions.

---

<sup>65</sup> Eric Hofstee, *Constructing a Good Dissertation: A Practical Guide to Finishing a Master's, MBA or Phd on Schedule* (EPE Publishers 2006 (2018) reprint).

## **11. Hypothesis**

At this stage, it is my considered opinion that the current legal framework governing drones in South Africa and Namibia substantially lacks considerations of information privacy and to that end, undermines the constitutional guarantee to the right of privacy and is a flagrant dereliction of human rights due diligence call on the States, the aviation regulatory agencies, drone operators and pilots.

Since the existing civil and criminal remedies in law do not give data subjects active control over their personal information, for example, the data subject does not have knowledge of the fact that his or her personal information has been collected, or that he or she can demand access to the information, or that he or she may correct incorrect information, etc.

This paper, therefore, argues that the protection of the right to privacy under criminal and civil law is not sufficient to provide adequate information privacy protection to the information privacy challenges posed by drone technologies.

Consequently, I postulate that the respective states and civil aviation regulators are constitutionally bound to take proactive steps to avert the information privacy threats occasioned by the use of drone technologies. This should be done through proactive due diligence human rights risk-based regulations to ensure that drone operators and pilots execute their operations in a way that protects and promotes the constitutional right to information privacy.

## **12. Synopsis of Chapters**

### **Chapter One: General Introduction**

This chapter sets out the general introduction to the thesis. It contains *inter alia* the background to the research problem, the objectives of the study and the methodology followed in the course of the research. To offer a signpost to readers, it also sets out a summary of the various chapters of the entire paper.

### **Chapter Two: Selected Literature Review**

This chapter examines the academic, judicial, policy, human rights and statutory framework of the right to information privacy in the RSA and Namibia. It also analyse the affiliation between information privacy protection and privacy and postulates that,

information privacy protection must be designated as a fourth-generational human right. It also deliberates on the contemporary debate regarding posthumous information privacy protection.

### **Chapter Three: The interplay between Drones and Privacy**

This chapter appraise the POPIA and the Data Protection Bill of Namibia,<sup>66</sup> in order to determine the information privacy principles, safeguards and mechanisms extended to data subjects within these jurisdictions, which must be adhered to in the course of regulating and deploying civilian drones.

### **Chapter Four: Applying the Legal Concept of Information PRIVACY Protection to Drone Laws in RSA and Namibia**

Following the abridgement of the international and national information privacy legal frameworks in the earlier chapters. This chapter canvass the drone-specific laws in RSA and Namibia to determine the extent to which they are consistent with the information privacy principles, particularly the stipulations in POPI (and the Namibian Bill on Data Protection). It will also explore the extent to which these laws can be purposed to protect people from the unlawful processing of their personal information by civilian drones.

### **Chapter Five: The European Union Legal Framework on Drones**

The EU is the first jurisdiction to acknowledge information privacy as an independent Human Right. Having recently reformed its legal framework to regulate drones, which is hailed to incorporate amongst others information privacy protection. This Chapter examines the legal framework on drones within the EU through the prism of information privacy, anticipating to glean possible lessons on how RSA and Namibia can promulgate a more information privacy-focused regulatory framework on drones, and hopeful to borrow lessons on how to weave in information privacy considerations across the drone regulatory spectrum

---

<sup>66</sup> Version workshopped 24-26 February 2020 GLACY+ Stakeholders Consultation Workshop and submitted to the Cabinet Committee on Legislation on 07 October 2021 <<https://mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25>> accessed 26 August 2020.

## **Chapter Six: Information Privacy within the Global Civil Aviation Drone Regulatory Regime**

This chapter investigates the place of information privacy within the scope of the global civil aviation regulatory regime and investigates the methodology adopted by the ICAO to address the information privacy challenges highlighted in chapters one and two of this thesis, as well as the avenue(s) available within the regulatory spectrum of ICAO to address the information privacy implications of drones, if any

## **Chapter Seven: Conclusions,**

This chapter sets out the main conclusions of this study as well as a summary of the key findings of this paper. It also illustrates my contribution to the research on which this thesis was built, as well as the agenda for further research. Most importantly, it endeavours to advocate for policy and legal interventions for the future regulation of drones to promote the right to information privacy.



## Chapter Two

### Selected Literature Review

---

*This chapter offers a synopsis of the academic literature that informs this thesis. It sets out a brief history and importance of information privacy. It also discusses the scope and significance of information privacy protection and investigates the relationship between the right to privacy and information privacy protection.*

#### 1. Introduction

A great deal of the consulted literature underscores the increasing eminence and expediency of drones.<sup>67</sup> A significant number of sources extrapolate the benefits and risks posed by drone technologies, which predominantly includes the unauthorised processing of personal information and the evisceration of the right to privacy.<sup>68</sup>

In light of the forecast that drone flights will become as common as road transport modes.<sup>69</sup> Much of the earlier research highlights the need for interventions to address the information privacy apprehensions of drone technologies. The hostility between privacy, information privacy and drone technologies are also neatly captured in various literature enquiries.<sup>70</sup> A great deal of the literature elaborately

---

<sup>67</sup> Robin Kellermann, Tobias Biehle and Liliann Fischer, 'Drones for Parcel and Passenger Transport: A Literature Review' (2020) 4 *Transportation Research Interdisciplinary Perspectives* 100088; Rodger Clarcke, 'The Regulation of Civilian Drones' Impacts on Behavioral Privacy' (2014) 30 (3) *Computer Law & Security Review* 286,305.

<sup>68</sup>Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (1st Edition, Oxford University Press 2014).

<sup>69</sup>Tim Hornyak, 'The flying taxi market may be ready for take-off, changing the travel experience forever' (CNBC, 9 March 2020 )< <https://www.cnbc.com/2020/03/06/the-flying-taxi-market-is-ready-to-change-worldwide-travel.html>>accessed 31 October 2021; Adrienne Bernhard, 'The Flying Car is here and it could Change the World' (BBC,12 November 2020) <<https://www.bbc.com/future/article/20201111-the-flying-car-is-here-vtols-jetpacks-and-air-taxis>> accessed 31 October 2021.

<sup>70</sup>Robin Kellermann, Tobias Biehle and Liliann Fischer, 'Drones for Parcel and Passenger Transport: A Literature Review' (2020) 4 *Transportation Research Interdisciplinary Perspectives* 100088; Jean-Paul Yaacoub et al, 'Security analysis of Drones Systems: Attacks, Limitations, and Recommendations'(2020) 11 *Internet of Things* <Published online <10.1016/j.iot.2020.100218> accessed 12 December 2021; Koliwe Majama, Janny Montinat and Anriette Esterhuysen (Cordinators), *Privacy and Personal Data Protection in Africa: A Rights- based Survey of Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021)

sets out the privacy and or information privacy menaces associated with the use of drones.<sup>71</sup>

The dominant academic opinion postulates that the unabated commercial use of drones will be tantamount to sanctioning trespass and thus constitute a serious infringement of the right to information privacy.<sup>72</sup>

Although there is still much debate regarding the scope and relationship between the right to privacy and information privacy protection, it is generally agreed that information privacy protection is an enabler of the right to privacy.<sup>73</sup>

## 2. History of Information Privacy

The concept of privacy developed as a consequence of the insistence on the private and public law divide.<sup>74</sup>

Literature attributes the ground-breaking academic work on information privacy to an 1890 Harvard Law Review paper titled *The Right to Privacy* which was authored by Samuel Brandeis and Louis Warren,<sup>75</sup> that investigated the threats caused by technological development. The authors defined information privacy as 'the right to be left alone'.<sup>76</sup>

---

<sup>71</sup> Rachel Finn et al, 'Study on Privacy, Data Protection and Ethical Risks in Civil RPAS operations' (Luxembourg: Publications Office of the European Union 2014) <<https://www.politico.eu/wp-content/uploads/2019/08/Study-on-privacy-data-protection-and-ethical-risks-in-civil-RPAS-operations-1.pdf>> accessed 28 April 2020.

<sup>72</sup> Rico Merket and James Bushell, 'Managing the Drone Revolution: A systematic Literature Review into the current use of Airborne Drones and Future Strategic Directions for their effective control' (2020) 89 *Journal of Air Transport Management* 101929.

<sup>73</sup> Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (1st Edition, Oxford University Press 2014).

<sup>74</sup> According to S K Amoo, *An Introduction to Namibian Law: Materials and Cases* (Macmillan Education Namibia, 2008); Private law applies to relationships between individuals in a legal system. e.g. contracts and labour laws. Public law applies to the relationship between an individual and the government. e.g. criminal law; Dorothy J Glancy, 'The Invention of the Right to Privacy' (1979) 21 *Arizona Law Review* < <https://law.scu.edu/wp-content/uploads/Privacy.pdf>> accessed 30 June 2020.

<sup>75</sup> Brandeis, Louis and Samuel Warren, 'The Right to Privacy' [1890] 5 *Harvard Law Review* 193; Jayanta Ghosh, 'Data Protection: A Different Dimension under Human Rights & Intellectual Property Law' (2015) (II) *International Journal of Justice & Legal Studies* 40; See also Bratman, B. E 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2002) 69 *Tennessee Law Review* 344.

<sup>76</sup> Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 (5) *Harvard Law Review* 193; Benjamin E Bratman, 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2002) 69 *Tennessee Law Review* 344; Fred R Shapiro, 'The Most-cited Articles' (1985) 73 (5) *California Law Review* 1545.

Other equally foundational academic writings on the subject, include Alan Westin's<sup>77</sup> book *Privacy and Freedom*<sup>78</sup> and Miller's *Assault on Privacy*.<sup>79</sup> Alan Westin<sup>80</sup> described privacy as 'the desire of people to freely choose under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others'.<sup>81</sup>

The older literature,<sup>82</sup> view information privacy, as a part of property law and invariably associates it with the initiatives of the Organisation of Economic Cooperation and Development (OECD).<sup>83</sup> The OECD supports information privacy, on the understanding that information privacy protection fosters the free flow of information, which in turn stimulates economic growth. It posits that the lack of free flow of information will cause apathy in electronic commerce.

A great deal of literature in this group presents information privacy within the parameters of intellectual property, patents and copyright law.<sup>84</sup> This school of thought<sup>85</sup> justify information privacy protection on economic grounds and postulates that information privacy protection outside the economic sphere is superfluous. Owing to this focus, the establishment of supervisory authorities and

---

<sup>77</sup> Alan Westin is hailed as the father of modern privacy explains privacy with reference to its significance and interplay with politics, socio-culture, as well as personal/ communal views.

<sup>78</sup> Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

<sup>79</sup> Arthur R Miller, *The Assault on Privacy* (Michigan University Press 1971) 326; Charles R. Ashman, 'The Assault on Privacy by Arthur R. Miller' (1971) 20 DePaul Law Review 1062 <<https://via.library.depaul.edu/cgi/viewcontent.cgi?article=2982&context=law-review>> accessed 23 December 2021.

<sup>80</sup> A F Westin, 'Social and Political dimensions of Privacy' (2003) 59 (2) Journal of Social Issues 431.

<sup>81</sup> Jayanta Ghosh, 'Data Protection: A Different Dimension under Human Rights and Intellectual Property Law' (2015) 1 (2) International Journal of Justice & Legal Studies 40.

<sup>82</sup> Adam Warren, James Dearnly and Charles Oppenheim, 'Sources on Data Protection and Human Rights' (2002) 2 Journal of information, Law and Technology <<http://elj.warwick.ac.uk/01-2/warren.html>> accessed 28 April 2020.

<sup>83</sup> OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980 [Revised in 2013]. Available at <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>> accessed 16 September 2022; OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (OECD, no date supplied) <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm#background>> accessed 24 December 2021.

<sup>84</sup> Nadezhda Purtova, 'Property in Personal Data: European Perspectives on the Instrumentalist Theory of Propertisation' (2010) 2 (3) European Journal of Legal Studies 35-54; Nadezhda Purtova, 'The Law of everything: Broad concept of Data Protection and future of EU Data Protection Law' (2018) 10 (2) Tilburg Institute of Law, Innovation & Technology and Society <DOI:10.1080/17579961.2018.1452176> accessed July 2021; Vera Bergelson, 'It is Personal, but it is Mine? Towards Property Rights' (2004) 37 (2) University of California, Davis Law Review School 379,451 <<https://doi.org/10.7282/00000015>> accessed 14 July 2021.

<sup>85</sup> Also referred to as the Instrumentalist Theory of Propertisation.

information privacy protection enforcement mechanisms were not accentuated within this assortment of the literature.<sup>86</sup>

This author is of the view that commoditising personal information de-humanises the human rights value of information privacy and lamentably fails to recognise the human rights significance of information privacy.

After the UN and the CoE became vested with information privacy, the literature in respect of information privacy became more human rights-focused.<sup>87</sup> Consequently, an extensive slice of the literature places information privacy within the parameters of human rights law.<sup>88</sup> This faction of the literature also introduced discussions on information privacy monitoring and supervisory mechanisms, such as the establishment of national and international information privacy protection authorities and cooperation networks.<sup>89</sup>

This human rights view of information privacy culminated in the recognition of information privacy as a human right separate from the right to privacy, under Article 7 of the EU Charter. This classification remains a prominent school of thought, particularly amongst EU scholars.<sup>90</sup>

---

<sup>86</sup>Magdalena Sepulveda et al, 'International Supervisory Mechanisms for Human Rights; in *Human Rights Reference Handbook* (3<sup>rd</sup> Revised, University for Peace Press 2004).

<sup>87</sup> Lee Andrew Bygrave, 'The Place of Privacy in Data Protection' (2001) 24 (1) *University of Wales Law Journal* 277, 283; Lee Andrew Bygrave, *Data Privacy—An International Perspective* (Oxford University 2014); Magdalena Sepulveda et al, 'International Supervisory mechanisms for Human Rights; in *Human Rights Reference Handbook* (3<sup>rd</sup> Revised, University for Peace Press, 2004); Graham Greenleaf, 'Independence of Data Privacy Authorities (Part 1): International Standards' (2012) 3 (13) *Computer Law & Security Review* 28.

<sup>88</sup> Adam Warren, James Dearnly and Charles Oppenheim, 'Sources on Data Protection and Human Rights' (2002) 2 *Journal of information, Law and Technology* <<http://elj.warwick.ac.uk/01-2/warren.html>> accessed 28 April 2020; Adrienn Lukacs, 'What Is Privacy? The History and Definition of Privacy' (2017) 25 (1) *Computer Law and Security Review* 84,87; David Banisar and Simon Davies, 'Global Internet Liability Campaign, Report on Privacy and Human rights: An International Survey of Privacy Laws and Practice' (Privacy International, no date supplied) <<http://gildc.org/privacy/survey/intro.html#defining>> accessed 21 March 2020; Nils Melezer, *Human Rights Implications of the usage of Drones and Unmanned Robots in Warfare* (European Union 2013) <<https://doi.org/10.2861/213>>.

<sup>89</sup>Graham Greenleaf, 'Independence of Data Privacy Authorities (Part 1): International Standards' (2012) 3 (13) *Computer Law & Security Review* 28; Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis (2022) *Computer & Security Law Review* <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022

<sup>90</sup> Article 8 of the Charter of Fundamental Rights of the European Union (signed 12 December 2007, took effect 1 December 2009) [2012/C 326/02] (Lisbon Treaty).

The recognition of information privacy as a distinct human right heightened the debate on the affiliation between the right to privacy and information privacy. Consequently, discourse relating to the interchange and nexus between privacy and information privacy protection emerged.<sup>91</sup>

The affiliation between privacy and information privacy protection remains an ongoing debate. Scholars remain divided on this, with some postulating that information privacy protection is an element of the right to privacy and others arguing that, since not all personal information is necessarily private, information privacy protection is an independent human right and not an element of the right to privacy, *per se*.<sup>92</sup>

As a result of this debate, several authors outrightly fail to draw a distinction between privacy and information privacy protection and employ these terms as substitutes.<sup>93</sup>

The international human rights focus and international prominence of information privacy protection is presently spearheaded by the CoE. The CoE initially limited information privacy protection to natural persons and automated processing.<sup>94</sup> The OECD<sup>95</sup> and the UN expanded the scope of information privacy protection to

---

<sup>91</sup>Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163; Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? Reconstructing a not so New Right' (2013) 3 International Data Privacy Law 88; Orla Lynskey, 'Deconstructing Data Protection: the Added Value of a Right to a Data in the EU Legal order' [2014] International and Comparative Law Quarterly 569-597; Lee Andrew Bygrave, 'The place of Privacy in Data Protection Law' [2001] University of New South Wales Law Journal 277-283; Maria Tzanou, *The Fundamental Right to Data Protection* (Hart Publishing 2017); J Neethling, 'The concept of Privacy in South Africa' (2005) 122 (1) The South African Law Journal 18, 22.

<sup>92</sup> F Bélanger and R E Crossler, 'Privacy in the Digital Age: A Review of Information Privacy Research in Information System' (2011) 35 (4) MIS Quarterly 1017. <<https://doi.org/10.2307/41409971>> accessed 30 June 2021, Gloria González Fuster, *The Emergence of Data Protection Law as a Fundamental Human Right of the EU* (Springer Heidelberg 2014).

<sup>93</sup> Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis (2022) Computer & Security Law Review <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022.

<sup>94</sup> The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) opened for signature on 28 January 1981; OECD, Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD: date not indicated)<<https://www.oecd.org/sti/economy/oecdguidelinesontheProtectionofPrivacyandTransborderflowsofpersonaldata.htm#recommendation>>accessed May 2021. (indicates work dates back to 19680).

<sup>95</sup> Magdalena Sepulveda et al, 'International Supervisory Mechanisms for Human Rights'; in *Human Rights Reference Handbook* (3rd Revised, University for Peace Press 2004); Graham Greenleaf,

international agencies, juristic persons, and manual processing.<sup>96</sup> The UN introduced additional considerations, such as the establishment of data protection authorities (DPA), procedural rules and enforcement mechanisms.<sup>97</sup>

Regional consciousness regarding information privacy protection is also underscored by the African Union (AU) and the Southern African Development Community (SADC).<sup>98</sup> Regrettably, the regional legal frameworks have not received the required political support for ratification, to operationalise the regional information privacy legal frameworks. Perhaps because these instruments, in the words of Greenleaf and Cottier, does not reflect 'the philosophical conception of privacy in the African context'.<sup>99</sup>

Notwithstanding, the leisurely progress of information privacy in the region and sub-region, the visceral joinder of technology and information privacy is firmly embedded and growing in prominence.

Information Privacy protection is annually internationally celebrated on 28 January, which is designated Data Protection Day (or Privacy Day outside Europe).<sup>100</sup>

---

'Independence of Data Privacy Authorities (Part 1): International Standards' (2012) 3 (13) *Computer Law & Security Review* 28.

<sup>96</sup> Magdalena Sepulveda et al, 'International Supervisory Mechanisms for Human Rights; in *Human Rights Reference Handbook* (3<sup>rd</sup> Revised, University for Peace Press 2004).

<sup>97</sup> Guidelines for the Regulation of Computerized Personal Data files adopted by the UN General Assembly Resolution 45/95 of 14 December 1990; Paul De Hert and Evangelos Papakonstantiniou, 'Three scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organisation, preferably a UN Agency?' (2013) 9 (2) *Journal of Law and Policy for the Information Society* 276, 324; Monika Zalnieruite, 'An International Constitutional moment for Data Privacy in the times of Mass Surveillance' [2015] *Journal of Law and Information Technology* 1, 35.

<sup>98</sup> Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) *International Data Privacy Law Journal* 163; Graham Greenleaf and Marie Georges, 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' [2014] *Privacy Laws & International Business Journal Report* 18-21 < <https://ssrn.com/abstract=2546652>> accessed 5 October 2021.

<sup>99</sup> Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis (2022) *Computer & Security Law Review* 3 <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022.

<sup>100</sup> On 26 April 2006 the CoE decided to launch a Data Protection Day to be celebrated each year on 28 January, the date on which the Council of Europe's data protection convention, known as Convention 108, was opened for signature; Nashilongo Gervasius, 'Data Protection and Privacy in the Absence of Law: A Namibian Exploration During Covid-19' *The Namibian* (Windhoek, 28 January 28, 2021) <<https://openinternet.global/news/data-protection-and-privacy-absence-law-namibian-exploration-during-covid-19>> (accessed 28 January, 2021).

Arguments are advanced that information privacy protection has become a rule of customary international law.<sup>101</sup>

### **3. Foundational Legal Framework on Information Privacy**

#### **3.1. International Legal Framework**

The right to privacy is widely hailed as a first generational fundamental human right.<sup>102</sup> Within the human rights sphere, privacy is principally avowed as an embargo on the unlawful intrusion of a person's 'private and family life, home and correspondences'.<sup>103</sup>

Article 12 of the UDHR<sup>104</sup> is reported to be the first instrument to recognise the right to privacy. Informed by the UDHR, Article 17 of the 1996 International Convention on Civil and Political Rights (ICCPR) obligated states to protect the right to privacy.<sup>105</sup> The UN also adopted two resolutions in 2014 and 2016 respectively on the right to privacy in the information age.<sup>106</sup>

As members of the Commonwealth Namibia and the RSA are bound by the Commonwealth Cyber Declaration, which commits States to bolster their information privacy and security legal frameworks 'to promote public trust in the internet, confidence for trade and commerce, and the free flow of data'.<sup>107</sup>

---

<sup>101</sup> Customary International Law consists of rules that come from a general practice accepted as a legal obligation without an express Treaty commitment.

<sup>102</sup> Caroline B Ncube, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems' (2004) (2) 4 *Journal of Information, Law and Technology* 1, 24, 27; Yayanta Gosh, 'Data Protection: A Different Dimension under Human Rights and Intellectual Property Law' (2015) (1) *International Journal of Justice and Legal Studies* 39.

<sup>103</sup> Jonathan Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009)13 (1) *Electronic Journal of Comparative Law* 1.

<sup>104</sup> United Nations General Assembly Resolution 217 A (III) of 10 December 1948; Universal Declaration of Human Rights (1948 UDHR).

<sup>105</sup> See General Comment issued by the Human Rights Committee on 23rd March 1988 (U.N. Doc. A/43/40) 180–183, paragraphs 7 & 10.

<sup>106</sup> African Human Rights Commission Resolution on the Right to Freedom of Information and Expression on the Internet in Africa (ACHPR/Res.362(LIX)2016).

<sup>107</sup> Commonwealth Cyber Declaration (adopted on 2018) Available at < <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/inline/Commonwealth-Cyber-Declaration.pdf> > accessed 1 Jan 2022.

Applying the reductionism theory on privacy,<sup>108</sup> the right to privacy is not enumerated in the Banjul Charter.<sup>109</sup> Despite this, it is argued<sup>110</sup> that the right to privacy is justiciable within the African Union (AU) system, by invoking it under the umbrella of other human rights or under the African human rights court's jurisdiction to adjudicate human rights recognised under other international rights instruments i.e. Article 17 of ICCPR.<sup>111</sup> I have however not sourced any jurisprudence from the African Human Rights Court and or the African Human Rights Commission dealing with information privacy.

Even though there is no explicit recognition of privacy under the *Banjul Charter*. The AU's commitment to information privacy is evident from its unsuccessful extension of information privacy protection under the *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa* and the adoption of the African Convention on Cyber Security and Personal Data Protection on June 27, 2014 (Malabo Convention).<sup>112</sup>

The Malabo Convention aims to penalise information privacy violations and boost the free flow of information. Article 13 of the Malabo Convention sets out baseline

---

<sup>108</sup> The Reductionism theory postulates that, privacy is a right reducible to other concepts and rights, such as the right to life and liberty. Consequently, it argues that privacy is a superfluous right on its own. See discussion of academic theories on privacy in Chapter 2 page 42 of this Thesis.

<sup>109</sup> Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter") adopted on 27 June 1981 (CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) <Available at: <https://www.refworld.org/docid/3ae6b3630.html>> accessed 1Jan 2022 [Namibia ratified the Charter on July 15,1992 and RSA on July 09,1996].

<sup>110</sup> Alex Bonafatius Makulilo, 'The long arm of GDPR in Africa: reflection on Data Privacy Law Reform and Practice in Mauritius' [2021] *International Journal of Human Rights*,117-146; See also Lee Andrew Bygrave, 'Data Protection: Pursuant to the right to Privacy in Human Rights Treaties' [1998] *International Journal of Law and Technology* 247.

<sup>111</sup> United Nations, 'The Right to Privacy in Namibia: Stakeholder Report Universal Periodic Review 24th Session' (Privacy International, June 2015) Available at< [https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR\\_PI\\_submission\\_FINAL.pdf](https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf)In 2006> accessed December 2020).

<sup>112</sup> Convention is not operational, at present. Namibia ratified the Convention of 01/02/2019 and the status report indicates that RSA has not yet signed the Convention. See Malabo Convention status list Available at < <https://au.int/sites/default/files/treaties/29560-slafrican%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf>> accessed July 2021.



information privacy protection principles for lawful processing.<sup>113</sup> The Convention further forbids profiling or automated decision-making and also regulates data matching.<sup>114</sup>

In addition to the above, information privacy protection is also promoted through the African Union Commission and Internet Society's 2018 Personal Data Protection Guidelines for Africa and the 2016 *African Declaration on Internet Rights and Freedoms*.<sup>115</sup>

Within SADC guidance on information privacy is extended through the 2013 SADC Model Law on Data Protection.<sup>116</sup> Parts IV, VI and VII of the Model Law sets out the basic information privacy principles.

### 3.2. National Legal Framework

The RSA and Namibian Constitutions extend protection to the privacy of all persons under section 14 and article 13, respectively. Section 8(1) and (2) of the RSA Constitution and article 5 of the Namibian Constitution enjoin the respective States, as well as all-natural and juristic persons, to protect and uphold the fundamental human rights and freedoms guaranteed under these Constitutions, which includes the right to privacy.<sup>117</sup>

The Namibian and the RSA Constitutions also stipulate that this right can only be restricted if legislation to that effect is promulgated, and the restrictions imposed are

---

<sup>113</sup>Consent and legitimacy; lawfulness and fairness; purpose, relevance, and storage; accuracy; transparency; confidentiality; and security; See also Graham Greenleaf and Marie Georges, 'African Regional Privacy Instruments: their effects on Harmonization' (2014) 132 *Privacy Laws and Business International Report* 19-21; V Mabika, 'Privacy and Personal Data Protection Guidelines for Africa' (ITU, 2018) <[https://www.itu.int/en/ITUUD/CapacityBuilding/Documents/IG\\_workshop\\_August\\_2018\\_Presentations/Session%207\\_Verengai%20Mabika.pdf](https://www.itu.int/en/ITUUD/CapacityBuilding/Documents/IG_workshop_August_2018_Presentations/Session%207_Verengai%20Mabika.pdf)> accessed 30 September 2020.

<sup>114</sup> Data matching (also referred to as interconnection of files) may only take place after authorisation by the Data Protection Authority, and should assist in achieving Legal or Statutory objectives which are of legitimate interest to data controllers.

<sup>115</sup> Majam Koliwe, 'African Digital Rights Networks to Collaborate on a Regional Strategy' (APC, 27 May 2021) <<https://www.apc.org/en/tags/african-declaration-internet-rights-and-freedoms>> accessed May 2021.

<sup>116</sup> Southern African Development Community (SADC) Data Protection Model Law <[www.itu.int/en/ITUUD/Projects/ITUECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc\\_model\\_law\\_data\\_protection.pdf](https://www.itu.int/en/ITUUD/Projects/ITUECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf)> accessed 27 January 2021.

<sup>117</sup> Juristic persons also enjoy fundamental rights and freedoms to the extent that it is feasible by virtue of Section 8(4) of the RSA Constitution. The definition of personal information under the Personal Information Act 4 of 2013 (POPIA) also covers personal data of juristic persons; Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53 (3) *Comparative and International Law Journal of Southern Africa* 8-9 <<https://doi.org/10.25159/2522-3062/7985>> accessed 16 November 2022.

reasonable and justifiable to foster democracy, public interest and national security, provided that the essential content of the human rights are not negated. In *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*<sup>118</sup> the court held that an assessment of the appropriateness of the limitations on human rights under chapter 3 involves the consideration of the nature essence and significance of the right<sup>119</sup>, the scope of limitation imposed, in light of the objective and consequences of the limitation and the feasibility of resorting to less restrictive measures, instead.

Even though historically based on the understanding that juristic persons are incapable of possessing personality rights, information privacy was limited to natural persons under common law.<sup>120</sup> the Constitutional Court (CC) of the RSA observed in *Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*<sup>121</sup> that:

[T]he right to privacy is applicable, where appropriate, to a juristic person [...] Their privacy rights, therefore, can never be as intense as those of human beings. However, this does not mean that juristic persons are not protected under the right to privacy.

Although acknowledged as a right under various international human rights instruments, there is academic consensus that it is extremely challenging to offer a universally acceptable description of privacy. Solove<sup>122</sup>, offers a synopsis of the views of selected researchers, in the following words: -

[T]ime and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy. Arthur Miller has declared that privacy is difficult to define because it is exasperatingly vague and evanescent. According to Julie Inness, the legal and philosophical discourse of privacy is in a state of chaos. Alan Westin has stated that few values so fundamental to society as privacy have been left so undefined in social theory. William Beaney has noted that even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right. Privacy has a protean capacity to be all things to all lawyers, Tom Gerety has observed. According to Robert Post, privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all. Several theorists have surveyed the interests that the law protects under the rubric of privacy and have concluded that they are distinct.

---

<sup>118</sup> [1998] ZACC 15; 1999 (1) SA 6 (CC).

<sup>119</sup> For purposes of fostering, an open and democratic society based on human dignity, equality and freedom.

<sup>120</sup> J Neethling and J M Potgieter, *Law of Delict* (8th ed, LexisNexis 2021); See also I Currie and J De Waal, *The Bill of Rights Handbook* (6th ed, Juta 2013); J M Burchell, *Personality Rights and Freedom of Expression: The Modern Actio Injuria rum* (Juta 1998).

<sup>121</sup> 2001 (1) SA 545 (CC) 557D-G.

<sup>122</sup> Daniel Johnathan Solove and Paul M Schwartz, *Information Privacy Law* (16th ed, Kluwer, 2018); Doreen Fariji Mwamlangala, 'Privacy and Security in the Cloud: Tanzania and South Africa in Comparative Perspective' (PhD Thesis, The Open University of Tanzania 2020).

True to Solove's observation, the South African courts also grapple with exacting the parameters of privacy. In *NM v Smith (Freedom of Expression Institute as Amicus Curiae)*<sup>123</sup> court conceptualised privacy as the

[R]ight of a person to live his or her life as he or she pleases and 'private facts' as those matters the disclosure of which will cause mental distress and injury to anyone possessed of ordinary feelings and intelligence in the same circumstances and in respect of which there is a will to keep them private.

Correspondingly, in *Black Sash Trust v Minister of Social Development and Others*,<sup>124</sup> which involved the unauthorised supply of the personal information of social grant beneficiaries to insurance companies, by a services provider contracted to distribute the grants. The court opined that the conduct of the service provider offended the privacy of the social grant beneficiaries. This judgment is a clear recognition and acceptance that privacy incorporates the ability to control who has access to one's personal information and how it is used.

This understanding was also stressed in the Johannesburg High Court, *Discovery Ltd and Others v Liberty Group Ltd judgement*,<sup>125</sup> in which the court dismissed a trademark infringement and anti-competitive behaviour claim, on the understanding that the personal information which formed the basis of the claim was owned by the customers and was made available to the competitor by the customers themselves and was not part of the proprietary information of the claimant.<sup>126</sup> The court held that, that upholding the claim would amount to restricting the customers from exercising the choice to use their personal information.

In defiance of the non-interface theory<sup>127</sup>, the RSA and Namibian Constitutions subject the right to privacy to limitations. To this end, articles 21(2) and 22 of the Namibian Constitution and section 14 (2) of the RSA Constitution stipulates that the right to privacy may be circumscribed, if legislation sanctioning such a restriction are promulgated and

---

<sup>123</sup> 2007 (5) SA 250 (CC) at paragraph 68.

<sup>124</sup> [2017] ZACC 8.

<sup>125</sup> (21362/2019) [2020] ZAGPJHC 67; [2020] 2 All SA 819 (GJ).

<sup>126</sup> See also Londiwe Buthelezi, 'How the Discovery vs. Liberty judgement changed the game' (News24, 20 Apr 2020) <<https://www.news24.com/fin24/companies/financial-services/analysis-how-the-discovery-vs-liberty-judgement-changed-the-game-20200417>> accessed 10 November 2022; Andrew Schepers and Novazi Zinhle, 'It's personal: Discovery vs Liberty on the use of personal information' (TABACK, 28 April 2020) < <https://www.tabacks.com/news-and-insights/2020/4/its-personal-discovery-vs-liberty-on-the-use-of-personal-information>> accessed 10 October 2022.

<sup>127</sup> The non-interference theory considers privacy as an absolute right and advocates that a person's privacy should not be interfered with by anyone in any way.

the restrictions are reasonable and justifiable with reference to recognised public interest grounds, provided that the core minimum content<sup>128</sup> of the right is not encroached on.<sup>129</sup>

The restricted nature of the right to privacy was confirmed in the *Tshabalala-Msimang v Makhanya*<sup>130</sup> judgment wherein it was acknowledged that the right to privacy may be limited by the freedom of expression. The court found that private information contained in the health records is worth protecting [...] and in this instance took precedence over the freedom of expression.

Applying the same principle, the court found in *De Reuck v Director of Public Prosecutions*, that although possession and consumption of child pornography often take place in the 'inner sanctum of the home', the law prohibiting possession of erotic materials limits the right to privacy. The court was of the view that the search of the accused home satisfied the requirements of the limitation clause in the RSA Constitution.<sup>131</sup>

This principle was also applied in the Namibian case of *S v Lameck*<sup>132</sup> wherein the court ruled that the bank records of an accused in a corruption trial were admissible, since the right to privacy was not unqualified and the information was obtained in terms of the Anti-Corruption Act, which constituted a justifiable limitation of the right to privacy.<sup>133</sup>

It is a further requirement that the limitation-imposed subject to section 14 (2) of the RSA Constitution, must be proportional and not arbitrary. Applying this principle, the CC ruled in *Mistry v Interim Medical and Dental Council of South Africa*,<sup>134</sup> that section 28(1) of the Medicines and Related Substances Control Act was overbroad and failed the proportionality test, in so far as it gave officials unchecked powers to conduct a search

---

<sup>128</sup>Minimum core content is described as the essential minimum guarantees for the protection of a human right. For example, the core content of the right to housing is that a person cannot be divested of title in property without due process of law and just compensation.

<sup>129</sup> Article 21(2) and 22 of the Namibian Constitution and Section 14 (2) of the RSA Constitution.

<sup>130</sup> (2008) (6) SA 102 (W).

<sup>131</sup> 2004 (1) SA 406 (CC) para 90.

<sup>132</sup> [2018] NAHCMD 214.

<sup>133</sup> Act 8 of 2003.

<sup>134</sup> 1998 [4] SA 1127.

and to seize items on the premises of suspected violators of the Act and thus violated the right to privacy.<sup>135</sup>

The court also underscored the requirement on proportionality of limitations on the right to privacy *Johncom Media Investments Limited v M and Others*<sup>136</sup> declared the provisions of section 12 of the Divorce Act unconstitutional on the ground that it was overbroad and disproportionate because it levied an unfettered prohibition from publishing information relating to divorce proceedings.<sup>137</sup> The court held that even though it was aimed at protecting the dignity and privacy of families going through divorce, it fell outside the recognised grounds for limiting a constitutional right.

All the aforementioned international, regional and national instruments are self-contained information privacy instruments.<sup>138</sup> The State(s), all-natural and juristic persons are thus obligated to respect, protect and promote information privacy from arbitrary or unlawful interference and to develop laws, policies and regulations to protect and promote the right to information privacy.

In order to domesticate the international, continental and sub-continental commitments discussed above and to give expression to the constitutional right to privacy. The RSA promulgated the Protection of Personal Information Act<sup>139</sup> (POPIA).<sup>140</sup>

Similarly, Namibia is also committed to developing a comprehensive national information privacy law. It is anticipated that the Data Protection Bill will be enacted in 2023.<sup>141</sup>

#### **4. Parameters and Significance of Privacy**

---

<sup>135</sup> Act 101 of 1965.

<sup>136</sup> CCT 08/08 [2009] ZACC 5; 2009 (4) SA 7 (CC).

<sup>137</sup> Act 70 of 1979.

<sup>138</sup> In *Visagie v The Government of the Republic of Namibia and Others* [2018] NASC 411, the High Court of Namibia ruled that Article 25 (4) of the Namibian Constitution gives the Court to award monetary compensation in respect of any damage suffered by an aggrieved person in consequence of an unlawful denial or violation of their fundamental rights or freedoms, where it is appropriate in the circumstances of a particular case.

<sup>139</sup> Act 4 of 2013. This Act is discussed in Chapter 3 hereof.

<sup>140</sup> The act was signed into law in 2013 and partially enforced in 2014, allowing for the establishment of the Information Regulator in 2016. However, it was not until 2020 that the POPIA came into effect. (Proclamation No. R. 21 of 2020 in Gazette No. 11136, Vol. 660 No 43461 dated 22 June 2020); See also Hunton Andrews Kurts, 'Privacy and Cybersecurity: South Africa's Protection and Personal Information Act, 2013 goes into effect July 1'(The National Review: 29 June 2020) <<https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1>> accessed 26 Jan 2021.

<sup>141</sup> See Discussion on the Namibian Data Protection Bill in Chapter two hereof.

## 4.1. Significance and Delineation of Privacy

The significance of privacy is well articulated by Alan Grayling, an English liberal, in his book<sup>142</sup> *Liberty in the Age of Terror: A Defence of Civil Liberties and Enlightenment Values*, wherein he makes the following observations:

No human rights convention is complete without an article that defends privacy, for the excellent reason that privacy is an indispensable adjunct of the minimum that individuals require for a chance to build good lives. One aspect of its importance is that it gives people a measure of control over the front they offer to others, and the amount of information that others have about them, concerning matters that are personal, intimate, eccentric or constitutive of the individual's inner life [...]

But the foremost reason for privacy is that it is crucial for personal autonomy and psychological well-being. Even lovers require a degree of privacy from each other, for the lack of a reserve selfhood is almost the same as not having a self at all.

Due to its multi-layered nature, this academic enquiry has not yielded an all-encompassing conceptualisation of the right to privacy. Correspondingly, there is scholarly accord that owing to its intrinsic elusiveness, political and socio-economic relativity, it is difficult to describe privacy with mathematical precision.<sup>143</sup>

Thirty-one years ago, the *Calcutt Committee* concluded that privacy is most difficult to explain and circumscribe.<sup>144</sup> In the same vein Gogarty, Brendan, Meredith and Hagger observe that 'privacy is an exoteric concept without precise objectively discernable boundaries'.<sup>145</sup> The South African Constitutional Court also came to the same conclusion and stated that privacy is 'amorphous and elusive' in *Bernstein v Bester*.<sup>146</sup>

---

<sup>142</sup> A C Grayling, *Liberty in the Age of Terror. A Defence of Civil Liberties and Enlightenment Values* (Bloomsbury London 2009) 23.

<sup>143</sup> Global Partners Digital, *Travel Guide to the Digital World: Data Protection for Human Rights Defenders* (Global Partners Digital, 2018) < <https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf> > accessed 1 Jan 2022.

<sup>144</sup> David Calcutt (Contributor), *Report of the Great Britain Committee on Privacy and Related Matters (Calcutt Report)* (London: H.M.S.O., 1990).

<sup>145</sup> Gogarty Brendan and Meredith Hagger, 'The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' (2008) 19 *Journal of Law, Information and Science* 73; See also F Dima, 'Drone Technology and Human Rights' (Bachelors Thesis, University of Twente 2017); Anneliese Roos, 'The Law of Data Protection: a Comparative Theoretical Study' (LLD Thesis, University of South Africa 2003).

<sup>146</sup> 1954(3) SA 244 (C).

Notwithstanding the caution extended by scholars that it is not judicious to define the right to privacy.<sup>147</sup> I found the following account of privacy expounded in *Smuts and Another v Botha and Another* a fair enumeration of its essential elements;<sup>148</sup>

Privacy enables individuals to create barriers and boundaries to protect themselves from unwarranted interference in their lives. It helps to establish boundaries to limit who has access to their space, possessions, as well as their commercial and other information. [...] The right to privacy is not sacrosanct, it must be balanced with the rights of other citizens.

## 4.2. Academic Theories on Information Privacy

Notwithstanding the famine of a uniform definition of privacy, several theories are generally expounded to conceptualise information privacy.<sup>149</sup> The academic opinion with regard to information privacy to date can be summarised in six prominent theories; namely:<sup>150</sup>

**Non-interference Theory**<sup>151</sup>, the non-interference theory considers privacy as an absolute right and advocates that a person's privacy should not be interfered with by anyone in any way;

**Information Control Theory**,<sup>152</sup> this theory views information privacy with reference to the degree of control a person has control over his personal information. For this reason,

---

<sup>147</sup> Hyman Gross, 'The Concept of Privacy' [1967] *New York University Law Review* 34-53,36; Richard R Parker, 'Definition of Privacy' (1974) 27(2) *Rutgers Law Review* 275, 276-279; Ruth Gavison, 'Privacy and the limits of the Law' [1980] *Yale Law Journal* 421-471; Lee Andrew Bygrave, 'The place of Privacy in Data Protection Law' (2001) *University of New South Wales Law Journal* 277-283, 279; Lee Andrew Bygrave, *Data Protection Law* (Kluwer 2002),46; Daniel Jonathan De Solove, 'Conceptualising Privacy' (2002) 90 *California Law Review* 1087, 1110; W Gregory Voss, 'Obstacles to Transatlantic Harmonization of Data Privacy Law in Context' (2019) 2 *University of Illinois Journal of Law, Technology & Policy* 405, 463; See also Kristine L. Florczak, 'Privacy: an Elusive Concept' (2021) 34 (2) *SAGE Journals: Nursing Science Quarterly* 113.

<sup>148</sup>(887/2020) [2022] ZASCA 3 (10 January 2022) paragraph 10.

<sup>149</sup> Róisín Áine Costello, 'The Impacts of AdTech on Privacy Rights and the Rule of Law': In Leenes R and Martin A (eds.), *Technology and Regulation* (Open Press Tilburg University 2021).

<sup>150</sup> Robert C Post, 'Three Concepts of Privacy' (2001) 89 *Georgetown Law Journal* 2087; Daniel Johnathan Solove, *Understanding Privacy* (Harvard University Press 2008); Daniel Solove and Paul M Schwartz, *Information Privacy Law* (16th ed, Kluwer 2018).

<sup>151</sup> Christian Fuchs, 'Towards an Alternative Concept of Privacy' (2011) 9 (4) *Journal of Information, Communication and Ethics in Society* 220,237.

<sup>152</sup> Luciano Floridi, 'Four Challenges for a Theory of Informational Privacy' (2006) 8 (3) *Ethics and Information Technology Journal* 109,115-119.

Phillip Nyoni and Mthulisi Velempin<sup>153</sup>, echoing Stahl<sup>154</sup> describe information privacy as 'information self-determination';

**Restricted Access Theory**,<sup>155</sup> this theory emphasise the importance of having situations, zones or contexts of privacy to restrict or limit outsiders from interfering with. It presupposes that a person's right to privacy is only protected when there is limited or restricted access to their person, property and or information;

**Intimacy Theory**,<sup>156</sup> this theory classifies personal information as sensitive or intimate. Accordingly, it argues that the right to privacy is infringed only if sensitive or intimate information is divulged;

**Reductionism Theory**,<sup>157</sup> this theory stresses that privacy is a right reducible to other concepts, such as the right to life and liberty. Consequently, it argues that privacy is a superfluous right on its own;

**Pragmatism Theory**,<sup>158</sup> this theory was developed to address the shortcomings of some of the traditional theories. It posits that privacy must be to explored contextually, by studying particular practices to determine whether something is private or not, instead of following a rigid predetermination.

It appears from the recent decision in *Discovery Ltd and Others v Liberty Group Ltd*<sup>159</sup> that the RSA courts lean towards the information control theory. The court dismissed a claim for trademark infringements arguing that the personal information which was alleged to have given rise to the infringement, belonged to the customers who were

---

<sup>153</sup> Phillip Nyoni and Mthulisi Velempin, 'Data Protection laws and Privacy on Facebook' [2005] South African Journal of Information Management 10,11.

<sup>154</sup> B C Stahl, *The impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace* (IBI Global 2000).

<sup>155</sup> Christian Fuchs, 'Towards an Alternative Concept of Privacy' (2011) 9 (4) Journal of Information, Communication and Ethics in Society 220,237.

<sup>156</sup> Robert S Gerstein, 'Intimacy and Privacy': In Ferdinand David Schoeman (eds), *Philosophical Dimensions of Privacy* (Cambridge University Press 1984) 265, 271; Julie C Inness, *Privacy, Intimacy and Isolation* (Oxford University, 1992).

<sup>157</sup> Amy L Peikoff, 'Beyond Reductionism: Reconsidering the Right to Privacy' (2008) 3 (1) New York University Journal of Law and Liberty < <http://www.migration.nyulaw.me/default/files>> accessed 15 April 2021.

<sup>158</sup> Citron, Danielle and Leslie M Henry, 'Visionary Pragmatism and the Value of Privacy In the Twenty-One Century' (2010) 108 Michigan Law Review 1107-26; Miriam Sweeney, 'Book Review on Understanding Privacy by Daniel J Solove' (2012) 28 (5) International Journal of the Information Society 1.

<sup>159</sup>(21362/2019) [2020] ZAGPJHC 67; [2020] 2 All SA 819 (GJ); 2020 (4) SA 160 (GJ). (15 April 2020), paragraph 68.4.



entitled to disclose it. This theory was also followed in January 2022 by the supreme court of appeal judgment of *Smuts and Another v Botha and Another*.<sup>160</sup>

This paper thus endorses the Information Control and Restricted Access Theories and to a lesser extent the Pragmatism Theory.

## 5. Information privacy protection as an Enabler of the right to Privacy

### 5.1. Parameters and Purpose of Information Privacy Protection

Information is designated, as the new oil of the internet and the new currency of the digital world.<sup>161</sup> Information generally refers to any kind of online or offline data that is intelligible to humans.<sup>162</sup>

Personal information is at the nerve centre of all discussions on information privacy. Personal information on the other hand refers to information that reveals or can be used to reveal who a person is, their relationships, health status, family background, biometric features, race, political affiliation, financial details, sexual preferences, beliefs etcetera and information from which the above can reasonably be deduced.<sup>163</sup> The universal yardstick is usually the degree to which information can be employed to directly or

---

<sup>160</sup>(887/2020) [2022] ZASCA 3 (10 January 2022) at paragraph 23; the court was of the opinion that Mr Botha had debilitated his right to privacy by placing his information within the public domain; See also Arinda Truter, 'Bool Smuts v Herman Botha -Right to Privacy v Freedom of Expression' (Dingley Marshall Lewin, February 23rd, 2022) < <https://www.dmlaw.co.za/bool-smuts-v-herman-botha-right-to-privacy-v-freedom-of-expression/>> accessed 20 May 2022 ; Nicole Dembitzer, 'Social media: when can the right to freedom of expression be limited by the right to privacy? Quarter 2 2022' (Withoutprejudice, Quarter 2 2022) < <https://www.withoutprejudice.co.za/free/article/7524/view#:~:text=In%20the%20recent%20case%20of,to%20privacy%20and%20can%20be>> accessed 20 May 2022..

<sup>161</sup> Global Partners Digital, *Travel Guide to the Digital World: Data Protection for Human Rights Defenders* (Global Partners Digital 2018)< <https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf>> accessed 1 Jan 2022; Kuvana Meglena, 'Personal data: The Emergence of a New Asset Class'(World Economic Forum 17 Jan 2011)<[https://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf)> accessed 21 December 2021.

<sup>162</sup> Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (1st Edition, Oxford University Press 2014).

<sup>163</sup> The conceptualisation of personal data has been expanded to encompass online and device identifiers (like IP addresses, cookies, or device IDs), location data, usernames, and pseudonymous data.

<sup>163</sup> Gregory M Huffman, 'Video-streaming Records and the Video Privacy Protection Act: Broadening the Scope of Personally Identifiable Information to include Unique Device Identifiers Disclosed with Video Titles' (2016) 91 Chicago Kent Law Review 737; Ciara Staunton et al, 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) (4) South African Medical Journal 232. Global Partners Digital, *Travel Guide to the Digital World: Data Protection for Human Rights Defenders* (Global Partners Digital 2018)< <https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf>> accessed 1 Jan 2022.

indirectly identify a living (natural) person.<sup>164</sup> Some jurisdictions only extend information privacy protection to living natural persons,<sup>165</sup> whilst others also protect juristic persons and even deceased persons.<sup>166</sup>

Jurisprudence<sup>167</sup> locates information privacy protection at the mid-point of the right to privacy.<sup>168</sup> Information privacy protection advocates for the observance of measures to safeguard 'personal information against unauthorised access or disclosure, destruction, modification and unauthorised use of information, as a means to uphold the right to privacy and to correct the imbalance of power between data subjects and those processing personal data.'<sup>169</sup>

This view is confirmed by Roos, who posits that information privacy protection laws<sup>170</sup> are a safeguard of the right to constitutional right to privacy.

---

<sup>164</sup> M Albers, Ronald Leenes and Hert De Paul, 'Realising the Complexity of Data Protection': In S Gurtwith, et al (eds), *Reloading data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 221; Dara Hallinan et al, *Data Protection and Privacy* (Volume 12 Hart, Publishing 2021) 51.

<sup>165</sup> See Article 4(1) and recital 27 of the GDPR makes it clear that the GDPR does not apply to juristic persons. Available at < <https://gdpr-text.com/read/article-4/>> accessed 16 October 2022.

<sup>166</sup> Juristic persons also enjoy fundamental rights and freedoms to the extent that it is feasible by virtue of Section 8(4) of the RSA Constitution. The definition of personal information under the Personal Information Act 4 of 2013 (POPIA) also covers personal data of juristic persons. Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53 (3) *Comparative and International Law Journal of Southern Africa* 8-9< <https://doi.org/10.25159/2522-3062/7985>> accessed 16 November 2022.

<sup>167</sup> Jonathan Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009)13 (1) *Electronic Journal of Comparative Law* 1; Alex B. Makulilo, 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius' (2021) *The International Journal of Human Rights* 117,146; M Alber, R Leenes and De Paul H, 'Realising the Complexity of Data Serge Gutwirth (eds), *European Data Protection: Coming of Age* (Springer Heidelberg 2013); Racel Finn, David Wright and Micheal Friedewald, 'Seven Types of Privacy': in Serge Gutwirths et al (eds), *European Data Protection: Coming of Age* ( Springer Heidelberg 2013).

<sup>168</sup> Kuvenga Meglena, 'Personal data: The Emergence of a New Asset Class' ( Speech at World Economic Forum 17 Jan 2011) <[https://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf).> accessed 21 December 2021; Chris Jay Hoofnagle, Bart Van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28 (1) *Information & Communications Technology Law Journal* < <https://doi.org/10.1080/13600834.2019.1573501>> accessed 16 October 2022.

<sup>169</sup> Daniel J Solove, 'A Taxonomy of Privacy' (2006)154 (3) *University of Pennsylvania Law Review* 477; Daniel J Solove, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 4 *San Diego Law Review* 745; Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89 (3) *The Yale Law Journal* 421, 471.

<sup>170</sup> Anneliese Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 11 (4) *Potchefstroom Electronic Law Journal* 62; Anneliese Roos, 'Personal Data Protection: explaining the International backdrop and Evaluating the current South African position' [2007] *South African Law Journal* 400; Anneliese Roos, 'Core Principles of Data Protection Law' [2006] *Comparative and Law Journal of South Africa* 102.

## 5.2. Nexus between Privacy and Information Privacy

An extensive degree of literature presents information privacy as an expression of the right to information privacy or as a subset of the right to privacy.<sup>171</sup> My analysis is, however, that although information privacy encapsulates components of the right to privacy, privacy is not absorbed in personal information privacy protection *per se*.

I am of the opinion that privacy more often than not concentrates on the spatial or corporeal, whereas the focus of information is primarily incorporeal.<sup>172</sup> Moreover, unlike privacy, information privacy protection enlists principles that are separate from the traditional principles invoked for the protection of privacy in so far as information privacy demands accountability through the adoption of proactive positive measures.

It is my observation that information privacy protection is *sui generis*,<sup>173</sup> in the sense that whilst it seeks to protect a first-generational human right, it does not impose a negative obligation as is customary in respect of first-generational human rights, but impose a positive obligation that requires states to adopt pro-active measures to protect the right to privacy.

I am further of the opinion that information privacy should be considered as the first of a new generation of human rights. Perhaps since it is a foundational right in what is commonly referred to as the 'fourth industrial revolution (4IR)',<sup>174</sup> information privacy and associated and incidental rights should be designated as fourth-generation human rights.<sup>175</sup>

---

<sup>171</sup> Lee Adrew Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer 2002).

<sup>172</sup> Lee Adrew Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer 2002).

<sup>173</sup> *Sui generis* is a Latin expression that translates to "of its own kind." It refers to anything that is peculiar to itself; of its own kind or class. In legal contexts, *sui generis* denotes an independent legal classification.

<sup>174</sup> The Fourth Industrial Revolution is a way of describing the blurring of boundaries between the physical, digital, and biological worlds. It is a fusion of advances in artificial intelligence (AI), robotics, the Internet of Things (IoT), 3D printing, genetic engineering, quantum computing, and other technologies. It's the collective force behind many products and services that are fast becoming indispensable to modern life.

<sup>175</sup> See Bart Custers, 'New digital rights: imagining additional fundamental rights for the digital era' (2022) 44 *Computer Law & Security Review* 105636, who speculates on the creation of new human rights for the digital age.

To this end, it is safe to conclude that information privacy protection is an essential enabler of the right to information privacy. I, therefore, agree with Bygrave<sup>176</sup> who advance that, privacy and data protection are not synonymous, and must not be used interchangeably.

### 5.3. Regulatory Approaches

Research further informs that, there are four key internationally sanctioned approaches to regulating data protection, namely comprehensive<sup>177</sup> or sectoral,<sup>178</sup> self-regulation and utilizing privacy-enhancing technologies (PETs).<sup>179</sup> Scholars are of the view that privacy is best protected by an amalgamation and parallel application of all these regulatory approaches.

I hold the same sentiments.

### 5.4. Stakeholders

The stakeholders within the information privacy ecosystem are the State<sup>180</sup>, data subjects<sup>181</sup>, private sector,<sup>182</sup> industry regulators and civil rights organisations<sup>183</sup>.

### 5.5. Possible Expansion of Scope: Post-Mortem (Posthumous) Data Protection

Notwithstanding, the fact that common law only protected the privacy of living persons, consideration is being afforded to extend protection to the personal information of deceased persons. Following the inclusion of recital 27 in the GDPR, contemporary

---

<sup>176</sup> Des Butler, 'The Dawn of the Age of the Drones: an Australian Privacy Law Perspective' (2014) 37(2) University of New South Wales Law Journal 434.

<sup>177</sup> This means that the legislation applies to personal data regardless of sector.

<sup>178</sup> This means that the legislation applies to data processed by either the public or private or to particular fields of industries.

<sup>179</sup> Ann Cavoukin, 'Privacy by Design Leadership Methods' and result: In Gutwirths S et al (eds) *European Data Protection: Coming of Age* (Springer Heidelberg 2013); Koliwe Majama, 'Data Protection in Zimbabwe under the African Continental Free Trade Area: Prospects and Challenges' (Master Thesis Africa University 2021) 13.

<sup>180</sup> The State includes Government departments, Regulators, Security and Law Enforcement Agencies, and other Public bodies.

<sup>181</sup> Users Data protection was developed to protect Data Subjects', however they are users not a homogenous constituency.

<sup>182</sup> Invariably the processors, network service providers and accountable institutions who perpetrate information privacy abuses.

<sup>183</sup> Civil society organisations, particularly non- governmental human rights organisations tend to have an interest in regulatory approaches.

literature particularly in the EU is exploring extending information protection post-mortem<sup>184</sup> (posthumous) data protection.<sup>185</sup>

Numerous commodification data theorists<sup>186</sup> justify extending information privacy protection posthumously, amongst others because, technological development gave rise to what is now commonly referred to as 'netizens'<sup>187</sup> which own 'digital assets' and host an array of personal information online with vast economic value to their lawful heirs, which is not summarily terminated upon death (often described as 'e-mortality').<sup>188</sup>

Even though there is a common view that the dead does not have a right to privacy.<sup>189</sup> The increased ability of emerging technologies such as Artificial Intelligence (AI) and hologram to effectively reconstruct the online lives or components of the physical existence of deceased persons, I am of the opinion that protecting information privacy posthumously is worth considering.<sup>190</sup>

Another view supported by this author is that posthumous information privacy protection inevitably protects the information privacy of deceased relatives such as the determination of hereditary diseases, Deoxyribonucleic Acid (DNA) mental health, and biometric data, and thus, deserves consideration for protection.<sup>191</sup>

---

<sup>184</sup> Melissa Gaided, 'Note, Data After Death: An Examination into Heirs' Access to a Decedent's Private Online Account' (2016) 49 Suffolk University. Law Review 281, 296.

<sup>185</sup> Asta Tūbaitė-Stalaušienė, 'Data Protection Post-Mortem' (2018) 4 (2) International Comparative Jurisprudence < See also 'Post-mortem privacy: is it time to prolong privacy after death' (Michalson, no date supplied)<<https://www.michalsons.com/blog/post-mortem-privacy-is-it-time-to-prolong-privacy-after-death/47338>> accessed 16 November 2022.

<sup>186</sup> The theory of Commodification of data advocates for the concept of Data Freedom and commodification of personal data of deceased persons.

<sup>187</sup> N N Gomes de Andrade and Monteleone S, 'Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioural Trends Regarding Privacy and Their Legal Implications': in Serge Gutwirths et al (eds), European Data Protection: Coming of Age (Springer Heidelberg 2013); V Oloni, 'Life after Death: Data Protection Rights of Deceased Persons' (African Academic Work on Internet Policy)< <https://aanoip.org/life-after-death-data-protection-rights-of-deceased-persons/>> accessed 14 February 2020.

<sup>188</sup> Facebook memorializes the profile pages of deceased users. In other words, Facebook will turn a deceased user's Facebook page into an online memorial. Users agree to this policy when they sign up for an account, therefore most of the content a deceased user had previously shared (e.g., photos, posts) will remain visible'.

<sup>189</sup> Kate C. Ashley, 'Data of the Dead: A Proposal for Protecting Posthumous Data Privacy' (2020) 62 William & Mary Law Review 649< <https://scholarship.law.wm.edu/wmlr/vol62/iss2/6>> accessed 16 November 2022.

<sup>190</sup> Daniel Sperling, Posthumous Interest (Cambridge: Cambridge University Press 2008) 304;

<sup>191</sup> Gianclaudio Malgierie, 'RIP: Rest in Privacy or Rest in (Quasi) Property Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions'(SSRN, 22 June 2018) <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3185249](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185249)> accessed 20 May 2020'

Moreover, bearing in mind that the Mental Health Act<sup>192</sup> presumes a person who is brain dead, is legally dead.<sup>193</sup> I support the notion to consider empowering the heirs or authorised representatives of deceased persons to exercise control over personal information following their death.<sup>194</sup>

This ongoing debate of whether or not to extend protection posthumously, gave rise to interventions such as the nomination of legacy friends in respect of individual social media accounts, which enables access to online information post-mortem.<sup>195</sup>

I am of the considered opinion that, the posthumous extension of information privacy protection is justified. This paper supports posthumous information privacy protection.

A good starting point in this regard would be to include a reference to the information of deceased persons in the definition of personal information in section 1 of the POPIA and the Namibian Data Protection Bill and the various international and regional legal instruments discussed.

I thus recommend the approaches adopted in either the Estonian Data Protection Act or French Data Protection Act.<sup>196</sup> The Estonian Data Protection Act<sup>197</sup> restricts the processing of personal information to ten years in respect of personal information of majors and 20 years in respect of that of minors, after the death of the data subject. The French Data Protection Act permits individuals to decide on

---

Gianclaudio Malgierie, 'RIP: Rest in Privacy or Rest in (Quasi) Property Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions'(SSRN, 22 June 2018)<[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3185249](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185249)> accessed 20 May 2020.

<sup>192</sup> Act 17 of 2002.

<sup>193</sup> S v Williams 1986 (4) SA 1188 (A) at 1194D-H, an accused defense on a murder charge that victims death was caused by the doctors disconnecting the ventilator and not the shot that caused her to be braindead.

<sup>194</sup> See also Natasha Chu, 'Protecting Privacy after Death' (2015) 13 (2) Northwestern Journal of Technology and Intellectual Property 225-275, 250.

<sup>195</sup> Alessandro Mantelero, 'The future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 Computer Law & Security Review 105500.

<sup>196</sup> Section 9 Personal Data Protection Act (PDPA) adopted by the Estonian Parliament on December 12, 2018 and entered into force on January 15, 2019. Article 40-1 Loi Informatique et Libertés No. 78-17 of 6 January 1978 [updated version from 20 June 2018] (called "LIL") allows data subjects to establish instructions for the management of their personal data after death. See also the French Digital Republic Act (Loi n 2016-1321 pour une République numérique).

<sup>197</sup> Section 9 Personal Data Protection Act (PDPA).

the use of their personal information following their death and the personal data will be processed as directed by the data subject.<sup>198</sup>

In contrast to the views expressed above, there is a school of thought which holds that the dead are incapable of possessing legal rights and that the right to privacy is non-transferable. Consequently, information privacy should only be extended to living persons.<sup>199</sup>

## 6. Current appraisal of Information Privacy Protection and Drones

There is comprehensive academic work on privacy and information privacy protection within an array of focus areas, as summarised above. However, the privacy implications of drones are a fairly new consideration both internationally and nationally.<sup>200</sup>

It is common cause that there is no settled policy direction within the international community concerning the regulation of the privacy implications of drones, at this point.

This paper is not a virgin analysis of the privacy implications of drones in respect of the RSA. It has to a limited degree been the subject matter of an article by Nomalanga Mashinini<sup>201</sup> who focused her discussion on whether or not photographic data captured by drones are governed and enforceable under POPIA.<sup>202</sup>

I am of the view that the mentioned article is limited in scope, in so far as it only deals with photographic data captured by drones. Resultantly, no scholarly attention is devoted to other information privacy protection risks associated with

---

<sup>198</sup> Article 40-1 Loi Informatique et Libertés No. 78-17 of 6 January 1978.

<sup>199</sup> Natasha Chu, 'Protecting Privacy after Death' (2015) 13 (2) *North-western Journal of Technology and Intellectual Property* 225,275, 250.

<sup>200</sup> Nomalanga Mashinini, 'The processing of Personal Information using Remotely Piloted Aircraft systems in South Africa' (2020) 53 *De Jure Law Journal* 140,158.

<sup>201</sup> Nomalanga Mashinini, 'The processing of Personal Information using Remotely Piloted Aircraft systems in South Africa' (2020) 53 *De Jure Law Journal* 140,158.

<sup>202</sup>The Article focuses on 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.

drones. It is similarly overly preoccupied with the discussion of the enforceability of POPIA, at a time it was not yet operational.

The papers also pay very little attention to the role of civil aviation regulators and the civil aviation regulations on drones in advancing information privacy protection throughout the regulatory process, which is the focus of this paper.

Drones and information privacy have also been discussed by Samantha Huneburg<sup>203</sup> who have commendably placed the present research question in perspective, but regrettably did not dissect the civil aviation regulations against the information privacy principles set out in the POPIA, nor presented a comparative analysis to determine the effectiveness and observance these principles across the civil aviation regulatory spectrum and its contribution in protecting the human right to privacy.

From my analysis, the aforementioned discourse falls short of delineating the differences between information privacy protection and privacy and does not adequately dissect and consider the information privacy implications of drone regulations. The literature also falls short of analysing the efficacy of the entire system and applicable procedural mechanisms within which the information privacy rules are applied (in this case the civil aviation system).

In conclusion, my considered opinion is that the present discussion is unique, to the extent that it offers an update of and address the lacunae left by the existing literature on the subject. Moreover, this discussion will be benchmarked against the Model UAS Regulations adopted by ICAO on 23 June 2020<sup>204</sup> and a package of EU drone regulations which will be operationalised on the 1 of January 2024. Moreover, this thesis includes a comparative study, which will culminate in recommendations on how the problem statement of this thesis can be addressed and offer perspective on further research.

Furthermore, this discussion is pertinent to ensure the protection of the right of privacy guaranteed under the RSA and Namibian Constitutions, in so far as it

---

<sup>203</sup> Samantha Huneburg, 'The Rise of the Drone: Privacy concerns' (2017) THRHR 586.

<sup>204</sup> Officially Issued on 17 December 2020.



issues a call to action to the aviation industry, particularly the regulators to exercise due diligence to ensure that the emergence of this disruptive drone technology does not eviscerate the right to privacy, whilst at the same time ensuring the sustainable development of the civilian drone industry and optimising the multiplicity of socio-economic benefits it holds for our respective countries across various sectors.

The following chapter will analyse the POPIA and the Namibian Data Protection Bill which are the principal laws (prospective in the case of Namibia) setting out the standards and safeguards for the lawful processing of personal information in the jurisdictions under discussion.

## Chapter Three

### Information Privacy Laws in RSA and Namibia

---

*This chapter examines the POPIA and the Data Protection Bill of Namibia, which are the principal legislation dedicated to ensuring the lawful processing of personal information in RSA and Namibia in order to determine the information privacy principles, safeguards and mechanisms extended to data subjects within these jurisdictions, which must be adhered to in the course of regulating and deploying of civilian drones.*

#### 1. Introduction

In the wake of an intensifying digital industry, there is universal consensus that a sound information privacy framework enables the free flow of information, which in turn trade and economic growth.

Information privacy, also called data privacy or data protection, refers to the legal principles and mechanisms employed to preserve the privacy of personal information in the course of the use, storage, access, transmission, retention, and destruction; the obligation to ensure the immutability and security of personal information.<sup>205</sup>

According to the International Association of Privacy Professionals (IAPP), the overriding objective of any information privacy legal framework is to protect persons against unjustified interferences of their right to privacy and to grant individuals the legal right to manage their personal information and to obtain redress if their personal information has been processed unlawfully.<sup>206</sup>

Since the right to privacy is limited on legitimate grounds, information privacy rules and safeguards are generally balanced with other fundamental, occasionally

---

<sup>205</sup> Stephen J Bigelow, 'Data Privacy (information privacy)' (TechTarget, no date supplied) <<https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy>>accessed 10 October 2022.

<sup>206</sup> Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in action: In Serge Gutwirth et al (eds), Reinventing Data Protection (Springer 2009); Muhammad Waqas Javed, Muhammad Waqas Javed and Muhammad Arbab Maitla, 'CCTV Cameras Surveillance, Data Protection and Privacy Under International Human Rights Laws' (2021) 3 (2) Journal of Law & Social Studies 174-186,177 <DOI: 10.52279/jlss.03.02.174186> accessed 8 February 2022.

conflicting, values such as freedom of speech,<sup>207</sup> the need for efficient law enforcement and prosecution of crimes, the administration of justice, as well as for historic, artistic and journalistic purposes, which invariably constitute justifiable exclusions to the information privacy rules.<sup>208</sup>

The rules and safeguards also endow data subjects with entitlements to exercise (pro)-active control over the processing of their personal information.<sup>209</sup>

From a procedural point of view, information privacy regimes similarly emphasise independent oversight to monitor and enforce compliance with information privacy laws and typically provide for redress mechanisms and penalties for non-compliance.<sup>210</sup>

## 2. Generations of Information Privacy Laws

It is argued that informational privacy laws evolved across three socio-technical generations.<sup>211</sup> Each of these generations represents the parallel progression in information technology and information privacy standards worldwide.

---

<sup>207</sup> Director-General of Namibian Central Intelligence Service and Another v Haufiku and Others [2019] NASC 7 the Supreme Court held the notion that once the Executive invoked secrecy and national security, freedom of expression must be tramped is not consonant with the values of an open and democratic society based on the rule of law. See also Kennedy Kariseb, 'Namibian Supreme Court finds that National Security Concerns do not Automatically Trump Free Speech' (Oxford Human Rights Hub, May 24, 2019) <<https://ohrh.law.ox.ac.uk/namibian-supreme-court-finds-that-national-security-concerns-do-not-automatically-trump-free-speech/>> accessed 1 February 2022 ; Roland Routh, 'NCIS appeal judgment: Supreme Court dismisses Intelligence appeal' New Era (Windhoek, 15 April 2019) <<https://neweralive.na/posts/ncis-appeal-judgmentsupreme-court-dismisses-intelligence-appeal>> 10 March 2022.

<sup>208</sup> D Brin, 'The Transparent Society: Will technology force us to choose between Privacy and Freedom': In Philip E Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (1998 MIT Press); D McQuoid-Mason, 'Privacy'; In Stuart Woolman et al (eds), *Constitutional Law of South Africa* (2<sup>nd</sup> ed, Juta, [Revised 2011] 2014) 38; Johann Neethling, 'Features of the Protection of Personal Information Bill, 2009 and the law of Delict' (2012) 75 *THRHR* 245.

<sup>209</sup> Anneliese Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa' (2008)(11) (4) *Potchefstroom Electronic Journal* <DOI: 10.4314/pelj.v11i4.42243> accessed 5 January 2020; Bert-Jaap Koops, 'The trouble with European Data Protection Law' (2014) 4(4) *International Comparative Law Quarterly* 250–261 <<https://doi.org/10.1093/idpl/ipu023>> accessed 14 February 2022; Johann Neethling, J M Potgieter and Anneliese Roos, 'Legal Protection of Personal Data'; In Neethlings *Law of Personality* (2<sup>nd</sup> ed, LexisNexis 2019).

<sup>210</sup> Ian Currie and K Allan, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa' [2007] *South African Journal on Human Rights* 23, 563-579; International Bar Association, 'The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa' (IBA, 2021) <<https://www.lssa.org.za/wp-content/uploads/2021/07/Data-Protection-Privacy-Guide-Africa.pdf>> accessed 11 December 2021.

<sup>211</sup> Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis (2022) *Computer & Security Law Review* <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022.

The information privacy canons encapsulated in the OECD Guidelines<sup>212</sup> and Convention 108<sup>213</sup> are generally considered, as baseline first-generation information privacy ideologies.<sup>214</sup>

The second-generation information privacy principles are an extension of the first-generation principles, which were introduced by the now-repealed 1995 EU Data Protection Directive<sup>215</sup> and the 2001 Amending Protocol to Convention 108 on the global front.<sup>216</sup> On the regional front, the 2013 SADC Model Law<sup>217</sup> and the Malabo Convention<sup>218</sup> encapsulates second-generation information privacy rules.

Convention 108+ and the GDPR, which are cumulative of the previous generations' information principles embody the youngest augmentation of information privacy protection principles.<sup>219</sup> This generation is hallmarked by its insistence on data Privacy by Design and Default (PbD), undertaking information privacy impact assessments (DPIA) and issuing information privacy compliance accreditation or

---

<sup>212</sup> OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] <<https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>> accessed 14 February 2022.

<sup>213</sup> Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data (adopted 28 January 1981, entered into force 1 October 1985) [CETS 108] <<https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=108>> accessed 14 February 2022.

<sup>214</sup> David Banisar and Simon G Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (2012) 18 (1) John Marshall Journal of Computer & Information Law 3; Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis' (2022) Computer & Security Law Review <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022

<sup>215</sup> [Repealed] European Commission Data Protection Directive (Directive 95/46/EC).

<sup>216</sup> Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data flows (ETS No. 181) [updated in 2018] <[https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention\\_108\\_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf)> accessed 14 February 2022.

<sup>217</sup> SADC Model Law on Data Protection, Electronic-Transactions and Cybercrime <<https://www.SADCModelLawonDataProtection,Electronic-TransactionsandCybercrime.itu.int/en/ITUD/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf>> accessed 14 February 2022.

<sup>218</sup> African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection [Malabo Convention] 2014 <[https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)> accessed 14 February 2022.

<sup>219</sup> Alessandro Mantelero, 'The future of data protection: Gold standard vs. global standard Author links open overlay panel (2021) 40 Computer Law & Security Review 105500 <<https://doi.org/10.1016/j.clsr.2020.105500>> accessed 12 March 2022.

obtaining information privacy compliance conformity endorsements amongst others.<sup>220</sup>

It is reported that there is at present a technological war (Tech War) to establish geopolitical and economic control in respect of the international ICT agenda. between the EU and its economic and political rivals, like the US and China.<sup>221</sup> The GDPR is hailed as the new golden standard of information privacy law.<sup>222</sup> Mantelero criticises the claim that the GDPR represents a golden information privacy standard, as over-ambitious. He contends that notwithstanding the global impact of the GDPR, the revised Convention 108+ represents an information privacy global standard. Mantelero defines a global standard with reference to having a great number of followers and a global standard being geo-politically acceptable.<sup>223</sup>

### 3. Yardsticks of a sound Information Privacy Legal Framework

Greenleaf<sup>224</sup> postulates that information privacy laws are effective if it applies to the most significant sectors within the private or public sector. Another hallmark of an effective information privacy legal framework is the call to observe a minimum set of basic information privacy principles, akin to the minimum standard provided for by the OECD Guidelines or Council of Europe Convention 108 [without its 2001 additional Protocol], plus some modality for officially-backed enforcement.<sup>225</sup>

---

<sup>220</sup> Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis (2022) Computer & Security Law Review <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3582478](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478)> accessed 7 January 2022.

<sup>221</sup> Agathe Demarais, 'How the U.S.-Chinese Technology War Is Changing the World' FP News (Online 19 November, 2022) <<https://foreignpolicy.com/2022/11/19/demarais-backfire-sanctions-us-china-technology-war-semiconductors-export-controls-biden/>> accessed 21 December 2022.

<sup>222</sup> Giovanni Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard' (European Data Protection Supervisor, 1 April 2016) < [https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard\\_en](https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_en)> accessed 21 December 2022; Margaret Taylor, 'Data protection: threat to GDPR's status as 'gold standard' ( International Bar Association, 25 August 2020) <https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED532> 21 December 2022. 25 August 2020

<sup>223</sup> Alessandro Mantelero, 'The future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 Computer Law & Security Review 105500,105503.

<sup>224</sup> Graham Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23 (1) Journal of Law, Information & Science 4-49,10; W.Gregory Voss, 'Obstacles to Transatlantic Harmonization of Data Privacy Law in Context' 2019 (2) Journal of Law, Technology & Policy< 405-463< fahal-02482174f <<https://ssrn.com/abstract=2280877>> accessed 20 February 2022.

<sup>225</sup> Anneliese Roos, 'Core principles of Data Protection Law' (2006) 39(1) *Comparative International Law South Africa* 102–130; Anneliese Roos, 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *South African Law Journal* 421; Jonathan Burchell 'The Legal Protection of Privacy in South Africa: A transplantable hybrid' (2009)

The above assertion is buttressed by Roos<sup>226</sup> and Bygrave.<sup>227</sup> This assertion is further supported by Bennet and Raab<sup>228</sup> who asserts that an informational privacy framework is sound if it includes a set of at least ten of the basic information privacy principles listed in the 1980 OECD Guidelines.

Even though the information principles demarcated in the 1980 OECD Guidelines and Convention 108 are considered as an indicator of a functional information privacy legal framework. The fact that these European legal instruments are employed as a litmus test to evaluate the efficacy of information privacy laws, should also not be accepted as an endorsement that countries outside Europe have less wholesome information protection laws.

Caution should also be exercised not to employ the presence (or otherwise) of data privacy laws as the sole index to measure the judiciousness of information privacy protection in a country. However, the efficacy of an information privacy system must also be assessed with reference to the totality of the legal framework, as well as the availability, accessibility and effectiveness of suitable redress mechanisms for aggrieved data subjects.<sup>229</sup>

---

13(1) *Electronic Journal of Comparative Law* 1; G Gunasekara 'Paddling in unison or just paddling? International trends in reforming Information Privacy Law' (2014) 22 (2) *International Journal of Law and Information Technology* 141; Koliwe Majama, Janny Montinat and Anriette Esterhuysen (Cordinators), *Privacy and Personal Data Protection in Africa: A Rights-based Survey of Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021); See also OECD, 'Thirty years After the OECD Privacy Guidelines', (DDPR.EU, no date supplied) <<https://gdpr.eu/what-is-gdpr/>> accessed 14 February 2022.

<sup>226</sup> Anneliese Roos, 'Core principles of Data Protection Law' (2006) 39(1) *Comparative International Law South Africa* 102–130; Johan Neethling 'Features of the Protection of Personal Information Bill, 2009 and the Law of Delict' (2012) *THRHR* 243; C Kuner 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 *Computer Law & Security Review* 307,308.

<sup>227</sup> Lee Andrew Bygrave, 'Data Protection pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 (3) *International Journal of Law and Information Technology* 250; Lee Andrew Bygrave, 'The Place of Privacy in Data Protection' (2001) 24 (1) *University of Wales Law Journal* 277; Lee Andrew Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002) 57.

<sup>228</sup> C Bennett and C Raab C, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006).

<sup>229</sup> Yvonne Burns and Burger-Smidt Ahmore, *Commentary on the Protection of Personal Information Act* (LexisNexis Durban 2018).

As confirmed by Roos in her contrast of the POPIA and the GDPR,<sup>230</sup> the POPIA offers better information privacy protection in some regards.<sup>231232</sup>

#### 4. Republic of South Africa

Even though there are information privacy topographies amongst others in the Promotion of Access to Information Act (PAIA),<sup>233</sup> Electronic Communications and Transactions Act,<sup>234</sup> Financial Intelligence Act,<sup>235</sup> National Credit Act,<sup>236</sup> Consumer Protection,<sup>237</sup> National Health Act,<sup>238</sup> Children's Act,<sup>239</sup> Interception of Communications and Provision of Communication-Related Information Act,<sup>240</sup> and the POPIA.<sup>241</sup>

In what follows, we will offer an overview of the most important information privacy principles, safeguards enforcement mechanisms and safeguards prescribed under POPIA and the Namibian Data Protection Bill as is relevant within the scope of this thesis. Owing to the scope of this research, the exposition in this paper is limited to the examination of the POPIA which is the prime information privacy law in the RSA

##### 4.1. Protection of Personal Information Act (POPIA)

---

<sup>230</sup>Roos, Anneliese. 'The European Union's General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) (3) 37 Comparative and International Law Journal of Southern Africa 53 <<https://doi.org/10.25159/2522-3062/7985>> accessed 17 November 2022.

<sup>231</sup> For example, POPI covers juristic persons whilst the GDPR does not.

<sup>232</sup>Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) International Data Privacy Law <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1960299](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299)> accessed 26 January 2022 ; Graham Greenleaf, 'Modernising' Data Protection Convention 108: A safe basis for a Global Privacy Treaty?' (2013) 29 Computer Law and Security Review 430 – 436 <<http://dx.doi.org/10.1016/j.clsr.2013.05.015>> accessed 20 February 2022; D McQuoid-Mason, 'Privacy': In Stuart Woolman (eds) and Others, In *Constitutional Law of South Africa: Commentary* (2<sup>nd</sup> ed, Juta 2014).

<sup>233</sup> Act 2 of 2000. See Sections 17, 19, 30, 34, 61, 71, 72, 88.

<sup>234</sup> Section 50 and 5, Act 25 of 2005.

<sup>235</sup> Act 2 of 2000.

<sup>236</sup> Act 32 of 2005.

<sup>237</sup> Act 68 of 2000.

<sup>238</sup> Act 61 of 2003, Section 14.

<sup>239</sup> Act 38 of 2005.

<sup>240</sup> Act 70 of 2002.

<sup>241</sup>A Naude and Sylvia Papadopoulou, 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments' (2016) (1) THRHR 51.

#### 4.1.1. Scope and Application

The Preamble of the POPIA stipulates that it aims to advance and safeguard the right to privacy commensurate with international standards.<sup>242</sup>

The POPIA applies to automated and non-automated and partially autonomous records of personal information of natural and juristic persons, groups and associations<sup>243</sup>, processed within the RSA or by a person domiciled in RSA as well as data subjects, responsible parties and operators within both the public and private sector.<sup>244 245</sup>

Consistent with common and constitutional law, the POPIA also covers personal information relating to juristic persons, including sole traders and partnerships.<sup>246</sup>

It is however surprising that the POPIA is silent on its applicability to the personal information of deceased persons, notwithstanding the fact that under sections 34(2) (i)-(ii) and 63 (2)(i) -(ii) of the PAIA,<sup>247</sup> it is justifiable to refuse access to information on the ground that availing the information will constitute an unreasonable exposé of personal information of a deceased person.

The definition of personal information under section 1 of the POPIA is extensive, but not definite. The definition was found to be wider in reach compared to the GDPR<sup>248</sup> which is described as an international gold standard.

The POPIA impose special safeguards in respect of the processing of personal data of children, or that relating to criminal records and where the processing involves data

---

<sup>242</sup> POPIA Preamble.

<sup>243</sup> Roos A, 'Data privacy law': In Van der Merwe et al, *Information and Communications Technology Law* (3<sup>rd</sup> ed, LexisNexis 2021).

<sup>244</sup> As defined under section 1 of the POPIA.

<sup>245</sup> Defined as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including- (a) the 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.

<sup>246</sup> Section 3 of the Protection of Personal Information Act 4 of 2013.

<sup>247</sup> Act 2 of 2000.

<sup>248</sup> Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' Vol. (2020) 53 (3) *Comparative and International Law Journal of Southern Africa* <<https://doi.org/10.25159/2522-3062/7985>> accessed 19 September 2022.



matching, in these instances pre-approval from the Information Regulator (IRSA) is required.<sup>249</sup>

Alongside the internationally recognised prohibited grounds of discrimination, health information is classified as sensitive information<sup>250</sup> and is subject to supplementary protection.<sup>251</sup>

#### 4.1.2. Exclusions

In line with jurisprudence on privacy, section 6 and 7 of the POPIA acknowledge that the right to privacy is subject to justifiable limitations.<sup>252</sup> Resultantly, the Act absolves the following processing activities from the scope of the Act:

- processing for **purely household and or personal use**<sup>253</sup>;
- processing effected in accordance with legislation encompassing adequate safeguards, aimed at advancing **national security, defence or public safety, criminal investigation and prosecution**;
- processing within the **scope of freedom of expression**;
- processing for **historical tenacities and literacy or artistic expression**;
- processing by the various **tiers of Government**;
- processing **anonymous or de-identified information**;
- processing by persons who are **subject to a code of professional ethics that provides adequate safeguards for the protection of personal information**;
- processing in the course of the administration of justice; and
- processing specifically exempted by the IRSA in terms of sections 37 and 38.

---

<sup>249</sup> According to Peter Christen, Data Matching (Springer, 2012) involves collating (syncing) data from various databases of data and unifying. It aimed at determining coincident entries and is employed to connect information large databases for advertising or other practical purposes.

<sup>250</sup> Information relating to children, religion or philosophy of life, race, trade-union membership, political persuasion, health and sexual life, and criminal behaviour etc.

<sup>251</sup> Section 34- 35 of the Protection of Personal Information Act 2013.

<sup>252</sup> Commensurate with Section 36 of the RSA Constitution which provides that rights may be limited by a law of general application that is 'reasonable and justifiable in an open and democratic society based on dignity, freedom, and equality'.

<sup>253</sup> In the *Bodil Lindqvist* case which involved the invocation of the household exception as a defense to a claim of violating the Swedish Data Protection Law, the court held that the fact that the incidence related to charitable or religious activities that could be indexed by search engines, excluded it from the personal or household exception.

### 4.1.3. Information Privacy Protection Principles

Section 8 of the POPIA obligates all responsible parties to ensure compliance with and adopt measures to give effect to the following **eight information privacy principles**;<sup>254</sup>

- **Accountability**

This condition assumes that all stakeholders in the information privacy protection ecosystem have a role to play in ensuring the protection of the right to information privacy. It necessitates the development of institutional information privacy protection policies, as well as the designation of internal data protection officers (DPOs), as safeguards for acquiescence with the POPIA. It speaks to developing and promoting an information privacy protection consciousness and institutional culture in all private and public spheres. Moreover, that information privacy compliance should where appropriate be ensured by a combination of PbD, self-, regulation and co-regulation mechanisms supported by clear implementation and enforcement mechanisms.

The disclaimer from the NaCCA website illustrated<sup>255</sup> in Chapter 1 and the general dereliction of privacy concerns within the civil aviation industry, in my opinion, constitutes a breach of the accountability principle.

- **Processing Limitation**

Compliance with this condition insists on processing personal information, in the least intrusive manner. The yardstick employed in this regard is that processing must not be arbitrary, or invasive and must be justifiable in law, or be pursuant to contractual obligations, or the data subject must have granted prior informed consent to the processing. This principle also demands that personal information should primarily be sourced from the data subject.

- **Purpose Specification**

---

<sup>254</sup> Part A Chapter 3, Section 8-25 of the Protection of Personal Information Act 2013.

<sup>255</sup> See Figure 1.

This principle demands that personal information may only be processed for a lawful, specified and explicitly defined purpose that correlates to the core function of the processor. It further demands that the data subjects must be informed of this lawful, specified and explicitly defined purpose prior to or at the time of collection.

This principle correspondingly insists that personal information must be destroyed (erased) or anonymised if the purpose of the collection is achieved.<sup>256</sup> In most legal systems, the right to erasure is commonly referred to as the 'right to be forgotten'<sup>257</sup> or right to oblivion.<sup>258</sup>

- **Further processing limitation (function creep)**

Tethering to the condition above, save for purposes that may fall within the exclusions under the POPIA, this condition inhibits further processing of personal information, which is incompatible with the lawful, specified and explicitly defined purpose of which the data subjects have been informed.<sup>259</sup>

It further constrains the blurring or widening of purposes for processing after the data subject agreed to initial collection or the (re-) use of personal information for purposes not initially foreseen or disclosed. The *Black Sash Trust v Minister of Social Development and Others*,<sup>260</sup> in which it was held that the transmission of the personal information of the social grant beneficiaries obtained for purposes of paying social grants, as per section 20 of the Social Assistance Act, to insurance companies was unlawful, is a great example of the application of this principle.<sup>261</sup>

- **Information Quality**

This condition requires that personal information must be processed efficiently. This obligates that caution must be exercised to ensure that processing, is accurate and

---

<sup>256</sup> Rolf H Weber, 'The right to be forgotten. more than a Pandora's Box' [2011] Journal of Intellectual Property, Information Technology and E-commerce 120,130; Viktor Mayer Schonberger, *Delete: the Virtue of Forgetting in the Digital Age* (Princeton University Press 2009).

<sup>257</sup> The right to be forgotten allows individuals to have personal information, videos, or images removed from specific online records, so that they are no longer appear in search engines.

<sup>258</sup> See Article 17 of the GDPR.

<sup>259</sup> Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 13 (1) Law, Innovation and Technology 29.

<sup>260</sup> (CCT48/17) [2018] ZACC 36; 2018 (12) BCLR 1472 (CC).

<sup>261</sup> Act 13 of 2014.

complete and where needed it is rectified, updated or appropriately annotated or deleted.

- **Openness**

This requirement is an enabler of all the data subject's rights. It stresses compliance with all notification requirements imposed under the POPIA <sup>262</sup> It also mandates that a manual detailing the source and legal basis for the processing of personal information and potential transfers must be kept by all processors or controllers.

It is in furtherance of this principle that the POPIA requires that the data subjects must be kept abreast, of all relevant facts regarding the processing of their personal information, particularly the name and contact details of the processor and where applicable all incidences of cross-border transfer of personal information and protections.<sup>263</sup>

Openness further requires that data subjects and the Data Protection Authority (DPA) must be informed of incidences of information privacy breach that is likely to cause serious harm to data subjects. Malgieria and Custer assert that this principle also demands that data subjects are informed of the economic value of their personal information.<sup>264</sup>

- **Security Safeguards**

As a means to reinforce the above principles, this condition demands that appropriate institutional and technical measures, aligned to generally accepted practices and procedures, are implemented to ensure observance of the requirements under the POPIA.<sup>265</sup> It further requires that reasonable measures must be invoked to detect foreseeable internal and external risks to personal information and to develop and uphold appropriate safeguards against risks identified, as well as to exercise vigilance in respect of emerging risks.<sup>266</sup>

---

<sup>262</sup> Section 11, 19,47, 50,55 and 51 of PAIA.

<sup>263</sup> Section 19.

<sup>264</sup> Gianclaudio Malgieria and Bart Custersb, 'Pricing privacy – the right to know the value of your personal data' Computer Law & Security Review (2018) 34 (2) 289-303.

<sup>265</sup> Section 19.

<sup>266</sup> Stephens Savanna and Jefferson Monique, 'Global Data Protection Laws of the World: Law

- **Data Subject Participation**

In response to the limited post-facto protection afforded to personal information under common law,<sup>267</sup> data subjects are afforded active control over the processing of their personal information through the right to request confirmation of whether their personal information is being processed or to request a record or description of personal information held of them and details concerning third parties who have access to the data subject's data. Data subjects are also accorded the right to request that personal data be corrected or deleted. Data subjects exercise their rights following the procedure prescribed under sections 18, 25 and 53 of the PAIA. Section 69 of the POPIA empowers data subjects to object to unsolicited electronic communications and automated decision-making.

#### **4.1.4. Oversight and Enforcement**

##### **Institutional Framework and functions**

Chapter 5 of the POPIA provides for the establishment of the IRSA,<sup>268</sup> an Enforcement Committee and other institutional frameworks.<sup>269</sup> The IRSA is mandated to exercise oversight of the implementation of the POPIA,<sup>270</sup> conduct educational campaigns and research on matters within the scope of the Act, as well as offering administrative interventions and dispute resolution mechanisms to enable aggrieved persons to seek redress for the infringement of their right to informational privacy.<sup>271</sup>

The Act also mandates the appointment of DPOs<sup>272</sup> under section 17 of the PAIA,<sup>273</sup> to monitor and enforce and implementation of the POPIA and PAIA in the course of the internal operations of data processors and controllers.<sup>274</sup>

---

In South Africa' (DLA Piper, no date supplied)

<[www.dlapiperdataprotection.com/dex.html?t=law7c=ZA](http://www.dlapiperdataprotection.com/dex.html?t=law7c=ZA)> (accessed March 2021)

<sup>267</sup> Section 23 and 24 of the Protection of Personal Information Act 2013.

<sup>268</sup> Section 39 the Protection of Personal Information Act 2013

<sup>269</sup> Section 50 of the Protection of Personal Information Act 2013.

<sup>270</sup> Section 40 of the Protection of Personal Information Act 2013.

<sup>271</sup> Section 40 (d) of the Protection of Personal Information Act 2013.

<sup>272</sup> The default position is that the head of a company is the 'information officer'.

<sup>273</sup> Act No 2 of 2000.

<sup>274</sup> Section 55 of the Protection of Personal Information Act 2013.

#### **4.1.5. Enforcement and Implementation**

The IRSA is authorised to undertake *mero motu* investigations into information privacy breaches and to deal with the complaints in accordance with the procedures laid out in the POPIA.<sup>275</sup> Subject to stipulated due processes, the IRSA is authorised to issue enforcement notices to ensure recompense of any information privacy protection transgression under the POPIA.

#### **4.1.6. Administrative Fines, Offenses and Penalties**

Chapter 11<sup>276</sup> strengthens the enforcement and implementation of the POPIA through the imposition of administrative fines and penalties for non-compliance with the Act.<sup>277</sup> IRSA is empowered to impose administrative fines not exceeding R 10 million, for non-compliance with the enforcement or information notice(s) in terms of section 109 of the POPIA.<sup>278</sup>

To strengthen the integrity of the enforcement process, the POPIA among others renders it an offence to provide false information, leak confidential information, interfere with warrants and investigations undertaken under this Act or for witnesses to present false testimony.<sup>279</sup>

#### **4.1.7. Penalties**

In addition to the imposition of administrative fines, unparalleled by even the GPDR, contravening certain provisions of the POPIA may result in an indictment under criminal law in terms of section 107 thereof, which provides that contravening the enumerated provisions of the Act, attracts a penalty of either or both, a fine with an upper cap of R10 million or 10-years custodial sentence.<sup>280</sup>

---

<sup>275</sup> Chapter 10, Sections 73-99 of the Protection of Personal Information Act 2013. The Act authorise the investigation of complaints, conduct searches and seize items, as well as the to summon and enforce appearances of witnesses and or for the discovery of relevant documents.

<sup>276</sup> Section 100- 109 of the Protection of Personal Information Act 2013.

<sup>277</sup> J Giles, 'GDPR vs POPIA: Compare the GDPR with the POPI Act?' (Michalsons,13 February 2020) <<https://www.michalsons.com/blog/gdpr-mean-popi-act/19959>> accessed 14 February 2021.

<sup>278</sup> Section 109 of the Protection of Personal Information Act 2013.

<sup>279</sup> Section 100-104 of the Protection of Personal Information Act 2013.

<sup>280</sup> Elizabeth de Stadler and Paul Esselaar, *A guide to the Protection of Personal Information Act* (Juta 2015).

#### 4.1.8. Parallel Civil Claim(s)

In terms of section 99 of the Act, either a data subject or the IRSA may institute a civil claim on behalf of the data subject(s) or a class of data subjects, without having to establish culpability on the part of the violator and claim compensation for patrimonial and non-patrimonial losses suffered, as a result of non-compliance with the Act.<sup>281</sup>

Indigent data subjects may be abetted by the IRSA to litigate any contravention of the POPIA. The Act permits the imposition of punitive damages proportional to the infringement in a particular instance, however, the aggrieved data subject will only receive the balance after all litigation costs are defrayed if the claim is successful.<sup>282</sup>

Recidivists' contraventions under the POPIA are likely to be slapped with punitive damages as alluded to in *Fose v Minister of Justice*<sup>283</sup> the court justified the imposition of aggravated claims because despite being aware that the claims were false the defendant alleged that the plaintiff was guilty of murder and rape over six years.<sup>284</sup>

#### 4.1.9. Collaboration and Sectoral Governance

The POPIA leverages private sector involvement and support to relieve the monitoring and enforcement burden on the IRSA, in industries with competent regulators and or adequate dispute resolution mechanisms for contravention of the POPIA on the principle of subsidiary.<sup>285</sup>

---

<sup>281</sup> patrimonial loss relates to the monetary loss suffered by a data subject as a result of the breach. Non-patrimonial loss is the infringement of personality rights or loss suffered as a result of inconvenience, pain and suffering caused by the breach.

<sup>282</sup> Johann Neethling, 'Punitive Damages in South Africa'; In Helmut Koziol and Reiner Schulze (eds), *Tort Law of the European Community* (Volume 25, Springer 2009) 123-136.

<sup>283</sup> 1997 3 SA 786 (CC); See also *Komapo v Minister of Basic Education and others* (1416/2015) [2018] ZALMPPHC 18 (23 April 2018).

<sup>284</sup> Paragraph 482: 'It is difficult to imagine one more gross, for the plaintiff was said to be guilty of the two most serious crimes known to the law [...] Under these circumstances, the Court should have awarded a very substantial sum by way of compensation to the plaintiff for the contumelia inflicted, and by way of penalty upon the defendant for his aggravated and malicious defamation

<sup>285</sup> Subsidiarity refers to the absolute right of local communities to take decisions for themselves, including the decision to surrender the matter to a larger forum.

To this end, chapter 7 empowers the IRSA to issue guidelines on the development of and or to endorse industry codes of conduct, following consultation with the relevant industry stakeholders and to review these codes from time to time. Approval of a code of conduct enables industry regulators to act in the stead of the IRSA, in respect of a particular industry,<sup>286</sup> without abrogating the powers of the IRSA under the POPIA.<sup>287</sup>

#### 4.1.10. Data Export

As a means to encourage the free flow of information and boost electronic commerce, the POPIA permits the cross-border transfer of personal information to jurisdictions that can guarantee substantially commensurate levels of information privacy protection under either their domestic law, contractual undertakings, professional rules or if the data subject consented to such cross- border transfer.<sup>288</sup>

#### 4.1.11 Cooperation Initiatives

Mindful that an efficient informational privacy framework requires national and intra-national cooperation of various stakeholders. Recognising that the RSA is part of a global village section 40(1)(d) of the POPIA permits the IRSA to partake in international enforcement cooperation initiatives,<sup>289</sup> such as the Network of African Data Protection Authorities (NADPA); the Round Table of African Data Protection Authorities (RADPA) and the Global Privacy Assembly (GPA).<sup>290</sup> The GPA has established a permanent International Enforcement Working Group (IEWG).<sup>291</sup> Syers<sup>292</sup> state that information privacy international cooperation initiatives are

---

<sup>286</sup> Section 78 of the POPIA empowers the IRSA to defer complaints received, in whole or part to various industry regulators.

<sup>287</sup> Sections 60-68 of the Protection of Personal Information Act 2013; See Shenaaz Munga and Nicole Gabryk, 'South Africa: POPIA Litigation and Claims for civil damages – What to Expect' (Mondaq ,03 September 2020) <<https://www.mondaq.com/southafrica/privacy-protection/981298/popia-litigation-and-claims-for-civil-damages-what-to-expect>> accessed 19 August 2022.

<sup>288</sup> Chapter 9, Section 72 of the Protection of Personal Information Act 2013.

<sup>289</sup> W Peekhaus, 'South Africa's Promotion of Access to Information Act: An Analysis of Relevant Jurisprudence' (2014) 4 Journal of Information Policy 570-96 <<https://doi.org/10.5325/jinfopoli.4.2014.0570>> accessed 12 January 2022.

<sup>290</sup> Formerly known as International Conference of Data Protection and Privacy Commissioners - ICDPPC).

<sup>291</sup> Koliwe Majama, Janny Montinat and Anriette Esterhuysen (Cordinators), African Declaration on Internet Rights and Freedoms Coalition, *Privacy and Personal Data Protection in Africa: A rights-based survey of legislation in eight countries* (APC, 20 May 2021)<[https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica\\_CountryReports.pdf](https://www.apc.org/sites/default/files/PrivacyDataProtectionAfrica_CountryReports.pdf)> accessed June 2021.

<sup>292</sup> Richard Syers, Powerpoint Presentation at the global privacy assembly 'International cooperation to facilitate cross-border data flows' (globalprivacyassembly.org, no date supplied)



forums for capacity building, connecting and supporting national and international DPAs to execute their duties and functions effectively.

## 5. The Republic of Namibia

During 2020 the UN body for ICT, the International Telecommunications Union (ITU) reported that Namibia received a meagre 2.84 ranking for putting in place legal measures to respond to information communication technology (ICT) challenges, 6.30 for capacity-building and 2.34 in respect of participation in cooperation initiatives.<sup>293</sup>

The need to bolster the information communications technology laws and policies to optimise the benefits of the 4IR as an enabler of economic growth <sup>294</sup> is emphasised in most of the strategic national documents, such as Vision 2030,<sup>295</sup> National Development Plan 5,<sup>296</sup> and Harambee Prosperity Plan 2.<sup>297</sup> The World Bank Group Digital Economy for Africa (DE4A) country diagnostic initiative reports also confirmed that policy development and regulation is one of the four key pillars, which will enable Namibia to transition toward a digital economy.<sup>298</sup>

---

<[https://www.wto.org/english/res\\_e/reser\\_e/1\\_richard\\_wto-gpa\\_slides.pdf](https://www.wto.org/english/res_e/reser_e/1_richard_wto-gpa_slides.pdf)> accessed 12 September 2022.

<sup>293</sup> Tujoromajo Kasuto, 'The 4IR in Namibia Faces Fundamental Issues' (IPPR Blog, 29 Nov 2021) < [https://29 Nov 2021 ippr.org.na/blog/4ir-faces-fundamental-issues-in-namibia/](https://29%20Nov%202021%20ippr.org.na/blog/4ir-faces-fundamental-issues-in-namibia/)> accessed 20 November 2022.

<sup>294</sup> 4IR refers to the fusion of development in artificial intelligence (AI), robotics, the internet of things (IoT), and other technologies.

<sup>295</sup> Office of the President, 'Namibia Vision 2030 Policy Framework for Long-Term National Development' (Namfisa, 2004) < <https://www.namfisa.com.na/wp-content/uploads/2017/10/Vision-2030.pdf>> accessed 12 February 2022.

<sup>296</sup> Fifth National Development Plan (NDP5) 2017/18 – 2021/2022 < <https://www.npc.gov.na/national-plans/national-plans-ndp-5/>> accessed 1 Jan 2022; See also National Planning Commission, Namibia, 'Launch of Namibia's Fifth National Development Plan (NDP5)' *Tralac* (South Africa, 02 Jun 2017) <<https://www.tralac.org/news/article/11698-launch-of-namibia-s-fifth-national-development-planndp5.html#:~:text=By%202030%2C%20Namibia's%20population%20is,disadvantaged%20persons%20into%20mainstream%20economy>> accessed 1 Jan 2022.

<sup>297</sup> Konrad Adenauer Stiftung, 'Harambee Prosperity Plan' (KAS, no date supplied) < <https://www.kas.de/documents/279052/279101/Der+Harambee+Prosperity+Plan+II.pdf/7691d89b-2e35-20e9-86d4-cd9779a40f61?version=1.0&t=1624947238275>> accessed 1 Jan 2022.

<sup>298</sup> Bernie Zaaruka, Charlotte Tjeriko and Henock Shilongo, 'Paper #1: Overview of Digital Transformation in Namibia' (Bank of Namibia Annual Symposium 4 November 2021, Windhoek) <<https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/c7/c7dc8056-584a-4558-a5a3-2d20c7f73279.pdf>> accessed 1 Jan 2022; Tujoromajo Kasuto, 'Fourth Industrial Revolution report ready for submission' *Windhoek Observer* (Windhoek, July 29, 2022) <<https://www.observer24.com.na/fourth-industrial-revolution-report-ready-for-submission/>> accessed 20 October 2022.

## 5.1 Governance **Institutions**

The Ministry of Information and Communications Technology (MICT) is responsible for promoting the use and effective regulation of ICT services in Namibia. The Parliamentary Standing Committee on Information, Communication, Technology (CCICT) and Innovation, currently serves as an oversight body to ensure that the MICT executes its mandate effectively.<sup>299</sup>

The oldest law in the Namibian information privacy legal landscape is the Protection of Information Act.<sup>300</sup> Sections 3 and 4 of the Protection of Information Act, prohibit obtaining and disclosing state information that threatens and/or jeopardises national security and counter-terrorism initiatives and impose a fine not exceeding N\$10,000 and or imprisonment for a period not exceeding 10 years, upon conviction.

Information privacy is further safeguarded through the general prohibition of interception and monitoring.<sup>301</sup> Interception and monitoring are only permitted as a measure of last resort in accordance with a high court order<sup>302</sup> under the Namibia Central Intelligence Service Act.<sup>303</sup>

The Communications Act also contains a few noteworthy pro-information privacy stipulations.<sup>304</sup> Part 6 of Chapter V (interception of telecommunications) was operationalised on 1 January 2023.<sup>305</sup> Part six remained suspended since the promulgation of the Act following an objection that it constitutes an unjustifiable restriction on the (right to informational) privacy.<sup>306</sup>

---

<sup>299</sup>CIPESA and Small Media, 'UPR Submission, Submission to the 38th session of the Universal Periodic Review, Namibia' < [https://cipesa.org/?wpfb\\_dl=436](https://cipesa.org/?wpfb_dl=436) > accessed 14 January 2022.

<sup>300</sup> Act 84 of 1982.

<sup>301</sup> Section 24 and 25 of the Namibia Central Intelligence Service Act 10 of 1997.

<sup>302</sup> Section 25 mandates the Director- General to obtain requires a warrant, which is pre-conditioned on providing evidence of a serious threat to state security and detailed specifics regarding a type of communication and target.

<sup>303</sup> Act 10 of 1997.

<sup>304</sup> Act 8 2009. The Communications became effective on 18 May 2011, with the exception of Parts 4 and 6 of Chapter V and Chapter IX, by GN 64/2011 (GG 4714); Chapter IX (establishment and incorporation of .na domain name association) will come into force on a date or dates set by the Minister by notice in the Government Gazette.

<sup>305</sup> Government Notice 292/2022 (Government Gazette 7917); Sections 70-77 of the Communications Act 8 2009.

<sup>306</sup> Communications Act 8 of 2009 (GG 4378) brought into force on 18 May 2011 with the exception of Parts 4 and 6 of Chapter V and Chapter IX, by GN 64/2011 (GG 4714); Part 4 of Chapter V was brought into force on 1 December 2016 by GN 285/2016 (GG 6188); the remaining provisions come into force on 1 January 2023. See (Government Notice 7481) Government Gazette

Interception for purposes of combating crime and national security in instances authorised by law, as well as any directives issued by the Director General of the Central Intelligence Services and subject to a warrant authorising such interception.

Section 71 of the Communications Act impose a duty on telecommunications service providers to ensure that their services are capable of being intercepted. They are also mandated to hoard *inter alia* information relating to the originator, destination, contents of, and other information relating to the services they provide.

Commendably, section 121(3) inhibits the Namibian Communications Regulatory Authority (CRAN) from collecting content data of any message or information transmitted over an electronic communications network or obtaining any information relating to the behaviour of any customer or user of any telecommunications service, in the course of effecting its regulatory functions.

Another law that has information privacy implications is the Electronic Transactions Act.<sup>307</sup> Chapter four<sup>308</sup> of this Act protects individuals from unsolicited communications and other unrequested promotional pop-ups.<sup>309</sup> Contravention attracts a fine not exceeding N\$20 000.

Recently, the Covid-19 State of Emergency Regulations<sup>310</sup> promulgated under Article 26 of the Namibian Constitution, also displayed the sensitivity of information privacy principles, in so far as it sought to protect the information entered into the registers intended to be used for contact tracing, as a means to control the virus.<sup>311</sup>

---

No. 40 of 15 March 2022 < <https://www.cran.na/yglilidy/2022/06/GG-7481-dated-15-March-2021.pdf> > accessed 10 November 2022.

<sup>307</sup> Act 4 of 2019. The Act (with the exception of Section 20, Chapter 4 and Chapter 5) became operational on 16 March 2020 by GN 75/2020 (GG 7142). <<https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=518&cid=19> > accessed 1 August 2021.

<sup>308</sup> Chapter four stipulates various provisions, suppliers offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make available to consumers to help them execute electronic transactions offers.

<sup>309</sup> Chapter 4 of the Electronic Transactions Act 4 of 2019. See also Nghinomenwa Erastus, 'Online shoppers' protection delayed' *The Namibian Newspaper* (Windhoek, 2 August 2021) <<https://www.namibian.com.na/208505/archive-read/Online-shoppers-protection-delayed> > accessed 1 January 2021.

<sup>310</sup> Proclamation No. 13 Amendment of State of Emergency COVID-19 Regulations: Namibian Constitution <https://www.lac.org.na/laws/2020/7180.pdf> > accessed 14 February 2022.

<sup>311</sup> See Regulation 15 read as follows: The persons who are required to open and maintain a register in accordance with sub regulation (5) must –  
(a) keep the register in a safe place for the duration of the State of Emergency;  
(b) on request, make the register available for inspection by an authorised officer; and

Non-compliance with these stipulations was sanctioned by a fine of N\$ 2000 and or six-month imprisonment.

Following deliberation by the CCICT, the Namibia Access to Information Bill<sup>312</sup> were recently approved by the National Council.<sup>313</sup> The Access to Information Bill aims to provide citizens with the right of access to information held by public and private entities to facilitate transparency, accountability and good governance.<sup>314</sup> Section 30 of the Access to Information Bill endows an enforceable right to access information held by public entities. Personal information of third parties is protected under section 66 of the Bill and health information is protected in terms of section 68.<sup>315</sup>

Namibia's principal law on information privacy is yet to be adopted. Namibia has developed several draft versions of legislation on information privacy; the earliest

---

(c) consider the information provided under this regulation to be confidential, and may not disclose that information to any other person except as provided in paragraph (d) or when required to so disclose in terms of any law.

6 (a) requires person(s) to keep the register in a safe place for the duration of the State of Emergency. Sub (c) does state that such 'information' is confidential and may not be disclosed to any other person except as provided in paragraph.

(7) The register referred to in sub regulation (6) must contain the following particulars in respect of each person who attended the gathering:

(a) the full names of the person; (b) the identification number of the person; (c) the nationality and country of residence or origin of the person; (d) the physical address of the person; (e) the contact telephone or cell phone number of the person; and (f) the email address of the person.

<sup>312</sup>Namibia Access to Information Bill. Available at <<https://www.parliament.na/index.php/archive/category/197-bills-2020?download=8797:access-to-information-bill>> accessed 12 October 2021.

<sup>313</sup> The National Council is the upper chamber of Namibia's bicameral Parliament. It reviews bills passed by the National Assembly and makes recommendations to incorporate regional considerations in the legislation, prior to final clearance by the National Assembly and signature by the President as provided under article 44 of the Namibian Constitution; See Martin Endjala, 'NA passed the access to information bill' Windhoek (Windhoek Observer, 4 October 2022)<<https://www.observer24.com.na/na-passed-the-access-to-information-bill/>> access 20 November 2022.

<sup>314</sup> Charmaine Ngatjiheue, 'Historic access to information bill passed' (The Namibian (Namibia, 22 June 2022) <<https://www.namibian.com.na/6221512/archive-read/Historic-access-to-information-bill-passed>> accessed 20 November 2022.

<sup>315</sup> Center for Democracy and Law, 'Namibia Analysis of the Access to Information Bill' > [https://www.law-democracy.org/live/wp-content/uploads/2021/04/Namibia.RTI\\_.Apr21.final\\_.pdf](https://www.law-democracy.org/live/wp-content/uploads/2021/04/Namibia.RTI_.Apr21.final_.pdf)> accessed 20 November 2022

draft was developed in 2013.<sup>316</sup> It was discussed by the CCL in October 2021 and returned to the MICT for further consultations.<sup>317 318</sup>

When promulgated Namibia's Data Protection Bill will serve as the main law on information privacy in Namibia.<sup>319</sup> Pending the promulgation of the bill, the Information, Communication and Technology Policy of 2008<sup>320</sup> offers policy guidance on information privacy in Namibia.

## **5.2 Data Protection Bill**

### **5.2.1. Terminology and Scope**

As a natural play-off of the drafting process of the bill, which was propelled by the Global Action on Cybercrime Extended (GLACY)+,<sup>321</sup> the language and definitions employed in the bill strongly resembles the EU information privacy legal instruments, particularly Convention 108+ and the GDPR, as evident from the title.<sup>322</sup> The substantive provisions of the bill are a blend of, and analogous to the provisions espoused in the SADC Model Law, Malabo Convention, Convention 108+ and the GDPR. It invariably leans towards an expose of third-generation information privacy principles.

---

<sup>316</sup> Nashilongo Gervasius, 'Data Protection and Privacy In Namibia: an Exploratory Study in the context of Covid-19' (Internet Society of Namibia, 2021) < <https://isocnamibia.org/wp-content/uploads/2021/04/Data-Protection-During-COVID-19-Study-in-Namibia.pdf>> accessed 3 March 2022; Council of Europe, 'GLACY+: Stakeholders' Consultation Workshop on the Data Protection Bill in Namibia' (Council of Europe, 24- 26 FEBRUARY 2020) <<https://www.dataguidance.com/news/international-coe-organises-workshop-draft-data-protection-bill-namibia>> accessed 12 February 2022.

<sup>317</sup> Minutes of Cabinet Committee on Legislation Tuesday, 22 October 2021 certified by Chisom Okafur (CCL Secretary).

<sup>318</sup> Action Access to Information Namibia, Government seeks public input on draft Data Protection Bill (Action Access to Information Namibia, Oct 26, 2022) < Action Access to Information Namibia> accessed 15 November 2022.

<sup>319</sup> The Preamble of the Bill highlights that it aims to protect the fundamental rights and freedoms of individuals, particularly their right to privacy which is protected by Article 13 of the Namibian Constitution.

<sup>320</sup> Available at <[https://www.researchictafrica.net/countries/namibia/NMICT\\_IT\\_Policy\\_2008.pdf](https://www.researchictafrica.net/countries/namibia/NMICT_IT_Policy_2008.pdf)> Information Technology Policy for the Republic of Namibia 2008> accessed 1 January 2022.

<sup>321</sup> The GLACY+ Project (Global Action on Cybercrime Extended), launched in October 2016, is a joint project of the European Union and the Council of Europe. The overall objective of GLACY+ is to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

<sup>322</sup> See the Project Summary <<https://rm.coe.int/3148-glacy-summary-v7/1680a57b61>> accessed 1 March 2022.

There is a strong resemblance between the bill<sup>323</sup> and POPIA. The bill also stipulates requirements for processing 'special categories'<sup>324</sup> (classified as sensitive data in section 1 of POPIA) of personal data and data of children.<sup>325</sup>

### **5.2.2. Exemptions**

Section 15 lists the exemptions from the scope of the bill that mirrors the public policy and competing human rights considerations that are also enumerated in POPIA and the International and Regional Instruments.<sup>326</sup> Save for exempting the processing of personal information for historical research and artistic purposes, the bill contains similar exemptions as those under POPIA.

Notably, the bill entrenches sections 3 (basic principles), 8 (data breach notification), Section 16 (transparency of processing) and Part III (rights of the data subject); consequently, amendments derogating from the aforementioned provisions are not permissible. In addition to entrenching the above-named provisions, section 15 (3)-(6) of the Bill stipulates that public interest exemptions should not be invoked arbitrarily, but must be defined in terms of a law that is not unreasonably broad but should not constitute a blanket prohibition.

### **5.2.3. Basic Principles for Lawful Processing**

Unlike POPIA which lists eight conditions of processing, the Bill lays down five basic principles for the lawful processing of personal information, which although captioned differently are in substance compared to the principles contained in POPIA. These are:

- (1) Fair, transparent and lawful processing;
- (2) Specific legitimate purpose and purpose limitation;
- (3) Data minimisation;
- (4) Accuracy;

---

<sup>323</sup> Section 1.

<sup>324</sup> Section 7(1).

<sup>325</sup>Section 7- revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and personal data relating to criminal offences, including criminal records, may entail risks to data subjects independently of the context of the processing, and is prohibited.

<sup>326</sup> Section of 4 (b) of the POPIA.

(5) Storage limitation.<sup>327</sup>

The Bill frames Accountability and Security as obligations of controllers and processors, independent from the basic principles.<sup>328</sup>

#### 5.2.4. Technical

Astoundingly, the Bill incorporates technical third-generation of Privacy by Default and Design (PbD) and Information Protection Impact Assessments (DPIA) principles,<sup>329</sup> which are not expressly incorporated in POPIA.<sup>330</sup>

PbD is an approach to systems engineering that seeks to ensure protection for the privacy of individuals by integrating considerations of privacy issues design and development stages of products, services, business practices, and physical infrastructures.<sup>331</sup> The PbD framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and the Data Protection Authorities in 2010.

On the other hand, a DPIA is used to identify and analyse personal information privacy risks likely to ensue from the use of a particular technology after which appropriate measures to avert, mitigate or remedy the risks are identified and implemented

#### 5.2.5. Data Subject Rights

Part three<sup>332</sup> of the Bill extends the following entitlements to data subjects:

**(1) The right to know and access:** The data subject has a right to know the identity and address of the controller, the purpose, source and recipients of data processed,

---

<sup>327</sup> Section 3-12. Discussion on the principles on page 19.

<sup>328</sup>Section 18 and 19.

<sup>329</sup>See Felix Bieker et al, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation'; In *4th Annual Privacy Forum Proceedings* (Springer, 2016); Michael Friedewald, *Data Protection Impact Assessments in Practice Experiences from Case Studies* (Springer 2022).

<sup>330</sup>Section 17 and 21 of the Namibian Data Protection Bill.

<sup>331</sup> Ann Cavoukin, 'Privacy by Design Leadership Methods' and result: In Serge Gutwirths and Others eds), *European Data Protection: Coming of Age* (Springer Heidelberg 2013).

<sup>332</sup> Section 8-14.

as well as data exports if applicable and should also be able to request a copy of the personal data processed.<sup>333</sup>

(2) **Right to rectification and erasure:** A data subject is entitled to prompt rectification of erroneous and incomplete processing of personal data or appropriate annotation, at no charge to the data subject. This right also entails the right to demand erasure on the grounds stipulated.

(3) **Right to object to processing:** This right enables a withdrawal of consent at any point and shields data subjects from unsolicited communications. Accordingly, data subjects should as a default opt-in and should be able to opt-out with ease at any given time.

(4) **Right to refuse automated decision-making, including profiling:** This right affords data subjects the right to refuse automated processing of their personal information and profiling and to insist that Controllers must adopt suitable measures for meaningful human intervention in the processing of personal data, particularly in respect of special categories of data.

(5) **Right to obtain assistance from DPA:** Section 25 of the Bill obligates the DPA to assist citizens and non-citizens to uphold their entitlements under the bill.

(6) **Right to be represented:** Even though class actions are not permitted in Namibia,<sup>334</sup> section 13 of the Bill introduces an avenue for data subjects to be represented by organisations or associations in the administrative process in the DPA, as well as extra-judicially.

(6) **Right to compensation:** Data subjects are eligible to claim compensation from controllers and processors, for all patrimonial and non-patrimonial loss suffered on account of information privacy contraventions proscribed in the Bill, under section 14 of the Bill.

---

<sup>333</sup> Section 8(3) provides that; the request must be honored within 30 days.

<sup>334</sup> Diane R Hazel, 'Litigating with class: Considering a potential framework for class actions in Namibia' (2014) 1 (6) Namibia Law Journal, 3; Law Reform and Development Commission of Namibia, 'Project 27: Locus Standi Discussion Paper' <<https://media.namiblii.org/files/na/other/law-reform-report/NALRDC%2027/27%20LRDC%20%20Locus%20Standi%20Discussion%20Paper.pdf>> accessed 14 February 2021.



(7) **Right of recourse to judicial authority:** The Bill also stipulates that data subjects are entitled to bring the decision of the DPA under review and or to appeal against its findings to a competent judicial body, should they be aggrieved. In addition, data subjects retain the right to seek judicial remedies for information privacy infringements.

### **5.2.6. Institutional Arrangements**

Part seven of the Bill envisage the creation of a competent independent<sup>335</sup> DPA responsible to implement and enforce the Act.

To clear out any doubt concerning the legal classification and relationship of information privacy and privacy, the Bill commendably stipulates that the DPA must deal with the right to information privacy, as a human right.<sup>336</sup>

To foster institutional and functional independence, section 28(4) of the Bill restricts the appointment of members who are attached to the government and or any of its agencies. As a way to strengthen its independence, sections 27(1) and 4 of the Bill emphasise that the DPA must be provided with the necessary resources to appoint staff with ICT expertise to ensure the effective execution of its functions.

The Bill sets out the functions and powers of the DPA, similar to that of POPIA.<sup>337</sup> Remarkably, section 34 stipulates that the DPA must be consulted before administrative and legislative proposals which have an impact on personal data protection are adopted. I am of the view that the insistence that the DPA consulted before adopting administrative and legislative measures that have a bearing on information privacy, will foster pro-information privacy policies and laws and the development of an information privacy-conscious legal and policy environment.<sup>338</sup>

---

<sup>335</sup> Section 26.

<sup>336</sup>Section 25.

<sup>337</sup> Section 33.

<sup>338</sup>Section 34 and 34.

### **5.2.7. Enforcements, Administrative Fines and Penalties**

When promulgated, the enforcement of the Act will be backed up with the imposition of *inter alia* administrative fines, bans, suspensions or cancellation of processing orders, and formal notices.<sup>339</sup>

Even though at present not quantified, the Bill provides for the imposition of penalties and fines for contraventions of the Act.<sup>340</sup>

### **5.2.8 Data Export**

Similar to Article 24(1) of the GDPR, section 24 of the Bill permits cross-border transfers to jurisdictions that afford a suitable level of information privacy protection.

### **5.2.9. International Cooperation**

Underscoring the aptness of participating in international cooperation schemes, section 36 of the Bill authorise the DPA to participate in international information privacy cooperation schemes.

## **6. Chapter Conclusion**

This chapter analysed the legislative framework on information privacy in RSA and the prospective Namibian Data Protection Bill. It is evident that at their core, and despite their gradations and generational relativity, the substantive provisions of POPIA and the Bill share strong commonalities and are substantively aligned with the relevant national, regional and international information privacy protection legal instruments.

I notice, however, that whilst information privacy principles contained in the POPIA and the Bill are broadly similar, there are a variety of mechanisms informed by their respective domestic realities, adopted for implementing and enforcing these principles.

From a substantive perspective, both the POPIA and Bill meet the constitutional imperatives.<sup>341</sup> It is commendable that the Bill reflects third-generation information

---

<sup>339</sup>Section 35.

<sup>340</sup> Section 38.

<sup>341</sup>Pria Chetty and Alon Alkalay, 'Namibia': In Koliwe Majama, Janny Montinat and Anriette Esterhuysen (Coordinators), *Privacy and Personal Data Protection in Africa: A Rights- based Survey of*

privacy principles which at present offer the most updated degree of information privacy protection.

In light of the limited jurisprudence on the efficiency of POPIA at this juncture, I stand guided by scholarly assessments by renowned information privacy specialists like Roos, who following an evaluation of the POPIA against the GDPR with reference to its substantive content concluded that the POPIA offers information privacy protection equivalent to the GDPR. She however acknowledges minor shortcomings under POPIA and advances seven commendations to bring the POPIA on par with the GDPR.<sup>342</sup>

In the same vein, Warikandwa also concluded that the POPIA is only marginally different from the GDPR and that it offers sufficient information privacy protection within the financial service market.<sup>343</sup> Gastrow and Adams also concluded that there are both 'areas of alignment and misalignment' between the POPIA and the GDPR<sup>344</sup>

Owing to the above, I am inclined to conclude that, both the POPIA and the Bill are effective information privacy law frameworks and can thus be employed as a yardstick to assess the extent to which the drone regulations in RSA and Namibia are information privacy responsive.

---

*Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021) 117; Juliet Nanfuka, 'Data Privacy Still a neglected digital right in Africa' (Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Jan 27, 2022) <<https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/>> accessed 27 January 2022.

<sup>342</sup>Anneliese Roos, 'Data privacy law': In Van der Merwe et al, *Information and Communications Technology Law* (3rd ed, 2021) 478; Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South Africa Data Privacy Law: An Evaluation (2020) 3 (53) Comparative and International Law Journal of South Africa 7985.

<sup>343</sup> Tapiwa V Warikandwa, 'Personal Data Security in South Africa' s Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared' (2021) 24 Potchefstroom Electronic Law Journal, 1-32 <<https://doi.org/10.17159/1727-3781/2021/v24i0a10727>> accessed 10 October 2022.

<sup>344</sup> Michael Gastrow and Rachel Adams, 'Digitalisation in Science and Technology Policy Engagement, Alignment, and Misalignment Between the European Union and South African Data Protection and Privacy Frameworks': In Chux Daniels, Benedikt Erforth and Chloe Teevan (eds), *Africa-Europe Cooperation and Digital Transformation* (Routledge, 2022) 162- 164.

Furthermore, it is safe to conclude that the civil aviation regulators in the jurisdictions under discussion have a constitutional duty and legislative mandate to take accountability for information privacy in the course of regulating drones.

In the next chapter, I will analyse the regulations governing drones, to determine the degree to which it heeds the information privacy principles enumerated in the laws discussed in this Chapter.

## Chapter Four

# Applying Information Privacy Protection Principles to Drone Laws in RSA and Namibia

---

*This chapter canvass the drone-specific laws in RSA and Namibia to determine the extent to which they are consistent with the information privacy principles, particularly the stipulations in the POPI and the Namibian Data Protection Bill. It also explores the extent to which these laws can be purposed to protect data subjects from the unlawful processing of their personal information by civilian drones.*

### 1. Introduction

The Chicago Convention is the Magna carter of Aviation Law.<sup>345</sup> aviation law. the deployment of mediums of navigation (aircrafts and drones and air balloons), air travel, airport operations including aircraft navigation and maintenance, air traffic control, aviation safety, security, and personnel and operator authorisation requirements, as well as associated legal and business issues.<sup>346</sup>

The fundamental principle of aviation law is territorial sovereignty.<sup>347</sup> In terms of Article 2 of the Chicago Convention, a state has unrestricted exclusive rights over its super-incumbent air space. Consequently, the consent of every state is necessary for the flight through and or in its air space.<sup>348</sup> The airspace of a state is determined with reference to Article 2 of the Chicago Convention, read with Article 55 of the United Nations Convention on the Law of the Sea (UNCLOS).<sup>349</sup>

---

<sup>345</sup> Louis Haeck, 'Military Aircraft and International Law: Chicago Opus 3' (2001) 66 (3) Journal of Air Law and Commerce 885; Jeffrey Klang, 'Celebrating the Chicago Convention's 75th Anniversary' (2019) 32 (4) The Air Space & Space Lawyer (Special Issue).

<sup>346</sup> David McClean et al, *Shawcross and Beaumont: Air Law* (4th ed, Issue 179, LexisNexis 2022) 28.

<sup>346</sup> Article 1 of the Chicago Convention.

<sup>348</sup> According to Article 2 of the Chicago Convention, territory is deemed to be "land areas and territorial waters only". However, Article 55 of the Law of the Sea Convention 1982, provides that the Exclusive Economic Zone (EEZ), does not form part of the territorial waters. Article 87 (1) (b) of 1982 United Nations Convention on the Law of the Sea (UNCLOS) also stipulates for 'freedom of over flight of the the airspace above the high seas; I H Philepina Diederiks-Verschoor; Isabella Henrietta Philepina and M A Butler, *An Introduction to Air Law* (8th [revised] edition, Kluwer 2012).

<sup>349</sup> United Nations Convention on the Law of the Sea adopted on Dec. 10, 1982, Montego Bay, Jamaica, 3rd UN Conference on the Law of the Sea [1833 U.N.T.S. 397,21 ILN 1261 (1982) Doc 7300/8.

It is against the foregoing international framework that the civil aviation authorities in RSA (SACAA) and Namibia (NACAA) exercise regulatory oversight in respect of civilian drones operated within their respective territories.

Heeding the challenge set in the ICAO Business Plan<sup>350</sup> to fully integrate drones within the international civil aviation industry by the year 2023 and to fully integrate 4D trajectory-based drone operations by the year 2028.<sup>351</sup> The RSA and Namibia promulgated regulations on drones guided by the ICAO Manual on Remote Pilot Aircraft Systems (Document 10019).<sup>352</sup>

This dissertation is built on the conclusions reached by Samantha Huneberg<sup>353</sup> and Nomalanga Mashinini<sup>354</sup> that the South African drone regulations are in want of an information privacy facelift.

In what follows, I will offer a synopsis of the drone regulations that have a bearing on information privacy within the RSA and Namibia and make recommendations on how these regulations can be purposed to align with the information privacy requirements of the laws discussed in the preceding chapter.

I anticipate that this academic enquiry will offer perspective on the policies and strategies which can be employed to extend greater protection to the right to information privacy, espoused under section 14 and article 13 of the RSA and Namibian Constitutions, as well as the minimum conditions of processing personal information stipulated under POPIA and the Data Protection Bill.

## **2. Policy, Legal and Institutional Framework**

### **2.1. RSA**

---

<sup>350</sup> Available at < <https://www.icao.int/Meetings/a41/Documents/ICAO%20Business%20Plan%202023-2025%20V1.0%2025%20July%202022.pdf> > accessed 11 November 2022; See also ICAO Business Plan 2023-accessed 11 November 2022.

<sup>351</sup> ICAO, 'RPAS 2022 Symposium Event Directory 7-9 November 2022' (Not supplied) < [https://www.icao.int/Meetings/RPAS2022/Documents/RPAS%202022%20-%20EventDirectory%20\(3\).pdf](https://www.icao.int/Meetings/RPAS2022/Documents/RPAS%202022%20-%20EventDirectory%20(3).pdf) > accessed 12 December 2022.  
Samantha Huneberg, 'The rise of drone: Privacy concerns' 2018 (81) THRHR 263.  
' (ICAO, 2015). Available at <<https://skybrary.aero/sites/default/files/bookshelf/4053.pdf>> accessed 14 February 2022.

<sup>353</sup> Samantha Huneberg, 'The rise of drone: Privacy concerns' 2018 (81) THRHR 263.

<sup>354</sup> Nomalanga Mashinini, 'The processing of personal information using remotely piloted aircraft systems in South Africa' [2020] De Jure Law Journal 140.

Section 2 of the Civil Aviation Act<sup>355</sup>(CAA) authorise the South African Civil Aviation Authority (SACAA) to exercise supervisory oversight over civil aviation safety and security in the RSA. The SACAA is a juristic person established in terms of section 71 of the CAA and a Schedule 3A national public entity<sup>356</sup> under the Public Finance Management Act.<sup>357</sup>

Section 73 and 163 of the CAA mandates the department of transport and the SACAA to develop regulations, technical standards, guidance materials and circulars aligned with the CAA and the Chicago Convention and to implement, monitor and enforce compliance.

The strategic and policy development functions of the SACAA vest in its Board of Directors (the Board)<sup>358</sup> which are appointed by the Minister of Transport. The Board is chaired by the director of the SACAA and is ultimately individually and collectively answerable to the Minister of Transport.<sup>359</sup> The SACAA's operational responsibilities are borne by the executive management, headed by the director alongside the other staff appointed in terms of the CAA.<sup>360</sup>

All civil aviation laws are informed by the revised 2017 white paper: national policy on civil aviation.<sup>361</sup> From a cursory glance, the overall legislative framework of the CAA evidences a commitment to safety and security and a limited extent environmental protection.<sup>362</sup>

Drones are regulated by the Eighth Amendment of the Civil Aviation Regulations, 2015 (SACARs)<sup>363</sup> promulgated under section 155 of the CAA.<sup>364</sup>These Regulations are

---

<sup>355</sup> No 13 of 2009.

<sup>356</sup> Section 75 and 77 of the CAA. The entities under Schedule 3 do not have an industry / sector specific supervisory body that oversees their governance and are required to report directly to the Financial Intelligence Centre <<https://nationalgovernment.co.za/units/type/6/public-entity>> accessed 1 March 2022.

<sup>357</sup> Act No.1 of 1999. Available at < <https://www.gov.za/documents/public-finance-management-act#:~:text=to%20regulate%20financial%20management%20in,management%20in%20that%20government%3B%20and>>

<sup>358</sup> The Board comprises seven (7) non-executive members and one Executive Director, being the Director of Civil Aviation, all of whom are appointed by the Minister of Transport. in September 2019.

<sup>359</sup> Section 100 of the CAA.

<sup>360</sup> Section 85 of the CAA.

<sup>361</sup> Available at <[https://www.gov.za/sites/default/files/gcis\\_document/201705/40847gen401.pdf](https://www.gov.za/sites/default/files/gcis_document/201705/40847gen401.pdf)> accessed 10 March 2022.

<sup>362</sup> Section 72 of the CAA.

<sup>363</sup> Part 101 Remotely Piloted Aircraft Systems, 2015 Government Notice 444 of 27 May 2015. (As amended by GNR 40376 of 28 October 2016, GNR 432 of 19 May 2017 (w.e.f. 21 June 2017) and GNR.1503 of 15 November 2021.

<sup>364</sup> Section 73 and 163 of the CAA mandates the department of transport and the SACAA to develop regulations, technical standards, guidance materials and circulars.

supplemented by the Civil Aviation Technical Standards (SA-CATS)<sup>365</sup> and the Aeronautical Information Circulars (AICs), adopted in terms of section 163 of CAA. The SACARs regulate the safety, security (and privacy concerns)<sup>367</sup> of drone operations.<sup>368</sup>

## 2.2. Namibia

The Namibian Civil Aviation Authority (NACAA) is a state-owned enterprise constituted under the Namibian Civil Aviation Act, 6 of 2016 (NCAA).<sup>369</sup> It holds similar a composition, strategic and operational structure, as its RSA counterpart.<sup>370</sup>

In terms of sections 9 and 10 of the NCAA, the NACAA is responsible to oversee aviation safety and security in Namibia, in accordance with the NCAA and the Chicago Convention.

The Minister of Works and Transport (MOWT) is authorised to pass regulations on any matter necessary and expedient to achieve the objectives of the NCAA and to incorporate standards and best practices recommended by ICAO into the regulations, by reference in terms of section 54 of the NCAA.

The regulations governing drones in Namibia are delimited in Part 101: Rules of the Air and General Operating Rules: Operation of Remotely Piloted Aircrafts' (NAMCARs) under the set of regulations passed under the NACAA.<sup>371</sup>

## 3. Selected Substantive CARS with Information Privacy Implications

---

<sup>365</sup> SA-CATS 101 (date of operation, July 1, 2015)  
<<http://www.caa.co.za/Legal%20Documents/SA-CATS%20101%20approval.pdf>, archived at <https://perma.cc/2FR4-ST74>> accessed 1 April 2022.

<sup>367</sup> The only reference to information privacy is under 101.01.7 of the SA-CATS 101. Available at <[caa.mylexis.co.za](http://caa.mylexis.co.za)> accessed 12 April 2022.

<sup>368</sup> Manana Wanyonyi Edison Rodgers, 'Integration of Unmanned Aircraft Systems into Civil Aviation: A Study of the U.S, South Africa And Kenya' (Phd Thesis, University of South Africa 2020).

<sup>369</sup> Act No. 6 of 2016. The NACAA was formerly a Department DCA (Directorate of Civil Aviation) within the Ministry of Works and Transport answerable to the Minister of Works and Transport.

<sup>370</sup> Part 3- 5 of the NCAA.

<sup>371</sup> Government Gazette No. 7157 of 27 March 2020. Available at <<http://www.ncaa.com.na/index.php/documents/primary-legislation/government-gazettes/5-materia-juridica/25-government-gazettes/171-gaz-7157?tmpl=component>> accessed 28 April 2022.



The substantive provisions of the SACARS,<sup>372</sup> except for the provisions on import, manufacturing, assembly,<sup>373</sup> and restrictions on the use of RPA's and RPA systems with infrared imaging technology equipment,<sup>374</sup> are substantially similar to the NAMCARs.<sup>375</sup>

Owing to the above and to avoid repetition, only the SACARS will be fully referenced in this discussion, however, the discussion is putative of the corresponding provisions of the NAMCARs, unless expressly stated otherwise.<sup>376</sup>

### 3.1 Design and Manufacture

#### SCARs

Notwithstanding, the fact that manufacturers are identified as crucial stakeholders and the design and manufacturing stages of drones are said to be crucial stages in achieving optimal information privacy protection.<sup>377</sup>

Additionally, whilst there are several drone manufacturers in RSA,<sup>378</sup> the SACARs are silent on the obligations of drone manufacturers and the manufacturing specifications of drones.<sup>379</sup>

---

<sup>372</sup> Eight Amendment to the 2001 Civil Aviation Regulations: Part 101 Remotely Piloted Aircraft Systems (as amended by Government Notice 40376 of 28 October 2016, Government Notice 432 of 19 May 2017 (w.e.f. 21 June 2017) and GNR.1503 of 15 November 2021).

<sup>373</sup> NAMCAR's: Subpart 4 (Other requirements relating to RPA and RPA Systems).

<sup>374</sup> NAMCAR's: Part 101.05.4 (4)-(7).

<sup>375</sup> NAMCARs Part 101 Government Gazette No 7157 of 27 March 2020.

<sup>376</sup> This paper does not aspire to offer a detailed summary of all CARs. Going forward this paper will only highlight the provisions of SACARs with information privacy implications.

<sup>377</sup> Bharat Rao, Ashwin Goutham Gopi and Maione, Romana, 'The societal impact of commercial drones' (2016) 45 *Technology in Society* 83-90 <10.1016/j.techsoc.2016.02.009>; DroneRules.eu PRO, 'Privacy-By-Design Guide a Dronerules.EU PRO Resource for Drone Manufacturers' <[https://dronerules.eu/assets/files/DRPRO\\_Privacy\\_by\\_Design\\_Guide\\_EN.pdf](https://dronerules.eu/assets/files/DRPRO_Privacy_by_Design_Guide_EN.pdf)> accessed 21 December 2022.

<sup>378</sup> Bhavna Deonarain, 'Technological Change and Sustainable Mobility: An Overview of Global Trends and South African Developments' (Trade & Industrial Policy Strategies (TIPS), March 2019) <[http://www.thedtic.gov.za/wpcontent/uploads/Technological\\_change\\_and\\_sustainable\\_mobility\\_.pdf](http://www.thedtic.gov.za/wpcontent/uploads/Technological_change_and_sustainable_mobility_.pdf)> accessed 10 January 2022; See also 'Drone Startups in South Africa' (Tracxn, October 23, 2022) <<https://tracxn.com/explore/Drones-Startups-in-South-Africa>> accessed 21 November 2022.

<sup>379</sup> Eleonora Bassi, 'From Here to 2023: Civil Drones Operations and the Setting of New Legal Rules for the European Single Sky' [2020] *Journal of Intelligent & Robotic Systems* <10.1007/s10846-020-01185-1> accessed 12 March 2022; Timothy Ravich, 'A global analysis of drone laws: best practices and policies': In Bart Custers (ed), *The future of Drone Use* (TMC Asser Press 2016) 302; Dale T McKinley, 'New Terrains of Privacy in South Africa: Biometrics/Smart Identification Systems, CCTV/AIPR, Drones, Mandatory SIM Card Registration and FICA' (Produced as part of a collaborative research project between the Right2Know Campaign and the Media Policy & Democracy Project)>

## NAMCARs

Although the NAMCARs ponders manufacturing, sub-part 4 of the NAMCARs regrettably addresses the import and export, assembly and testing of drones<sup>380</sup> with a solitary focus on ensuring the observance of customs and excise duties.<sup>381</sup>

The NAMCARs further provides that, the manufacturing, assembling, modification and testing should comply with the requirements of the drone's state of origin and or the stipulations that may be issued by the director of the NACAA.<sup>382</sup>

Thoughtful that the 3<sup>rd</sup> generation of information privacy principles emphasise on adherence to PbD, as propounded by Ann Couvoukin.<sup>384</sup> The PbD principle acknowledges that laws and policies alone are insufficient to curtail the unlawful processing of personal information and therefore stresses the addition of Privacy Enhancing Technologies (PETs)<sup>385</sup> at the design and manufacturing stage(s) in order to build-in information privacy by default and mitigate information privacy concerns associated with emerging technologies, in this instance drones.<sup>386</sup>

---

<http://www.mediaanddemocracy.com/> accessed 1 February 2022.

<sup>380</sup> NAMCAR's: Part 101.04.1.

<sup>381</sup> N Khyanyile, 'Fun with a Warning' (News24, South Africa) <<https://www.news24.com/SouthAfrica/News/fun-with-a-warning-20190204-2>> accessed 4 January 2022.

<sup>382</sup> NAMCAR's: Part 101.04.1.

<sup>384</sup> Peter Hustinx, 'Privacy by Design: Delivering the Promises' (2010)3(2) *Identity in the Information Society* 253-255; Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosystem* (Office of the Privacy Commissioner, 2012) 16; See also John Nwachukwu Okoye, 'Privacy by Design' (Master's Thesis, Norwegian University of Science and Technology 2017); Ann Cavoukian and Nandini Jolly, 'Embedding privacy and security to gain a competitive advantage' (2018) 1 (4) *Journal of Data Protection & Privacy* 400-409.

<sup>385</sup> Lee-Andrew Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105-120 ; L Jasmontaite et al, 'Data Protection By Design and by Default: Framing Guiding Principles Into Legal Obligations in the GDPR' (2018) 4 *European Data Protection Law Review* 168, 189; Dale T. McKinley, 'New Terrains of Privacy in South Africa'(December 2016) <<http://www.mediaanddemocracy.com/>> accessed 2 January 2022.

<sup>386</sup> Ottavo Marzocchi, 'Privacy and Data Protection Implications of the Civil Use of Drones' (Brussels, Belgium, 2015) <<https://free-group.eu/2015/06/12/privacy-and-data-protection-implications-of-the-civil-use-of-drones/>> accessed on 16 January 2017; Joseph Suh, 'Drones: How They Work, Applications, and Legal Issues'[2019] *Georgia Law Technology. Review* 502 <<https://georgetownlawtechreview.org/wpcontent/uploads/2019/05/3.1-Suh-pp-502-514c.pdf>> accessed 21 March 2022.

<sup>386</sup> Marc Jonathan Blitz et al, 'Regulating Drones Under the First and Fourth Amendments Regulating Drones Under the First and Fourth Amendments' (2015) 57 (1) *William & Mary Law Review* 49 < <https://scholarship.law.wm.edu/wmlr/vol57/iss1/3> > accessed 1 March 2022.

Couvoukin recommends seven foundational principles of PbD that offers guidance in respect of the practical implication of the PbD principle.<sup>387</sup> Manufacturers are generally advised to contemplate information privacy in respect of drone hardware and software.<sup>388</sup>

Drones.PRO suggests among others that information privacy in drones can be enhanced by designating cameras visibly, and by enabling payload feedback,<sup>389</sup> ensuring automated data minimisation and incorporating programmed flight activity logs functionality.<sup>390</sup>

Common PETs advocated for in respect of drones include geofencing technology which includes configuring drones with a list of no fly Global Positioning Systems (GPS) coordinates in respect of areas prone to processing of personal information.<sup>391</sup> In the case of POPIA, these areas would primarily be those where there is a high likelihood to process information outlawed in terms of sections 26 and 34 of the POPIA, such as churches, political parties or trade union headquarters or events, health facilities, schools, playgrounds courts, correctional facilities, etc.<sup>393</sup>

Another strategy is through the design of flight maps which enables drone operators to choose less personal information intrusive routes to minimise the unlawful processing of personal information.<sup>394</sup>

---

<sup>387</sup> Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner, Ontario, Canada, January 2011) < <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>>. accessed 1 April 2022

<sup>388</sup> For example, drawing attention to them through bright colours surrounding a camera lens.

<sup>389</sup> The payload sensors will flicker or changing colour when payloads processing personal information are engaged.

<sup>390</sup> To ensure accountability of drone pilots and operators, this functionality will store operational data such as time-stamps, geo-fencing uploads or of the flight paths and when payload sensors engagement.

<sup>391</sup> Especially sensitive information and children of children information.

<sup>393</sup> Murison, Malek. 'ISO Proposes Global Drone Standards' (DRONELIFE, 22 Nov 2018) <[dronelife.com/2018/11/22/iso-proposes-global-drone-standards/](https://dronelife.com/2018/11/22/iso-proposes-global-drone-standards/)> 1 January 2022; Joshi Divya, 'Here Are the World's Largest Drone Companies and Manufacturers to Watch and Invest' (Business Insider, 18 July 2017) <[www.businessinsider.com/top-drone-manufacturers-companies-invest-stocks2017-07](https://www.businessinsider.com/top-drone-manufacturers-companies-invest-stocks2017-07)>. 2> accessed 2022.

<sup>394</sup> Eleonora Bassi et al, 'The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win-Win Approach to Data Protection, Aerospace Engineering, and Risk Management' (2019)9(4) *Minds and Machines* 579; Eleonora Bassi, 'Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance' (2020) *Law in Context. A Socio-legal Journal* <<https://doi.org/10.26826/law-in-conte>> accessed 20 April 2022.

In addition to the PETs, the CAA is also free to approach the South African Bureau of Standards (SABS)<sup>395</sup> to initiate a process to adopt pro-information privacy compulsory specifications (national standards) under the Standards Act<sup>396</sup> to which all drones imported, exported manufactured and assembled and sold in RSA should conform.

### 3.2. Import and Export

Save for the stipulations of subpart 4 of the NAMCARS that concentrate on the observance of customs and excise duties when importing and exporting drones, there are similarly no specific rules regarding the importation and exportation of drones.<sup>398</sup>

A drone itself may contain a range of personal (sensitive) information about the user of the drone, its mission profile, client data and other sensitive business information and the personal information of others collected during previous operations.<sup>399</sup> It should be appreciated that the importation and exportation of drones to and from various states invariably occasion the extra-territorial transfer of personal information. The SACARs should therefore address the import and export of drones within the context of section 72 of POPIA.

Section 72 confines the transfer of personal information to foreign jurisdictions that have laws, to institutions that organisations that ascribe to binding corporate rules that offer comparable information privacy protections or if consent was obtained for such transfer, or if the transfer is effected to fulfil a contractual undertaking or is for the benefit of the data subject.<sup>400</sup>

In light of the safeguards imposed under the POPIA in respect of the cross-border transfer of personal information, there is a need to extend the application of the SACARs

---

<sup>395</sup> The SABS is mandated to: develop, promote and maintain South African National Standards (SANS); promote quality in connection with commodities, products and services; and render conformity assessment services and assist in matters connected therewith.

<sup>396</sup> Act No 8 of 2008.

<sup>398</sup> NAMCARS: Part 101.04.1.

<sup>399</sup> Christian Pauletto, 'Options towards a global standard for the protection of individuals with regard to the processing of personal data' (2021) 40 Computer Law & Security Review 105433.

<sup>400</sup> Sizwe Snail Ka Mtuze and Lebogang Stroom-Nzama, 'GDPR – oriented privacy laws in South Africa and Mauritius' (PowerPoint Presentation, WEBINAR, 22 APRIL 2021) <<https://www.privacylaws.com/media/3449/southafrica.pdf>> accessed 28 November 2022.

to minimise the risk of incidental or intentional unauthorised processing of personal information when drones are imported and exported trans-nationally.

This consequence should also be borne in mind when dealing with the request for drone operations that commence in RSA, but end in another jurisdiction and *vice versa*.

### **3.3. Sale and Labelling**

SACARs Part 101.01.05 renders it unlawful for retailers to sell or resell a drone unless its packaging bears a notice stipulating that, the use of drones is subject to the SACARs and the oversight of the SACAA.<sup>401</sup>

Even though, this provision represents a creditable attempt to infuse the principle of accountability projected under section 8 of the POPIA. Yet, owing to many variables this notice by itself offers no guarantee of compliance with the law or safeguard that the unlawful processing of personal information by drones will be averted.

I, therefore, support Huneburg<sup>402</sup> who propounds that instead of mere notice, mandatory registration with SACAA at the point of sale, should be a prerequisite to acquiring ownership of a drone in RSA. Additionally, I propose that this notice must likewise inform drone operators of their duty to comply with the POPIA. This will enable greater transparency and accountability and improve information privacy enforcement.

With regard to the authorisation to own and or operate a drone, SA-CATS101.0.2.4. prescribes that all drones must bear their registration marks on an identification plate affixed to it or must be ingrained on the drone. The SA-CATS specifies the colour(s), fonts and location of these marks.<sup>404</sup>

In light of sections 5(b) and 18 of the POPIA which insist on transparency in processing personal information.<sup>405</sup> It is my opinion that the labelling requirements should be revised to ensure that the identity, contact details and registered business address of

---

<sup>401</sup> Exact wording of notice is prescribed in SA-CATS101.

<sup>402</sup> Samantha Huneberg, 'The rise of drone: Privacy concerns' 2018 (81) THRHR 263.

<sup>404</sup> SA-CATS, Part 101.02.4. 129 SA-CATS, Part 101.02.4. 2 (1) (a)-(d).

<sup>405</sup> Corresponding Sections 23 and 16 of the Bill.

the drone owner or operator are easily attainable, to enable aggrieved data subjects to pursue their rights under the POPIA.

Given the ubiquity of drones, it may be necessary to further impose that drones should be endowed with either a broadcast or network-centred remote identification through which all persons in the vicinity of the tower where a drone is (or will be) operating, will be notified of its presence whilst at the same time protecting the personal information of the operator.<sup>406</sup>

### 3.4. Technical Classifications of Drones

The SA-CATS 101 clusters drones according to their line-of-sight energy (kJ), height (feet) and maximum take-off mass (MTOM).<sup>407</sup> Resultantly drones are grouped as either Class 1 or Class 2 drones. Class 1A (less than 1.5 kilograms (kg) and Class 1B (less than 7 kg) and Class 1C. Class 2 consists of Class 2A Done (less than 20 kg).<sup>408</sup>

### **NAMCARs**

NAMCAR's: Part 101.02.1(1) groups drones into three categories. Category I (recreational) drone operations are those for essentially personal resolves (excluding public sporting and academic research) undertaken on a casual basis within the boundaries of private property and which do not result in any pecuniary gain.

NAMCARs Part 101.02.1 (2) propositions a unique definition for recreational drone operations. It stipulates that for purposes of NAMCARs:

---

<sup>406</sup> Ahmed Alamouri, Astrid Lampert and Markus Gerke, 'An Exploratory Investigation of UAS Regulations in Europe and the Impact on Effective Use and Economic Potential'(2021) 5 MDPI Drones 63 <<https://doi.org/10.3390/drones5030063>> accessed 14 February 2022; K Kirthan Shenoy and Divya Tyagi, 'Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky' (2022) 9 (1) International Journal of Aviation, Aeronautics, and Aerospace < <https://commons.erau.edu/ijaaa/vol9/iss1/7>> accessed 1 March 2022.

<sup>406</sup> Section 23, 24 99 of the POPIA.

<sup>407</sup> Quintin Mokoena and Others, 'Development of a framework for improving the turnaround time of the application process at the South African Civil Aviation Authority' (2022) 8(8) Heliyon 10075 < [doi: 10.1016/j.heliyon.2022.e10075](https://doi.org/10.1016/j.heliyon.2022.e10075)> accessed 22 December 2022.

<sup>408</sup> Remotely Piloted Aircraft Systems Part (Part 101) Regulations Workshops, (South African Civil Aviation Authority) < <http://www.caa.co.za/.../Part%20101%20-%20RPAS>> accessed 12 January 2021.

a drone operation qualifies as recreational, if it is a self-propelled<sup>409</sup> drone with a gross weight of fewer than 250 grams, which is incapable to carry any payload and has no camera or similar recording functionality and is operated below 120m (above ground level) and 5m from the operator, at a speed not exceeding 10 knots.

Even though, I am sceptical that there would be any justification or business sense to produce the drone envisaged above, this classification of a recreational drone is pro information privacy protection, in that it alleviates the opportunity that a recreational drone can offend the information privacy of others.<sup>410</sup>

Category II (sports, recreational and research operations) includes recreational operations that take place outside the confines of the private property of the operator and in excess of the height and Visual Line of Sight (VLOS) applicable to recreational drones, undertaken exclusively for sports, academic research, organised leisure, and tourism purposes or in relation to competitions provided no economic benefit accrues from it.

Category III (commercial) includes all drone operations with a commercial objective or purpose, or that results in economic benefit.

Research appraises that drones of any size are capable of carrying a payload that can capture personal information; the size of the drone, therefore, has no bearing on the information privacy risk a particular drone poses.<sup>411</sup>

---

<sup>409</sup> Not powered by a fuel system.

<sup>410</sup> Jones Ingham et al, 'Consideration for UAV design and Operation in South African airspace' (2006) 11 *The Aeronautical Journal* 23; Ann Cavoukian, 'Staying one step ahead of the GDPR: Embed privacy and security by design' (2018) 2 (2) *Cyber Security: A Peer-Reviewed Journal* 173-180; Alvarado, 'Drone Industry Barometer 2021' (Drone Industry Insights, September 13, 2021) <<https://droneii.com/project/drone-industry-barometer>> accessed 14 February 2022.

<sup>411</sup> David Goldberg, 'Dronalism: Journalism, Remotely Piloted Aircraft, Law and Regulation' (2015) 10 *Florida International University College of Law* 405. <<https://ecollections.law.fiu.edu/lawreview/vol10/iss2/8>> accessed 20 March 2022; Samantha Huneburg, 'The Rise of the Drone: Privacy concerns' [2017] *THRHR* 586; Joseph Suh, 'Drones: How They Work, Applications, and Legal Issues' [2019] *Georgia Law Technology Review* 502 <<https://georgetownlawtechreview.org/wpcontent/uploads/2019/05/3.1-Suh-pp-502-514c.pdf>> accessed 21 March 2022; Nomalanga Mashinini, 'The processing of personal information using remotely piloted aircraft systems in South Africa' [2020] *De Jure Law Journal* 140; K Kirthan Shenoy and Divya Tyagi, 'Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky' (2022) 9(1) *International Journal of Aviation, Aeronautics, and Aerospace* <<https://commons.erau.edu/ijaaa/vol9/iss1/7>> accessed 1 April 2022; Rodgers Wanyonyi Manana and Nelson Otieno, 'Drones Operations in Kenya: Perspectives on Privacy Challenges and Prospects' (2022) 47 (1) *Air and Space Law* 75-92

Given the constitutional<sup>413</sup> requirement under section 36<sup>414</sup> of the RSA Constitution of reasonableness, necessity, and proportionality, as dissected in the *S v Manamela & Another (Director-General of Justice Intervening)*<sup>417</sup> judgment, wherein it was held that as a general rule, the more serious the impact of the measure on a constitutional right, the more persuasive or compelling the justification for the interference must be.

For this reason, the SACARs will do well to classify drones with reference to the information privacy intrusiveness of the payloads a particular drone is embedded with.

Consequently, SACARs must consider imposing usage restrictions, so that extensively information privacy-intrusive technology payloads, like biometric technology, should only be employed in instances where it is reasonable, necessary and proportional to do so.<sup>418</sup> A good example of usage restrictions as set out in NAMCAR's: Part 101.05.4 (6), which reserves the use of drones with infrared or other similar thermal imaging technology equipment, exclusively for firefighting, law enforcement, scientific research, investigation of forests, estate management, crop and livestock farming operations and earth observation purposes.

### **3.5. Private (Recreational) Drone Operations**

#### **3.5.1. SACARS**

---

<sup>413</sup> Stu Woolman and Henk Botha, 'Limitations': In Theunis Roux and Michael Bishop (eds), *Constitutional Law of South Africa* (2<sup>nd</sup> ed, Juta 2008) 136.

<sup>414</sup> **Limitations**

(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including

- (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
- (e) less restrictive means to achieve the purpose.

(2) Except as provided for in subsection (1) or any other provision of this Constitution, no law shall limit any right entrenched in the Bill of Rights.

<sup>417</sup> 2000 (3) SA 1 (CC), 2000 (5) BCLR 491 (CC).

<sup>418</sup> Anna Popowicz Pazdej, 'The proportionality principle in privacy and data protection law'; (2021) 4(3) *Journal of Data Protection & Privacy*, 322-331.



The SACARs restrict private operations to Class 1A RPA (less than 1.5 kilograms in weight) or Class-1B RPA (less than 7 kilograms in weight) drones.<sup>419</sup> Drone operations are classified as private if the operations take place within and on private property or on property on which an operator has the necessary permission to fly and from which no commercial benefit ensues.<sup>420</sup>

There is no obligation to apply for approval to use or operate, register or undergo any form of training, to undertake private drone operations.<sup>421</sup>

Private Operations are additionally excused from observing the rules on the conveyance of dangerous goods, putting in place safety management systems and remedial action plans (for instance, ensuring that an RPA is in a 'fit-to-fly condition'), as well as from the duty to keep flight logbooks.

The compliance obligations of private drone operations are exclusively self-regulated<sup>422</sup> and are limited to the following:

- **Aerodromes** – refraining from flying 10km within airport, helipad or airstrip;
- **Weather Conditions** – operating during the day and when the weather conditions do not hamper visibility;
- **Intoxication** – refraining from operating drones while under the influence of a psychotic substance or within 8 hours of consumption;
- **Limiting the drone operation to the Restricted Visual Line-of-Sight<sup>423</sup> (R-VLOS)**; limiting the operations to a maximum distance of 500 metres from the pilot

---

<sup>419</sup> SACARS: Part 101.01.2(1)-(3) and 101.05.10.

<sup>420</sup> CR Burger and T Jones, 'Adapting existing training standards for unmanned aircraft: finding ways to train staff for unmanned aircraft operations' (International Aerospace Symposium of South Africa (IASSA), Centurion, South Africa, 26-28 September 2011); See also Hanibal Goitom, 'Regulation of Artificial Intelligence in Selected Jurisdictions' (Law Library of Congress 2019) <<https://www.loc.gov/regulation-artificial> .> accessed 8 November 2021; C Christodoulou and Mavrikis Inc, 'Drone Regulation in South Africa. (Lexology, 2019) <<https://www.lexology.com/library/detail.aspx> > accessed 8 November 2021.

<sup>421</sup>SACAA "Remotely Piloted Aircraft Systems: Pilot Licensing and Instructor Rating" <http://www.caa.co.za/Pages/RPAS/RPAS%20pilot%20licensing.aspx> (Date of use: 7 September 2020); Samantha Huneberg, 'The rise of drone: Privacy concerns' 2018 (81) THRHR 263, 270.

<sup>422</sup> Private drone operations are also relieved from complying with sub-parts 2 (Approval and Registration), 3(Personnel Licensing), 4(Operating Certificate), and 6(Maintenance). Private drone Operations are also excused from observing Regulation 101.05.5 (2) (Restriction of Landing on roads); 101.05.8(1)(b), (Operational requirements in SA-CATS 101) (c) and (d); 101.05.9(1)(a) (fit to-fly condition) and (b) (Pilot license).

<sup>423</sup> Section 2 (i) of the Civil Aviation Act defines a restricted visual line-of-sight means an operation within 500 metres of the remote pilot and below the height of the highest obstacle within 300 metres of the UAS, in which the remote pilot maintains direct unaided visual contact with the UAS to manage its flight and meet separation and collision avoidance responsibilities".<sup>87</sup>

and their private property and 300m below the height of the highest obstacle of the drone, whilst maintaining direct unaided visual contact with the drone;<sup>424</sup>

**persons, group of people, structure or public road;** drone operations must also not be within a lateral distance of 50 meters from any person, group of people, structure or public road unless the owners and persons agreed that the drone may operate at a distance less than 50 meters or such was approved by the Director.

### 3.5.2 NAMCARs

Under the NAMCARs, 'recreational drone operations'<sup>425</sup> together with drones used by the security cluster and for environmental protection in national game parks or reserves, fall entirely outside the regulatory scope of the NAMCARs.<sup>426</sup>

Similar to the SACARs recreational use of drones in this jurisdiction is also self-regulated. There are no requirements to register, undergo training or observe information privacy principles when operating a recreational drone.

Mindful of sections 7, 8<sup>427</sup> and 39 (2)<sup>428</sup> of the RSA Constitution and article 5 of the Namibian Constitution, which bind all persons (including natural persons and private operations) to respect and promote constitutional rights.<sup>429</sup> Hence the constitutional right

---

<sup>424</sup> Johannesburg City Parks and Zoo, 'Guidelines on the usage of drones in public open spaces and other JCPZ depots and facilities' (website and date not supplied) <<https://www.ward23jhbsouth.co.za/drones-21July2017.pdf> > accessed 25 April 2022.

<sup>425</sup> NAMCARs Part 101.02.1 (2) defines a recreational drone; is as a self-propelled drone with a gross weight of less than 250 grammes, incapable to carry any payload with no camera or similar recording functionality, that is operated below 120 m (above ground level) and 5m from the operator at a speed not exceeding 10 knots.

<sup>426</sup> NAMCAR's: Part 101.02.

<sup>427</sup> Section 8 reads 'The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state. (2) A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, considering the nature of the right and the nature of any duty imposed by the right. (3) When applying a provision of the Bill of Rights to a natural or juristic person in terms of subsection (2)' a court - (a) in order to give effect to a right in the Bill. must apply, or if necessary develop, the common law to the extent that legislation does not give effect to that right; and (b) may develop rules of the common law to limit the right, provided that the limitation is in accordance with section 36(l).

<sup>428</sup> Section 39(2) of the Constitution states that '[when interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights'

<sup>429</sup> *Du Plessis And Others v De Klerk and Another* 1996 (3) SA 850; In re: Certification of the Constitution of the Republic of South Africa, 1996, 1996 (10) BCLR 1253 (CC) certified that Section 8 (2) of Chapter 3 unequivocally provided for the horizontal application of the Bill of Rights; see *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC). 2002 (8) BCLR 771; See also Ian Currie and J De Waal, *The Bill of Rights Handbook* (6th edition, Juta 2013) 32, 64, Danwood Mzikenge Chirwa, 'The horizontal application of constitutional rights in a comparative perspective' [2009] *Saflii Journals* <<http://www.saflii.org/za/journals/LDD/2006/9.pdf>> accessed 1 April 2022. Chetty

to (information) privacy does not only have a vertical effect but also applies horizontally and should therefore be respected even in instances of private drone operations.

For this reason, I support the assertion by Huneberg and Namanlingi<sup>430</sup> that the regulatory threshold (complete exemption and self-regulation of recreational drones) adopted in SACARs in respect of private drone operations, amplifies the prospect that private persons can unlawfully process the personal information of others.

I am further of the view that the private operations philosophy embedded in the SACARs disregards the fact that (personal) information captured is typically stored on online platforms such as Google Drive or iCloud or social networks and blogs<sup>431</sup> which factually distorts the notion of processing for household purposes, as contemplated in terms of section 6(1)(a) of the POPIA.

Additionally, in the absence of the point-of-sale registration suggested above, exempting private operations from the scope of the SACARs (and NAMCARs) undermines the principle of accountability<sup>432</sup> and transparency,<sup>433</sup> in so far as it may be employed to infringe the information privacy of persons, without the possibility of ever being apprehended,<sup>434</sup> unless the drone is physically caught.<sup>435</sup>

Notwithstanding the legitimate concerns associated with reckless or nefarious private drone usage and the obvious need to extend the registration requirements to private drone operations, the private operations methodology threshold in the SACARs parallels the exclusion offered in respect of processing personal information for purely

---

Karun,' The horizontal application of the South African Bill of Rights' (LLM Thesis, University of Natal, 1998).

<sup>430</sup> Samantha Huneberg,'The rise of drone: Privacy concerns' 2018 (81) THRHR 263; Nomalanga Mashinini,' The processing of personal information using remotely piloted aircraft systems in South Africa' [2020] De Jure Law Journal 140.

<sup>431</sup> Article 29 Working Party, Annex 2 Proposals for Amendments regarding exemption for personal or household activities 1 < [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm)> accessed 1 April 2022.

<sup>432</sup> Section 8 of the POPIA.

<sup>433</sup> Section 17 of the POPIA.

<sup>434</sup> Kristen Thomasen, 'Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation' (2018) 16 (2) Canadian Journal of Law and Technology 307; Ahmad Nehaluddin; Chaturvedi Saurabh and Masum Ahmad, 'Unregulated drones and an emerging threat to right to privacy: A critical overview' (2021) 4 (2) Journal of Data Protection & Privacy 124-145(22).

<sup>435</sup> Jennifer M. Bentley, 'Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology' (2019) 70 Hastings Law Journal 249 <[https://repository.uchastings.edu/hastings\\_law\\_journal/vol70/iss1/6](https://repository.uchastings.edu/hastings_law_journal/vol70/iss1/6)> accessed 12 February 2022; Des Butler, 'The Dawn of the Age of the Drones: An Australian Privacy Law Perspective' (2014) 37(2) New South Wales Law Journal 434.

personal and household purposes contemplated under the RSA and Namibian information data legal frameworks.<sup>436</sup>

To this end, the information privacy risks of recreational drones will be best addressed by insisting that recreational and private drones are embedded with PbD drone functionalities discussed above.

### **3.6 Approval and Registration**

The SACARs obligate the SACAA to keep and maintain a register of drone owners, as well as operators (Operators Certificate (ROC) holders), in respect of all non-private drone operations (these are commercial, non-profit and corporate drone operations).<sup>437</sup>

These registrar functions render the SACAA liable to comply with the POPIA as a processor of personal information as contemplated in section 3(1) of the POPIA. The SACAA should accordingly observe and implement the eight conditions for the lawful processing of personal information stipulated under section 4 of section 5 of the POPIA.

Even though the rulemaking authority of the SACAA does not expressly mandate the SACAA to develop regulations addressing information privacy protection within the industry in general or specifically in respect of drones,<sup>438</sup> it is my conviction that the SACAA as regulator, holds a constitutional duty and legislative mandate under the POPIA to promote and protect the right to information privacy within the civil aviation industry.<sup>440</sup>

To this end, this paper proposes that the SCAA is obliged to weave information privacy considerations into the internal and external compliance framework on drones, to protect the right to privacy espoused in section 14 of the Constitution and the POPIA.<sup>441</sup>

---

<sup>436</sup> Sections 6 (1) (a) of the POPIA.

<sup>437</sup> See L Kemp, MP Roux, M Kemp and R Kock, 'Application of Drones and Image Processing for Bridge Inspections in South Africa' (Website name and date not provided) <[https://researchspace.csir.co.za/dspace/bitstream/handle/10204/12124/Kemp\\_2021.pdf?sequence=1](https://researchspace.csir.co.za/dspace/bitstream/handle/10204/12124/Kemp_2021.pdf?sequence=1)> accessed 1 February 2022.

<sup>438</sup> Chapter 6 of CAA.

<sup>440</sup> Sections 7, 8, 14, and 39 of the RSA Constitution.

<sup>441</sup> Jantine Verboven, 'No Fly Drone Drones versus the right to privacy (LLM Thesis, University of Tillburg 2016)

### 3.7. Personnel Licensing

SACARs provides that all non-private drone operations must only be operated by remote pilot license holders, authorising them to undertake operations in any of the three drone operation categories<sup>442</sup> and endorsed with any of three visibility ratings.<sup>443</sup>

Subpart 3 of SACARs details all the pre-requirements to obtain a drone license. I only mention the ones with glaring information privacy implications.

SACATS Part 101.01.7(d) provides that 'drone pilots must observe all statutory requirements relating to liability, privacy and other laws enforceable by other authorities'. Whilst this provision offers a glimmer of hope that information privacy considerations have arrived in the drone regulatory arena. It is my considered view that this bare call to (self) action, amounts to a passive dereliction of this crucial constitutional duty and legislative mandate.<sup>445</sup>

It is my opinion that a more active approach would have been to impose an obligation that the drone operators' manual must demonstrate how the privacy laws will be complied with and how the conditions for lawful processing imposed under the POPIA will be implemented monitored and enforced by the drone operator or pilot.

In addition to this, it would be prudent for the SACAA to apply to the IRSA in terms of section 60 of the POPIA to approve a code of conduct for the civilian drone industry (perhaps the entire civil aviation industry), specifying *inter alia* how the minimum conditions for lawful processing of personal information will be practically applied within the drone industry. Once this code of conduct is accredited by the IRSA, failure to comply with it will be considered a breach of the conditions for lawful processing under the POPIA.<sup>446</sup>

Another requirement under SACARs to qualify as a drone pilot is to submit either a medical certificate or a self-declared medical assessment report to the SACAA. Section 26 read with 32 of the POPIA renders it unlawful to process information relating to the health status and sex of persons, subject to some exceptions. From my analysis, the

---

<sup>442</sup> Aeroplane, Helicopter and Multirotor.

<sup>443</sup> VLOS (Visual Line of Sight), (Extended) E-VLOS, (Beyond) B-VLOS.

<sup>445</sup> Manana Wanyonyi Edisn Rodgers, 'Integration of Unmanned Aircraft Systems into Civil Aviation: A Study of the U.S, South Africa And Kenya' (Phd Thesis, University of South Africa 2020).

<sup>446</sup> Section 68 of the Protection of Personal Information Act, 4 of 2013. The definition of 'this Act' in section 1 includes all regulations and codes of conduct.

processing of the medical assessment reports of pilots appears to be justifiable. It may however be necessary for the SACAA to obtain general authorisation from the IRSA to process this information, as provided for under section 27 (1) (c)<sup>447</sup> or chapter 4 of the POPIA.

In respect of required expertise, drone pilots are expected to hold a restricted certificate of proficiency in radiotelephony (aeronautical), undertake flight training, pass a theoretical knowledge examination and undergo competency skills training. The pilots are expected to take a re-validation test upon the expiry of their licenses.<sup>449</sup>

The RSA AICs<sup>450</sup> prescribes the training curricula, the contents of the training models and the procedures for drone pilot training, as well as the requirements to be accredited as a Remote Pilot Training Organisation (RTO) to train all aviation drone pilots and other essential personnel.<sup>451</sup> All training offered outside the SACAA is offered by private persons that have been accredited by the SACAA.

The promotion of information privacy within the aviation industry will be bolstered if the drone pilot training incorporates a mandatory qualifying assessment on the provisions of the POPIA, for all drone pilots to sensitise pilots and operators and equip them with theoretical and practical skills to avert unlawful processing of personal information when deploying drones.

I am of the view that this test presents a prodigious avenue for the Regulator<sup>452</sup> to utilise these training opportunities to execute its functions to provide education in line with section 40(1)(a)(i)(ii) of the POPIA. Section 40 of the POPIA, stipulates the powers, duties and functions of the IRSA. The IR is authorised to undertake educational programmes that foster the protection of personal information by itself or in conjunction with others in terms of section 40(1)(a)(i)(ii) of the POPIA.

A drone pilot is also required to maintain a logbook detailing every flight they undertake, which must be retained for sixty months from the date of the last entry.

---

<sup>447</sup> 'Processing is necessary to comply with an obligation under public international law'.

<sup>449</sup> SACARs: Part 101.03.2.6; See also Sandra Kock, 'An overview of South African RPAS regulation' (Geomatics Indaba Proceedings 2015) < <https://dronecon.co.za/wp-content/uploads/2018/05/Sonet-Kock-RPAS-Regulations.pdf>> accessed 14 February 2022.

<sup>450</sup> Available at <<http://www.caa.co.za/Pages/RPAS/Remotely%20Piloted%20Aircraft%20Systems.aspx>> accessed 21 March 2022. [See also Paragraph 7.9 of the ICAO Circular No. 328-AN/190].

<sup>451</sup> SACAA Aeronautical Information Circular No 008/2015 of 23 July 2015 (hereinafter the AIC 008/2015), Paragraph 2.

<sup>452</sup> Section 40 (1) (a) of POPIA.

Keeping this logbook is a great measure to give effect to principle six (6) of the minimum information privacy principles, namely openness (transparency), set out in section 17 of the POPIA.<sup>453</sup> Properly utilised the logbooks can be purposed to serve as a compliance portfolio or otherwise with the POPIA and as evidence in instances where information privacy violations are alleged.

As required by the purpose specification principle under the POPIA, there is a need for the SACARs to expressly specify the purpose for which the logbooks are to be retained. This is important to ensure compliance with section 15 of the POPIA which bars function creep for incompatible purposes.

Moreover, SACARs must expressly proscribe the processing of personal information in logbooks. In compliance with sections 13 and 14(4)-(5) of the POPIA, it must furthermore stipulate that the logbooks should be destructed or deleted in a way that forestalls reconstruction in an intelligible manner or anonymised after six months.<sup>454</sup>

### **3.8. Drone Operators Certificate (ROC)**

All non-private drone operators are required to obtain an operator's certificate for every drone they intend to operate. Commercial operators are further expected to obtain air service licenses before being issued with a ROC.<sup>455</sup>

Following scrutiny of Subpart 4 (RPAS Operators Certificate), it is important to highlight the following given the requirements under the POPIA.

#### **Operations Manual<sup>457</sup>**

It is a requirement that an application for a ROC must be accompanied by an operations manual. The operations manual must particularise all the measures that will be undertaken to ensure compliance with all the SACARS and how safety standards set out in the SA-CATS 101 will be attained in the course of the drone operations.<sup>458</sup>

---

<sup>453</sup> Section 17 provides that, a responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the POPIA.

<sup>454</sup> Section 14 (5) of POPIA.

<sup>455</sup> Issued in terms of the air service License Act No 115 of 1990.

<sup>457</sup> SACARs: Part 101.04.5. (1).

<sup>458</sup> SACARs: Part 101.04.5 (1)

It is a further requirement that the operations manual must also set out the scope of the envisaged operations, as well as all operational and legislative activities and responsibilities the operator must fulfil relative to the size and scope of its envisaged operations.

The SACARs: Part 101.04.5 (1) further obligates the operator to train all its personnel in line with the operations manual (as amended from time to time).<sup>459</sup>

It is a foregone conclusion that all ROC Operators have a legal duty to comply with the POPIA. Consequently, the SACARS should impose a duty that the operations manual must detail all the measures that will be undertaken to ensure compliance with the POPIA or the accredited code of conduct. Most significantly, the training offered to the ROC holders and their employees should likewise include information privacy protection.

### **Documents and Records**

SACARs: Part 101.04.6. impose a duty to establish a suitable record-keeping system, capable of reliably evidencing all the operator's undertakings. It further provides that the record-keeping system must enumerate the lines of responsibility and accountability within the drone operator, and the safety policy applied by such.

It is a specific requirement that these records must identify all potential aviation safety hazards of its operations and specify how the hazards and associated risks will be mitigated, as well as detail the personnel training to be offered and stipulate all quality, safety and security measures that will be observed, in the course of the drone operations.

I am of the considered opinion that this requirement can be extended to give effect to section 17 of the POPIA with great ease. Section 17 provides that, a responsible party must maintain the documentation of all processing operations under its responsibility as referred to in sections 14 or 51 of the POPIA.

---

<sup>459</sup>D Hofmeyr, 'Here is why South Africa's new drone regulations are ridiculous' <<https://businesstech.co.za/news/general/92072/here-is-why-south-africas-droneregulations-are-ridiculous/>> 8 July 2017



In addition to documenting the processing activities, and keeping these records, these records can similarly be utilised to satisfy the requirements of section 19(2) of the POPIA. Section 19(2) of the POPIA obligates all responsible persons to implement appropriate technical and organisational measures to avoid unlawful access, processing and loss damage and destruction of personal information.

### **3.9. Safety Management**

Drone operators are further required to put in place a safety management system(s) proportional to the scope and complexity of their operations and the size of the organisation or entity.<sup>464</sup> The safety management plan must *inter alia* include an assessment of actual and potential safety threats, as well as an associated safety risk mitigation and remedial action plan. The operator is correspondingly responsible to undertake continuous and regular assessments of the appropriateness and effectiveness of the safety management measures.

These requirements align with the principle of ‘accountability’ under the POPIA and is a great avenue to introduce a parallel requirement to undertake a DPIA of the envisaged drone operations and to develop an information privacy risk mitigation strategy, as contemplated in section 19 (2) of the POPIA. Section 19(2) of POPIA calls for the establishment of foreseeable internal and external risks and to put in place security measures to ensure the integrity and confidentiality of personal data processed.

### **3.10. Security**

As a means to ensure the security of its operations SACARs: Part 101.04.5.8 requires the ROC holder to conduct background checks and to conduct criminal record checks on all its employees, bi-annually.<sup>467</sup>

---

<sup>464</sup> SACARs Part 101.04.5.

<sup>467</sup> SACARs: Part 101.04.8.

To avoid contravening section 26 read with sections 32 and 33 of the POPIA, which limits the processing of criminal or unlawful or objectionable conduct on behalf of third parties.

Mindful of this prohibition and to protect the legitimate interest of the employees of ROC holders, the SACARs must offer guidance on how these background and criminal record checks should be conducted without unreasonable inroads on the privacy of their employees. Most importantly, the SACARs must alert the ROC holders to seek authorisation or an exemption in terms of sections 27, and 37-38 of POPIA to process this special information, provided the operations qualify for such authorisation.

A ROC holder is also required to store the drone safely to avoid undetected unauthorised interference or use and to undertake flight preparations to detect unlawful interference. This requirement also borders on section 19(a) of the POPIA, which insists that appropriate reasonable technical and organisational measures should be maintained to avert unauthorised processing, loss and damage of personal information. I thus suggest that SACARs can avert the unlawful processing of personal information processed by drones, by simply imposing an analogous obligation in respect of information privacy.

It is further required that the ROC holder must also appoint or designate a security officer to exercise control over the implementation of the safety management plan and offer all its employees security awareness training. In the same vein, the SACARs must incorporate the requirement to appoint or designate a DPO<sup>468</sup> as envisaged under section 55 of the POPIA who will be responsible for overseeing compliance with the information privacy protection commitments the operator and pilots stipulated in the manual or the industry code of conduct.

#### **4. Selected General Drone Operation Limitations**

I proceed to discuss selected provisions of the SACARs below. Eventhough these provisions are primarily focused on ensuring the safety and security of drones and draw

---

<sup>468</sup> Section 55 of POPIA.

no appreciable differentiation between information privacy and the physical dimensions of the comprehensive right to privacy, these provisions also have information privacy underpinnings or may be purposed to protect information privacy in the course of the deployment of drones.<sup>i</sup>

### **Weather conditions**

As a means to strengthen the openness requirement of transparency in the POPIA, SACARs provide that drones must only operate during the day and when the weather conditions do not hamper visibility<sup>469</sup>;

### **Operation in the vicinity of people, property, or public roads**

Take-off and landing on public roads are forbidden, unless the operator is a ROC holder and has obtained approval from the Director and the relevant local authority or the road is closed to the public for public use.<sup>470</sup>

Similarly, flying a drone overhead or at a lateral distance of 50 meters from any person, or in the vicinity of structures or buildings, is only permitted by a ROC holder or where express consent has been obtained from the affected persons.<sup>471</sup>

This provision should be revised, in light of literature that advances that drones have the technological capabilities to conduct surveillance from distances greater than those prohibited.<sup>472</sup>

Although requiring the consent of owners of private property is a great start to acknowledging the (information) privacy effect of drones, the fact that these obligations are self-regulatory and may not necessarily translate into actual information privacy protection.

Instead of leaving it to the goodwill of drone operators, who may find it challenging to understand and interpret the complex and technical SACARs. For this reason, this research recommends that<sup>473</sup> insistence should rather be placed on deploying drones

---

<sup>469</sup> SACARs: Part 101.04.5.1.

<sup>470</sup> SACARs: Part 101.04.5.2.

<sup>471</sup> SACARs: Part 101.04.5.13.

<sup>472</sup> Jennifer M Bentley, 'Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology' (2019) 70 *Hastings Law Journal* 249.

<sup>473</sup> William J. Black III, 'A No-Drones Home: Solving the Home Airspace Dilemma' [2018] *J Marshall Law Journal* 1, 27.

embedded with PETs, such as geofencing and or redaction programming.<sup>474</sup> Geofencing impose an invisible ceiling for the drone, even though it may technically be able to fly beyond such a ceiling.<sup>475</sup> Redaction programming automatically conceals or removes personal information (special information and personal information of children) and only collects specifically aimed data.<sup>476</sup> Other PETs include the use of encryption, blurring and data anonymisation. <sup>477</sup>

### **Objects or substances**

The SACARs prohibit drones to convey goods the drone is operated by a ROC and the Director approved such.

Mindful that the Drone Barometer<sup>478</sup> signposts that following the Covid-19 pandemic, drones are overtly being employed to deliver humanitarian assistance such as food, and medicine. This restriction, therefore, undermines the economical and beneficial use of drones but strengthens information privacy to the extent that it forestalls information privacy protruding payloads that can be carried on drones.

### **No drone can be operated at night unless under ‘Restricted-Visual Line of Sight**

---

<sup>474</sup> Ann Cavoukian and Khaled El Emam, *Dispelling the Myths Surrounding Deidentification: Anonymization Remains a Strong Tool for Protecting Privacy* (Office of the Privacy Information Commissioner Ontario, 2011) <<https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf>> 12 March 2022; Ann Cavoukian, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* (Privacy Commissioner of Ontario 2013).

<sup>475</sup> Ann Cavoukian and Khaled El Emam, *Dispelling the Myths Surrounding Deidentification: Anonymization Remains a Strong Tool for Protecting Privacy* (Office of the Privacy Information Commissioner Ontario, 2011) <<https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf>> 12 March 2022.

<sup>476</sup> Ann Cavoukian, *Operationalising privacy by design: a guide to implementing strong privacy practices* (Privacy Commissioner of Ontario 2013) <<https://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf>> Accessed 11 April 2021.

<sup>477</sup> Article 29 Data Protection Working Party, ‘Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones’ adopted on 16 June 2015 <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf)> accessed 14 February 2021; Rachel Finn and David Wright, ‘Privacy, Data Protection and Ethics for Civil Drone Practice: A survey of Industry, Regulators and Civil Society Organisations’ (2016) 32 *Computer Law & Security Review* 577-586; Elisa Serafinelli, ‘Imagining the social future of drones’ [2022] *The International Journal of Research into New Media Technologies* 1–16 < DOI: 10.1177/13548565211054904> accessed 12 January 2022.

<sup>478</sup> Ed Alvarado, ‘Drone Industry Barometer 2021: The State of the Drone Industry’ (Drone Industry Insights, 15 September, 2021) < <https://droneii.com/drone-industry-barometer-2021-survey>> accessed 13 March 2022.

It is required that all drones must only be deployed between dawn and dusk, save if otherwise approved.<sup>480</sup>This restriction holds information privacy protection implications, in so far as drones operated during the day augment their visibility which in turn strengthens the accountability and enforcement requirements under the POPIA.

**Flying in formation or swarm or towing other aircraft**, and performing aerial or aerobatic displays, are similarly debarred, except if approval was obtained. The insistence on a single drone operation at a time strengthens the accountability, transparency and data subject enforcement principles set out in the POPIA.

**Near or above sensitive areas:**<sup>481</sup> in order to protect critical infrastructure, the SACARs prohibit drone operations near or above nuclear power plants, prisons, police stations, crime scenes or courts. I am of the view that the definition of sensitive areas in the SACARs must be expanded to include areas that will invariably result in processing (special) personal information and information of children within the context of sections 26 and 33 of the POPIA, such as hospitals, political and trade union buildings and events, parks, schools, early childhood development centres, youth centres, health facilities, prisons, refugee camps.<sup>482</sup>

**Visual Line of Sight Operations:**

the general rule is that all drones should only be deployed within their Visual Line of Sight (VLOS) to enable compliance with the separation and avoidance responsibility of drone pilots. Beyond Visual Line of Sight Operations are only allowed if the Operator holds a Remote Pilot Operator's Certificate and it is approved by the Director.<sup>483</sup>This rule limits the physical span of drone operations and thus ostensibly thwarts the possibility of surveilling an unlimited terrain, which in turn limits the expanse available to process personal information.

**Radio Communication Requirements:** the SACARs insist that all drone operations must be conducted within a radio line of sight (RLOS).<sup>484</sup> To this end, an operator must obtain a radio station license from the Independent Communications Regulatory

---

<sup>480</sup> SACARs: Part 101.04.5.12.

<sup>481</sup> Manana Wanyonyi Edisn Rodgers, 'Integration of Unmanned Aircraft Systems into Civil Aviation: A Study of the U.S, South Africa And Kenya' (Phd Thesis, University of South Africa 2020).

<sup>482</sup> As defined in Section 1 of POPIA.

<sup>483</sup> SACARs: Part 101.04.5.11.

<sup>484</sup> SACARs: Part 101.04.5.16.

Authority of South Africa (ICASA).<sup>485</sup>Owing to this, provision should be made to ensure that the personal information processed during a drone operation is not unlawfully intercepted during transmission. It may further be necessary to ensure that the communications over the radio frequency are end-to-end encrypted and other security measures should be imposed on drone operators to ensure that personal information is protected when utilising the radio frequencies. Unlawful interception constitutes a criminal offence in terms of section 49 of the Regulation of Interception of Communications and Provision of Communication-related Information Act <sup>486</sup>and attracts a penalty of a fine not exceeding two million rands or a period of imprisonment not exceeding 10 years.<sup>487</sup>

## **5. Liability**

The SACARS: Part 101.05.9 prohibits any person from operating a drone negligently or recklessly in a manner that 'jeopardises the safety of any person, property or other aircraft in the air or on the ground'. Section 8 of CAA enables aggrieved persons to claim material damage or loss suffered owing to an occasion that took place in flight, whilst taking off or landing, or by any article falling from the aircraft.

For the avoidance of doubt, this stipulation must be amended to expressly include the unlawful processing of personal information envisaged under the POPIA. Resultantly, the SACARs should therefore expressly inhibit unlawful processing of personal information through the instrumentality of a drone<sup>488</sup> and afford data subjects the right to be compensated for personal information breaches under POPIA<sup>489</sup> caused by the reckless use of drones.

## **.5 Insurance**

---

<sup>485</sup> Sonet Kock, 'An overview of South African RPAS Regulations '(Geomatics Indaba Proceedings 2015 Stream) <<https://www.ee.co.za/wp.../uploads/2015/08/Sonet-Kock.pdf> > accessed 11 March 2021.

<sup>486</sup> Act No. 70 of 2002.

<sup>487</sup> Section 51(1)(b) Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

<sup>488</sup> Chris Christodoulou and and Inc, 'Drone Regulation in South Africa. (Lexology, 10 December 2019) <<https://www.lexology.com/library/detail.aspx> .> accessed 8 November 2021.

<sup>489</sup> Or an accredited Civil Aviation Industry Code.

In addition to clarifying the distribution of liability for information privacy contraventions occasioned by drones, the SACARs should go a step further and mandate all drone operators to maintain adequate third-party insurance to recompense any loss and damage brought about by unlawful processing of personal information in the course of drone operations.<sup>491</sup>

To enable drone operators to comply with the obligation to compensate data subjects for any material and non-material loss or damage suffered as contemplated in sections 107 and 109 of POPIA, the insured amounts should be proportionate to the compensation payable for the fines and compensation under the POPIA.

## **6. Enforcement of the SACARs**

SACARs: Part 101.04.02 stipulates that ROC holders must subject themselves and commit to requiring their partners and subcontractors, to safety and security inspections, audits and oversight by authorised persons.<sup>492</sup> To this end, the inspectors from the SACAA may at any time evaluate any drone operator or pilot's compliance with the CAA, the operator's manual (or if adopted the code of conduct) and conditions imposed in any aviation document.

The monitoring and compliance enforcement functions of the SACAA are governed by Chapter 7 of the CAA. Section 113(3) of the CAA prohibits that any confidential, personal, commercially sensitive or proprietary information obtained in the course of enforcement, must be published or disclosed to any person without the consent of the person to whom the information relates. There is thus an obligation to respect information privacy throughout the enforcement and monitoring process.

The monitoring and enforcement provisions in the CAA are a functional equivalent of that envisaged in POPIA. The SACAA is correspondingly empowered to enforce the CAA and the Regulations adopted thereunder through the issuance of compliance orders<sup>493</sup> and the suspension of certain privileges of a pilot or operator under any

---

<sup>491</sup>SACARs: Part 101.04.12. See also Orgo Athanasios Yiannakis, 'Does the Current Drone Legislation in South Africa and the United Kingdom adequately assist Insurers and their Underwriters to assess and address the Liability Risks associated therewith? A Comparative Study' (Masters Thesis, University of Johannesburg 2019).

<sup>492</sup> Inspectors enlisted in accordance with Section 88 of the CAA.

<sup>493</sup> Section 114 CAA.

aviation document. The CAA further provides for an internal appeal process to an independent appeals committee, established in terms of section 122 of the CAA.

Since the enforcement procedures under the POPIA and the CAA is a mirror image of each other, I am of the considered opinion that it would be judicious to expand the current monitoring and enforcement powers under the CAA, to cover information privacy protection within the civil aviation industry, particularly in the drone industry.

Another way to cultivate a pro-information privacy culture within the drone industry and to facilitate a uniform and industry-appropriate implementation of the POPIA principles across the regulatory spectrum, the SACAA should consider seeking accreditation of a code of conduct for the civil aviation industry, as contemplated in terms of chapter 7 of the POPIA.<sup>494</sup>

A code of conduct prescribes practices, procedures and processes which is to be observed within a particular industry, to give effect to the information privacy protections extended under the POPIA. Most especially it makes provision for resolving grievances concerning the unlawful processing of personal information<sup>495</sup> protected under the POPIA and gives data subjects scope to exercise and enforce their data subject rights accorded under the POPIA.<sup>496</sup> Once this code has been accredited failure to comply with it will be considered a breach of the conditions for lawful processing under the POPIA.<sup>497</sup>

Resultantly, in addition to the safety and security monitoring and enforcement functions, the inspectors (or authorised persons) within the SACAA must additionally assume enforcement powers and functions in respect of unlawful processing of personal information under the POPIA or an approved code of conduct.

In order to ensure that data subjects have active control over the processing of their personal information within the drone industry and access to efficient and impartial dispute relations mechanisms, the Appeals Committee within the SACAA should be

---

<sup>494</sup> Sections 60-68 of the POPIA.

<sup>495</sup> Section 63(1) of POPIA provides that a code may prescribe procedures for making and dealing with complaints alleging a breach of a code without limiting or restricting the provisions of Chapter 10 of POPIA.

<sup>496</sup> These provisions are subject to the compliance procedures governing 'Enforcement' in Chapter 10 and "Offences, Penalties and Administrative Fines" in Chapter 11 of POPIA.

<sup>497</sup> Section 68 of the POPIA. The definition of 'this Act' in section 1 includes all regulations and codes of conduct.



empowered to adjudicate complaints regarding the unlawful processing of personal information occasioned by drones, as envisaged under section 63 of the POPIA.<sup>498</sup>

Moreover, there is no doubt that the efficient enforcement of the information privacy issues related to matters canvassed herein requires proper processes and resources to acquire the costly enforcement infrastructure and technologies to effectively monitor and enforce the information privacy-focused drone regulations.<sup>499</sup>

In addition to the above, even if the drone regulations receive an information privacy facelift, the lack of enforcement infrastructure and technologies, within the SACAA and other law enforcement agencies and the lack of skilled personnel to monitor and enforce the information privacy implications of drones will greatly hamper the enforcement of the SACARs.<sup>501</sup>

## **7. Notable Information Privacy Namcars Provision**

It will be remiss of me, to not highlight some of the notable information privacy provisions reflected in the NAMCARs, which are great reference points in the quest to adopt pro-information privacy drone regulations.

NAMCAR's: Part 101.05.4 (4)-(7) deserves mention. Part 101.05.5. (4):

- '(1) prohibits the deployment of a drone which will amount to or result in surveillance of another person, save if consent was obtained;
- (2) forbids surveillance of movable and immovable property, except if the owner has acquiesced thereto;
- (3) bans photographing or filming any person without their consent for purposes of publicly disseminating.'

Notwithstanding the absence of a dedicated information privacy protection legislation in Namibia, unlike the single abstract reference calling on drone operators to observe RSA

---

<sup>498</sup> Information Regulator RSA, Standard for making and dealing with complaints in a Code of Conduct <<https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-Standard-CodeOfConduct-Complaints-20210301.pdf>> accessed 1 April 2022.

<sup>499</sup> Ashley Taborda, 'Privacy & Drone Surveillance: The Illusive Remedy' [2017] Canadian Journal of Law and Technology 379.

<sup>501</sup> Steve Calandrillo and Jason Oh, 'Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety' (2020) 23 *Stanford Technical Law Review* 182; Haomiao Du & Michiel A. Heldeweg, 'An experimental approach to regulating non-military unmanned aircraft systems' (2019) 33 (3) *International Review of Law, Computers & Technology* <285<DOI:10.1080/13600869.2018.1429721>

privacy laws, this provision expressly details conduct prohibited with a clear link to the promotion of information privacy.<sup>502</sup>

Another noteworthy observance is the allowance made for drone 'journalism'<sup>503</sup> and for newsgathering at events or places to which the general public is invited' provided the Director's prior approval has been obtained and all safety and security considerations are addressed.

This allowance underscores the fact that the right to privacy is not absolute, subject to reasonable and justifiable limitations.

The NAMCARS also embrace the principle of proportionality and thus strictly reserves the use of drones carrying infrared or other similar thermal imaging technology payloads to non-recreational drone operations on the grounds recognised, as general exceptions under section 15 of the Bill<sup>504</sup> namely: firefighting, police, search and rescue or crime investigation and scientific research purposes.

In addition to these two traditional grounds, NAMCARS: Part 101.05.5. (6) permits drones with these intrusive technologies to be used exclusively for mapping and evaluating the earth's surface, including terrain and surface water bodies and other features, investigation and evaluation of crops, livestock or farming operations and investigation of forest and for estate management.

NAMCARS: Part 101.05.5. (7) also empowers the Director of the NACAA, an inspector or any authorised person under the NCAA to seize or detain or ground or otherwise direct a drone, if the anticipated operation will amount to a contravention of the Civil Aviation Act and the<sup>505</sup> NAMCARS.

Even though these provisions are ambiguous and fall short of addressing the information privacy concerns of drones comprehensively, it is nevertheless an estimable recognition and effort to heed the information privacy concerns levied in respect of drones. Although it leaves much to be desired, it demonstrates an acknowledgement and commitment of the NACAA to protect the constitutional right to information privacy

---

<sup>502</sup> See SA-CATS 101. 01.7 (d). Available at <caa.mylexis.co.za> accessed 12 April 2022.

<sup>503</sup> Jonas Harvard, Mat Hyvönen and Ingela Wadbring, 'Journalism from Above: Drones and the Media in Critical Perspective' (2020) 8 (3) Media and Communication Journal < DOI: 10.17645/mac.v8i3.344> accessed 1 May 2022.

<sup>504</sup> Similar to the exceptions under section of the POPIA.

<sup>505</sup> Act 6 of 2016.

and comply with their obligations to promote and protect the right to privacy guaranteed under Article 13 of the Namibian Constitution.<sup>506</sup>

Furthermore, it is impressive that provision is made for the NACAA to take proactive action where there is an eminent threat of a contravention of any of the provisions of the NAMCARs: Part 101.05.5. (7). Given the criticism of the *post-ante* remedial action traditionally associated with common law and delictual courses of action regarding infringements of information privacy, but falls short of the active control information privacy, principle as well as to ensure active participation of data subject rights and to avert information privacy contraventions and to avoid the cost of information privacy contraventions.

## 8. Chapter Conclusion

This Chapter assessed the contents of the SACARs and NAMCARs which regulates the use of drones in the RSA and Namibia.

It established that, whereas the rulemaking authority of the SACAA does not expressly mandate the SACAA to develop regulations addressing information privacy protection, there is a constitutional duty on the SACAA and associated institutions (as well as all stakeholders including private drone operators) to protect and promote the right to information privacy.<sup>507</sup>

Resultantly, there is a need for the SACAA to accept accountability to address the information privacy implications of drones and to adopt a policy, promulgate laws and implement measures to avert the possibility of unlawful processing of personal information through the instrumentality of drone technologies.

The substantive provisions of the SACARs overtly focus on controlling and minimizing safety and security risks and adopt a passive derelictive approach to information privacy. It also regrettably excludes key stakeholders such as drone manufacturers and consequently omits pertinent 3<sup>rd</sup>-generational technical principles such as PbD, DPIA and the mandatory use of PETs. Little consideration has also been accorded to the

---

<sup>506</sup> Article 5 of the Namibian Constitution.

<sup>507</sup> Section 7,8,14 and 36 of the RSA Constitution and Article 5 of the Namibian Constitution.

cross-border transfer of personal information surrounding the importation and exportation of drones.<sup>508</sup>

The analysis herein demonstrates that the current legal framework on drones leaves numerous gaps, concerning the protection of information privacy within the drone industry.

However, above and beyond these gaps there are also plenty of opportunities to re-purpose, expand and converge the existing requirements in the SACARs to achieve parallel compliance with the POPIA and the Namibian Data Protection Bill.

---

<sup>508</sup> Even though NAMCARs includes an ambiguous express acknowledgement of information privacy considerations, it appears to have slipped in as an afterthought, as appose to strategic considerations thereof.

## CHAPTER FIVE

### The European Union Legal Framework on Drones

---

*The EU is the first jurisdiction to acknowledge information privacy as an independent human right. It has recently reformed its legal framework regulating drones, which is hailed to incorporate amongst others information privacy protection. This chapter examines the legal framework on drones within the EU through the prism of information privacy, anticipating to glean possible lessons on how RSA and Namibia can promulgate a more information privacy-focused regulatory framework on drones, and hopeful to borrow lessons on how to weave in information privacy considerations across the drone regulatory spectrum.*

#### 1. Introduction

All European Union (EU) member states are parties to the Chicago Convention and seven EU member states formed part of the ICAO Council for the period 2019-2022. Several other others hold observer status in various ICAO bodies.<sup>509</sup>

Perceived as the biggest manufacturer, exporter and user of drones internationally, the EU is hailed as the 'Model Flying Union'.<sup>510</sup>

---

<sup>509</sup> European Commission- Proposal for a Council Decision on the position to be taken on behalf of the European Union in the 222nd session of the Council of the International Civil Aviation Organization (ICAO) as regards the envisaged adoption of Amendment 177 to Annex 1, Amendment 47 to Annex 2, Amendment 108 to Annex 8, Amendment 90 to Annex 10 and of the new volume VI to Annex 10 the Convention on International Civil Aviation' Brussels, 5.2.2021 COM(2021) 48 final 2021/0027 (NLE) Available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0048&rid=1>> accessed 20 June 2022.

<sup>510</sup> Elaine Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity* (Bloomsbury Publishing 2022); María de Miguel Molina and Virginia Santamarina Campos (eds), 'The Drone Sector in Europe': In *Ethics and Civil Drones European Policies and Proposals for the Industry* (Springer 2018); See also Juan Plaza, 'What is the Value of the European Drone Market?' (Commercial UAV News, October 15, 2019)

It is predicted that the EU drone market will annually contribute over fifteen billion euros by the year 2050. It is expected that the European drone industry will directly absorb more than one million employees by the year 2035.<sup>511</sup>

Living up to the above acolytes and in anticipation of the eminent growth of the drone industry, the EU is the first continent to embark on ameliorating its legal framework on drones.

This transformation emanated from a 2018 EASA opinion,<sup>512</sup> which sturdily encouraged the adoption of a detailed operation-centric, proportionate, risk- and performance-based and uniform European civil aviation legal framework and singled out environmental protection, privacy, data protection, and safety and security, as explicit reform objectives.

This chapter sets out a content analysis of the regulations governing drones in the EU. Given its involvement in ICAO, the EU laws on drones also present a vital point of reference for an international evaluation from a comparative perspective.

## 2. Key Institutions

The drone landscape within the EU comprises of the following institutions:

### 2.1 EU Aviation Safety Agency

---

<<https://www.commercialuavnews.com/europe/value-european-drone-market>> accessed 20 May 2022.

<sup>511</sup> SESAR, European Drones Outlook Study Unlocking the value for Europe (SESAR European Drones Outlook Study, November 2016)<[https://www.sesarju.eu/sites/default/files/documents/reports/European\\_Drones\\_Outlook\\_Study\\_2016.pdf](https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf)> accessed 28 April 2022; Eleonora Bassi, 'From Here to 2023: Civil Drones Operations and the setting of new legal rules for the European Single Sky' (2020)100 (2) Journal of Intelligent & Robotic Systems 493.

<sup>512</sup>European Aviation Safety Agency Opinion No. 01/2018 Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories EASA Opinion published on February 2018. Adopted(hereinafter referred to as the 'EASA proposal') <<https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2001-2018.pdf>> accessed 26 June 2022; Anna Tomová and Andrej Dudáš'An Aviation Strategy for Europe: A critical assessment of delivered results' [2018] 6 (3) MAD - Magazine of Aviation Development 17-22 <DOI:10.14311/MAD.2018.03.03> accessed 12 July 2022.

The EU Aviation Safety Agency (EASA) was constituted in 2002<sup>513</sup> as an independent juristic person and is principally seated in Cologne, Germany.<sup>514</sup> The EASA has regulatory and executive functions in respect of the civil aviation industry within the EU. The scope of its mandate is defined by the EU Regulation 2018/1139<sup>515</sup> (Basic Regulation (BR)). It is primarily responsible for drafting aviation legislation and providing advice to the European Commission (EC), EU Member States and national civil aviation authorities on civil aviation matters.<sup>516</sup> EASA's functions are buttressed by the European Organisation for Civil Aviation Equipment (EUROCAE) and Joint Authorities for Rulemaking on Unmanned Systems (JARUS).<sup>517</sup>

## **2.2. European Organisation for Civil Aviation Equipment**

The European Organisation for Civil Aviation Equipment (EUROCAE) is responsible for conscripting airworthiness and operational standards for aircrafts within the EU.

## **2.3. Joint Authorities for Rulemaking on Unmanned Systems**

The Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is a voluntary organisation, comprising national civil aviation authorities within the EU, as well as non-EU countries and regional organisations. Its objective is to recommend technical, safety and operational requirements for the certification and safe integration of large and small drones into the airspace and at airports.

## **2.4. National Aviation Authority (NAA)**

---

<sup>513</sup> EASA was constituted under Council and Parliament Regulation (Regulation (EC) 1592/2002, which was repealed by Regulation (EC) No 216/2008, as amended by Regulation (EC) 1108/2009).

<sup>514</sup> Regulation (EC) 216/2008.

<sup>515</sup> Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91. (OJ L 212, 22.8.2018) (hereinafter Basic Regulation). Available at <<http://data.europa.eu/eli/reg/2018/1139/oj>> accessed 27 July 2022.

<sup>516</sup> Deepan Sarma and Paul Quinn, 'Data protection, Social, Ethical and Legal Frameworks Delivery' (not supplied, Feb 2018) <[http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN\\_D3.1\\_DataProtectionSoEL\\_Framework\\_V1\\_0\\_PU.pdf](http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN_D3.1_DataProtectionSoEL_Framework_V1_0_PU.pdf)> 31 May 2022.

<sup>517</sup> Damiano Taurino, Drones4Safety: Regulatory Gap/Barriers Analysis (drones4safet, Version 1.0 14 September 2020) <<https://drones4safety.eu/wp-content/uploads/2021/01/D2.2-Regulatory-Gap-Barriers-Analysis.pdf>> accessed 2 June 2022.

NAAAs are responsible for implementing the EASA regulations in the domestic legal systems of the various EU Member States, as well as for nationalising aspects delegated by the EASA and for the overall national administration and oversight of the EASA regulations.

## **2.5. European Organisation for the Safety of Air Navigation**

The European Organisation for the Safety of Air Navigation (EUROCONTROL) Eurocontrol is a civil and military aviation organisation established in 1960 comprising of over forty Members States from across Europe and two Comprehensive Agreement States (Morocco and Israel). Its principal mandate is to promote a seamless and safe European Air Traffic Management (ATM) system across Europe.<sup>518</sup>

## **3. Overview of the EU Legal Framework on Drones**

In this paragraph we will give a brief overview of the regulations governing drones in the EU, this overview will be followed by a summary discussion of the substantive provisions that hold information privacy implications.

Following the European Commission's endorsement of a novel aviation strategy for Europe on 7 December 2015, the EU promulgated a compendium of transnational drone regulations, putting an end to what scholars describe as 'regulatory anarchy' and collaged national approaches.<sup>519</sup>

---

<sup>518</sup>Rene Bulin, 'The European Organisation for the Safety of Air Navigation -Eurocontrol': In Robertson, A.H. (eds) *European Yearbook / Annuaire Europeen* (Springer 1976) <[https://doi.org/10.1007/978-94-015-1197-1\\_5](https://doi.org/10.1007/978-94-015-1197-1_5)> accessed 20 June 2022.

<sup>519</sup> Anna Konert and Tadeusz Dunin, 'A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 (3) *Advances in Science, Technology and Engineering Systems Journal* 93-99; Tadeusz Zieliński and Wiesław Marud, 'Challenges for integration of remotely piloted aircraft systems into the European sky (2019) 102 *Scientific Journal of Silesian University of Technology Series Transport* 217-229 <DOI: <https://doi.org/10.20858/sjsutst.2019.102.18>> accessed 21 June 2022.



The transformation commenced with the adoption of the Basic Regulation (BR).<sup>520</sup> The BR is in essence simply an enabling law<sup>521</sup> setting out the overarching civil aviation legal principles and does not contain any substantive provisions on drone operations *per se*.

The Basic Regulation however brought all drones, regardless of their size and weight, within the regulatory scope of the EASA.

Articles 75 and 76 of the BR sets out the harmonised key legal principles and standards as a milestone for the integration of drones in the Single European Sky Strategy (SES). It also emphasise the EASA's monitoring and supervisory functions and introduce rules on the mutual recognition of aviation documents and cross-border cooperation amongst the EU NAAs.

Article 132 of the BR opened the doorway for information privacy into the drone regulatory framework in the EU. This Article provides that the GDPR and the national information privacy laws of member states must be respected, at all times in the implementation of the BR and all implementing legislation.

Additionally, Article 71 of the BR permits member states to endorse national laws which restricts the operation of drones on account of public security and protection of privacy and personal data motives.<sup>522</sup>

In order to implement the BR, the EU adopted the Commission Delegated Regulation (DR)<sup>523</sup> and the Commission Implementing Regulation on the rules and procedures for the operation of unmanned aircrafts (Implementing Regulation (IR)).<sup>525 526</sup>

---

<sup>520</sup> Regulation 2018/1139 of the Europe and Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. *OJ L 212*, 22.8.2018, p. 1–122. Available at < <http://data.europa.eu/eli/reg/2018/1139/oj> >

<sup>521</sup> See Article 57 and 58 of the Basic Regulation.

<sup>522</sup> Zlatko Grigorov, 'The Future of Unmanned Flight (Part 1)' (Kambourov & Partners Attorneys at Law, 21 April 2021) < <https://www.kambourov.biz/en/publications/the-future-of-flight-an-introduction-to-drone-regulations-in-the-eu-and-bulgaria> > accessed 30 May 2022.

<sup>523</sup> Commission Delegated Regulation (EU) 2019/945 of 12 March 2019: on unmanned aircraft systems and on third-country operators of unmanned aircraft systems entered into force & became applicable on 1 July 2019. (*OJ L 152*, 11.6.2019, p. 1–40) Available at < [http://data.europa.eu/eli/reg\\_del/2019/945/oj](http://data.europa.eu/eli/reg_del/2019/945/oj) > accessed 1 Jan 2022.

<sup>525</sup> Commission Implementing Regulation (EU) 2019/947 of 24 May 2019: on the Rules and Procedures for the Operation of Unmanned Aircraft entered into force on 1 July 2019 and became applicable on 31st December 2020(*OJ L 152*, 11.6.2019, p. 45–71) Available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN> > accessed 28 April 2022.

<sup>526</sup> F Fiallos, 'The Applicability of Public International Air Law Regime to the Operation of UAS', In Benjamin Ian Scott (ed) *The Law of Unmanned Aircraft Systems: An Introduction to the Current and Future Regulation under National, Regional and International Law* (Kluwer 2016).

At their core, the IR and DR condense the legal framework for the operation of civil drones in the EU. These regulations offer a risk-based regulatory approach to drones and consequently draw no distinction between leisure or commercial civil drone activities.<sup>527</sup>

The IR essentially sets out the requirements for the design and manufacture of drones intended for the open category (defined below) and the requirements to be met by designers, manufacturers, importers and distributors in order to obtain conformity markings and monitor the market and promote fair competition.<sup>528</sup>

DR sets out a wide-ranging system of unified civil aviation legal rules across a spectrum of three defined categories based on the risks involved in their operations, their mass, and their application.

Complementary to the above-mentioned regulations, in April 2021 the European Commission adopted and published a drone traffic management policy package (referred to as U-space) consisting of three implementing regulations which became operational on 26 January 2023 and will be implemented in four phases.<sup>529530</sup>

Regulation 2021/664 on U-space sets out the rules and procedures such as requirements to submit flight plans and to notify Air Traffic Controllers (ATC) prior to the commencement of a drone operation.<sup>531</sup>

---

<sup>527</sup> Eleonora Bassi, 'European Drones Regulation: Today's Legal Challenges' (2019) International Conference on Unmanned Aircraft Systems (ICUAS) 443–450 < DOI:10.1109/ICUAS.2019.8798173> accessed 30 July 2022; Eleonora Bassi, 'Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance'(2019b) 36 (2) Law in Context. A Socio-legal Journal < <https://doi.org/10.26826/law-in-context.v36i2.114>> accessed 1 April 2022; Eleonora Bassi, 'From Here to 2023: Civil Drones Operations and the Setting of New Legal Rules for the European Single Sky' [2020] Journal of Intelligent and Robotic Systems <<https://doi.org/10.1007/s10846-020-01185-1>> accessed 1 April 2022.

<sup>528</sup> Luis Fernando and Fiallos Pazmiño, *The International Civil Operations of Unmanned Aircraft Systems under Air Law* (Kluwer Law International 2020) 284.

<sup>529</sup> European Civil Aviation Conference (ECAC), 'The new EU regulatory framework for U-space' (UAS Bulletin#2, December 2021) < <https://www.ecac-ceac.org/activities/unmanned-aircraft-systems/uas-bulletin/22-uas-bulletin/505-uas-bulletin-2-the-new-eu-regulatory-framework-for-u-space>> accessed 26 June 2022.

<sup>530</sup> According to its development roadmap, SESAR JU aims to see full deployment of U1 by 2022 and U2 by 2027, with U3 and U4 deployed in the mid-2030s; See SESAR JU, 'U-Space Blueprint'(SESAR JU, 2017) 5 <<https://rpas-regulations.com/community-info/sesar-ju-u-space-blueprint-170616/>> accessed 7 January 2021.

<sup>531</sup> Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space. OJ L 139, 23.4.2021, p. 161–183 Available at <[http://data.europa.eu/eli/reg\\_impl/2021/664/oj](http://data.europa.eu/eli/reg_impl/2021/664/oj)> accessed 26 June 2022; European Civil Aviation Conference (ECAC), 'The new EU regulatory framework for U-space' (UAS Bulletin#2,

Regulation 2021/664 is complemented by two regulations, namely Regulation 2019/666<sup>532</sup> and 2019/665<sup>533</sup> which introduce the necessary modifications to the manned aircraft operations regulations and the existing Air Traffic Management (ATM) or Air Navigation Services (ANS) regulations.<sup>534</sup>

Technical and operational guidance for the implementation of these regulations is offered through guidelines titled Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947 issued by EASA on 10 October 2019.<sup>535</sup> These two documents support the NAAs with the implementation of the laws.<sup>536</sup>

Large segments of the above-mentioned regulations are still in an infant stage, most of the regulations only became operational on 1 Jan 2023.<sup>537</sup>

#### 4. Substantive Information Privacy Provisions

---

December 2021) < <https://www.ecac-ceac.org/activities/unmanned-aircraft-systems/uas-bulletin/22-uas-bulletin/505-uas-bulletin-2-the-new-eu-regulatory-framework-for-u-space>> accessed 26 June 2022; Natia Jiniuzashvili. 'To what extent does the current EU Regulatory Framework for Civilian Drones address Privacy Issues?' (2021) 1(2) Vectors of Social Science <<https://openjournals.ge/index.php/vss/article/view/3635/3870>> accessed 1 April 2022; Eleonora Bassi et al, 'The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win-Win Approach to Data Protection. Aerospace Engineering, and Risk Management (2019) 29 (4) Minds and Machines 579–601.

<sup>532</sup> Implementing Regulation (EU) 2021/666 amends Regulation (EU) No. 923/2012 (laying down the rules of the air (SERA Regulation), establishing the common rules for effectively making the presence of manned aircraft operating in U-space airspace electronically conspicuous. (L 139/187) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2021666>> accessed 26 June 2022.

<sup>533</sup> Implementing Regulation (EU) 2021/665 amends Implementing Regulation (EU) 2017/373, establishing common requirements for air traffic management and air navigation service providers to establish the specific coordination procedures and communication facilities between ATS units, U-space service providers and UAS. (L 139/184) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2021665-0>> accessed 26 June 2022.

<sup>534</sup> Yves Morier, 'Introduction of a regulatory framework for the operation of drones in the open and specific category (Presentation to ICAO 2nd RPAS Symposium 19 September 2021) <<https://www.icao.int/Meetings/RPAS17/Presentations/Yves%20Moirier.pdf>> accessed 20 May 2022.

<sup>535</sup> AMC and GM to Regulation (EU) 2019/947 (Issue 1, Amendment 2)<<https://www.easa.europa.eu/downloads/135910/en>> accessed 12 July 2022.

<sup>536</sup>Dr Analiza Abdilla. 'UAS Regulation Requirements' (Powerpoint Presentation: Civil Aviation Directorate, January 2022) <<https://www.readkong.com/page/easa-drone-regulations-7593667>> accessed 20 May 2022; Damiano Taurino, Drones4Safety: Regulatory Gap/Barriers Analysis (Version 1.0 Release Date: September 14) <<https://drones4safety.eu/wp-content/uploads/2021/01/D2.2-Regulatory-Gap-Barriers-Analysis.pdf>> accessed 2 June 2022.

<sup>537</sup> Maria Rossberg, 'Interim period extended with implementing regulation (EU) (Dronivo, 23 March 2022) <<https://www.dronivo.de/Regulation-Drone-Regulation-2022-EU-Drone-Regulation-2022>> accessed 20 June 2022.

The rest of this chapter will primarily focus on the IR and DR. I will offer a summary of both Regulations, underlining the areas with information privacy significance, and highlighting only aspects that are significant or different from the current RSA and Namibia Civil Aviation Regulations (CARs).

## 5. Classification

The IR classifies the entire scope of drone operations in the EU as either open, specific or certified.<sup>539</sup>

### Open Category ('Buy & Fly')

Article 4 of the IR provides that the *conditio sine qua non* for drone operations in the open category is a maximum take-off mass of less than 25kg, flying at a maximum altitude of less than 120m above the ground that is conducted within visual line of sight (VLOS). Drone operations in the open assemblage are generally considered low menace. This category is factually self-regulated and does not require authorisation from the NAA unless the drone is embedded with a camera or sensor proficient to process personal information, in which instance registration is required.<sup>540</sup>

The Open Category comprise of three (3) operational clusters, A1 (flying over people), A2 (flying close to people) and A3 (flying far from people) attracting varying restrictions depending on the mass of the drone and the certification of the pilot. The three Clusters are further segmented over 6 clusters, bearing labels C0-C6.<sup>541</sup>

### Specific Category

---

<sup>539</sup> Pusztahelyi, Réka, *Recent EU Legislation relating to Drones in the Light of Right to Privacy* (International Multidisciplinary Scientific Conference University of Miskolc, 23-24 May, 2019) ISBN 978-963-358-177-3 < DOI: 10.26649/musci.2019.062> accessed 11 May 2022.

<sup>540</sup> Article 14 of the DR.

<sup>541</sup> Ahmed Alamouri, Astrid Lampert and Markus Gerke, 'An Exploratory Investigation of UAS Regulations in Europe and the Impact on Effective Use and Economic Potential' (2021) 5 MDPI Drones 63 <<https://doi.org/10.3390/drones5030063>> accessed 14 February 2022.

To qualify for the specific designation, drone operations must be deployed over convocations, convey people or dangerous goods. Operations in the specific category are generally operated beyond the visual line of sight (BVLOS).<sup>542543</sup>

Approval for operations in this category can be obtained in four ways.<sup>544</sup>

Firstly, if deployed by a drone operator license holder: A drone operator license is issued after the national civil aviation authority approves an operational risk assessment (SORA) submitted by the applicant.<sup>545</sup>

In terms of Article 11(22) of the IR, SORA should be undertaken for unconventional and composite drone operations.<sup>546</sup> A SORA should follow the methodology developed by JARUS.<sup>547</sup>

This methodology aligns with Article 35 of the GDPR<sup>548</sup> which mandates that a DPIA must be undertaken to identify likely information privacy violations and to put in place mitigating interventions whenever information privacy violations are likely.<sup>549</sup>

According to the EASA guidelines, the current SORA methodology overtly concentrates on ground and air risk only. The present methodology affords little consideration to the information privacy risks of drones. It is my observation that similarly to the CARs the SORA methodology excludes an assessment of the information privacy implications of

---

<sup>542</sup> Article 4 of the IR.

<sup>543</sup> Prof. Dr. Martin Maslaton, 'Drones and European Law Part I: Overview of Hobby & Commercial Drones' (Dedrone, no date supplied) <<https://blog.dedrone.com/en/drones-and-european-law-part-i-what-hobby-and-commercial-pilots-need-to-know>> accessed 1 June 2022.

<sup>544</sup> Article 3(b) of IR stipulates this category requires authorisation in line with Article 12 or an authorisation received in accordance with Article 16, or, under circumstances defined in Article 5(5).

<sup>545</sup> AMC and GM to Regulation (EU) 2019/947 (Issue 1, Amendment 2) <<https://www.easa.europa.eu/downloads/135910/en>> accessed 12 July 2022.

<sup>546</sup> Ahmed Alamouri, Astrid Lampert and Markus Gerke, 'An Exploratory Investigation of UAS Regulations in Europe and the Impact on Effective Use and Economic Potential' (2021) 5 MDPI Drones 63 <<https://doi.org/10.3390/drones5030063>> accessed 14 February 2022.

<sup>547</sup> Carol Martinez and Others, 'SORA Methodology for Multi-UAS Airframe Inspections in an Airport' 2021 5 (4) Drones 141 <<https://doi.org/10.3390/drones5040141>> accessed 10 June 2022; See also <<http://jarus-rpas.org/>> accessed on 4 May 2022.

<sup>548</sup> Article 35 stipulates that 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'.

<sup>549</sup> Carol Martinez and Others, 'SORA Methodology for Multi-UAS Airframe Inspections in an Airport' 2021 5(4) Drones 141 <<https://doi.org/10.3390/drones5040141>> accessed 10 June 2022.

drones.<sup>550</sup> It is my considered view that the SORA methodology should be revised to incorporate an assessment of the information privacy risks of drones.

Secondly, for more streamlined linear drone operations, provision is made for a Pre-defined Risk Assessment (PDRA).<sup>551</sup> PDRAs are common operational circumstances to which prescribed mitigating interventions are ascribed. Operators whose intended operations fall within any of the four (4) PDRA's are exempted from undertaking a SORA and is simply required to undertake to apply the pre-defined mitigating measures identified, for authorisation.<sup>552</sup>

Thirdly, if the drone operations match any of the Standard Scenarios (STS). The IR<sup>553</sup> introduce two Standard Scenarios; STs 1 and STs 2 in respect of drones within the class C5 or C6 classes, as an addition of two new parts in the annex to IR.<sup>554</sup> The amended Regulation sets out the technical requirements that need to be complied with to qualify to operate within either of the STS categories.

STS are considered a measure of expediency, in so far as it relinquishes the duty to undertake a SORA. Instead of conducting a SORA, drone operators are expected to simply file a declaration with their NAA, if their intended operations match any one of the STS and commence their operation provided the safety of the operation has been insured and the necessary mitigation steps have been taken.<sup>555</sup>

---

<sup>550</sup> EASA, 'Guidelines on Design verification of UAS operated in the 'specific' category and classified in SAIL III and IV' (EASA, Issue 1, 31 March 2021) < <https://www.easa.europa.eu/downloads/126318/en>> accessed 10 July 2022.

<sup>551</sup> Article 11 of IR; AMC and GM to Regulation (EU) 2019/947 Issue 1, Amendment 2 < <https://www.easa.europa.eu/downloads/135910/en> > accessed 12 July 2022.

<sup>552</sup> Acceptable Means of Compliance and General Guidance Material to Regulation (EU) 2019/947: AMC & GM to Regulation (EU) 2019/947 (Issue 1, Amendment 2 (EASA, 09 Feb 2022) Available at < <https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2022002r>> accessed 10 July 2022.

<sup>553</sup> Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight. Available at < <https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2020639>> accessed 3 July 2022.

<sup>554</sup> Article 23(4) IR; Part 16 and 17 of the Annexure to the DR.

<sup>555</sup>.AMC and GM to Regulation (EU) 2019/947 (Issue 1, Amendment 2) < <https://www.easa.europa.eu/downloads/135910/en> > accessed 12 July 2022.

The EU Commission has published Regulation (EU) 2022/425, amending Implementing Regulation (EU) 2019/947 which postpones the implementation of the effective date for the STS to 1 Jan 2024.<sup>556</sup>

The fourth alternative is in respect of operations deployed by drone operators (juristic persons that hold a Light UAS Operator Certificates (LUC) with privileges.<sup>557</sup> A LUC is an organisational approval certificate issued by NAA to entities that have demonstrated that they are competent to assess their own operational risks. LUC privileges may include conducting operations covered by STS without submitting the declaration or conducting their own risk assessments and authorising their own flights within the specific category.<sup>558</sup>

It is a requirement that LUC holders must implement and maintain a safety management system consistent with the nature, extent and intricacy of the entity's operations. It may be prudent to impose a similar obligation on LUC holders to introduce and maintain an information privacy management system alongside the safety management system.

The IR obligates all operators within the specific category to retain their records setting out *inter alia* details of their operations, identifying potential risks and mitigating measures, as well as the qualifications and experience of the personnel involved in the operations, for at least 3 years from the date of the operation.<sup>559</sup> These requirements may support the transparency and accountability information privacy principles.

---

<sup>556</sup> The EU Commission has published Regulation (EU) 2022/425, amending Implementing Regulation (EU) 2019/947; Jenny Beechener, EASA, 'Updated EU Regulation 2022/425 postpones transition dates for some BVLOS unmanned operations' (Unmanned Airspace, March 16, 2022) <<https://www.unmannedairspace.info/emerging-regulations/updated-eu-regulation-2022-425-postpones-transition-dates-for-some-bvlos-unmanned-operations/>> accessed 17 July 2022.

<sup>557</sup> Article 12 of the IR; Nico Saputro and Others, 'Privacy-Preserving Control of Video Transmissions for Drone-based Intelligent Transportation Systems' (IEEE Conference on Communications and Network Security (CNS) 2019) < doi: 10.1109/CNS.2019.8802665> accessed 30 May 2022.

<sup>558</sup> The full requirements for a LUC, and the responsibilities and privileges of a LUC holder are included in Part C of the Annex to the IR; See also Wiebe de Jager, 'DRONAMICS first cargo Drone Airline to obtain Light UAS Operator Certificate' (Drone Watch EU, May 25, 2022) <<https://www.dronewatch.eu/dronamics-first-drone-cargo-company-to-obtain-light-uas-operator-certificate/>> accessed 7 July 2022; EASA Pro, 'FAQ: I would like to know about the light UAS operator certificate (LUC)' (EASA Pro, no date supplied) < <https://www.easa.europa.eu/the-agency/faqs/i-would-know-about-light-uas-operator-certificate-luc>> accessed 2 July 2022.

<sup>559</sup> Dr Analiza Abdilla, 'EASA Drone Regulations: Overview and Implementation' (Powerpoint presentation Civil Aviation Directorate, December 2019) <[https://www.transport.gov.mt/Drones\\_Presentation\\_website.pdf-f4647](https://www.transport.gov.mt/Drones_Presentation_website.pdf-f4647)> accessed 1 May 2022;

It is commendable to note that Article 12(1)(c) of the IR obligates operators to deploy their intended operations, subject to applicable privacy and information privacy protection laws. This provision is commendable, unlike the CARs, this Article impose a direct obligation on drone operators and pilots to adhere to information privacy laws.

The requirement to undertake a SORA is in line with Article 35 of the GDPR which requires that a DPIA should be undertaken to determine the information privacy risk of a technology prior to using it.

In the same way, the data retention limitation and the duty to observe privacy laws go a long way in promoting information privacy within the specific category.

These measures may nevertheless be bolstered by implementing by introducing a provision that echoes Article 37 of the GDPR, mandating the appointment of DPO within the organisational structure of data controllers or processors. Resultantly, a provision necessitating the appointment of DPOs within the internal structures of drone operators, particularly operations deployed subject to STS, PDRA or LUC must be considered.

### **Certified Category**

The determinants of this category are specified under Article 40 of the DR. Drone operations in this grouping are considered to pose the greatest risk to people and property.<sup>560</sup> Operations in this category largely operate in congested areas and involves transporting natural persons or hazardous goods with drones measuring more than 3 meters.<sup>561</sup>

Certified drone operations are exclusively undertaken by a certified drone, deployed by a certified operator and a licensed pilot.<sup>562</sup>

---

Anna Konert and Tadeusz Dunin, 'A harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 (3) *Advances in Science, Technology and Engineering Systems Journal* 93-99.

<sup>560</sup> Article 6 of the IR.

<sup>561</sup> Article 6 1 (b) of the IR, read with Article 40 of the DR.

<sup>562</sup> Article 6 (2) of the IR.



Certified drone operations are subjected to regulatory scrutiny equivalent to that of conventional aircrafts. Accordingly, drones in this category must be designed, produced and maintained as per prescribed standards by approved organisations. They are required to be registered with NAA and are subjected to periodical airworthiness assessments<sup>563</sup> and observe strict maintenance obligations.<sup>564</sup>

#### 4. Manufacturing

As mentioned earlier, the DR is primarily aimed at enabling synergy within the EU civil aviation industry. Chapter II read of the DR principally prescribes the technical specifications for the design, manufacture, sale and operation of drones.<sup>565</sup> This chapter is amplified by Annex IX (Essential requirements for unmanned aircraft) of the BR.<sup>566</sup>

Drone manufacturers are obliged to comply with these technical specifications and to put in place quality control measures in line with parts 7 to 9 of the Annexure to the DR.<sup>567</sup> The Manufacturers bear the responsibility to carry out confirmatory assessments with independent standards institutions in order to demonstrate compliance with the mentioned technical specifications.<sup>568</sup> The NAAs are authorised to undertake design

---

<sup>563</sup> Article 10 of the IR; The ICAO RPAS Concept of Operations of March 2017 defines; 'Airworthiness certification considers system configuration, usage, environment, and the hardware and software of the entire system. It also considers design characteristics, production processes, interoperability, reliability, and in-service maintenance procedures that adequately mitigate safety risks. Technical standards may be used to certify specific components of the RPAS' <<https://www.icao.int/safety/UA/Documents/ICAO%20RPAS%20Concept%20of%20Operations.pdf>> accessed July 2017.

<sup>564</sup> Article 3(c) of the IR.

<sup>565</sup> Luis Fernando Fiallos Pazmiño, *The International Civil Operations of Unmanned Aircraft Systems under Air Law* (Kluwer Law International 2020) 284; Anna Konert and Tadeusz Dunin, 'A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 (3) *Advances in Science, Technology and Engineering Systems Journal*, 93-99.

<sup>566</sup> A Alamouri, A Lampert, M Gerke, *An Exploratory Investigation of UAS Regulations in Europe and the Impact on Effective Use and Economic Potential*. 2021 5 (63) *MDPI Drones* <<https://doi.org/10.3390/drones5030063>> accessed 28 April 2022; Eleanora Bassi, 'European Drones Regulation: Today's Legal Challenges' (2019) *International Conference on Unmanned Aircraft Systems (IEEE)* 443-450 <<https://www.semanticscholar.org/paper/European-Drones-Regulation%3A-Today%E2%80%99s-Legal-Bassi/55a901e21bf56a86132722cb8e9d2d7ab59162b6>> accessed 20 June 2022.

<sup>567</sup> Article 6 of the DR.

<sup>568</sup> Recital 18 and 44 of the DR.

verifications<sup>569</sup> and to issue design verification reports, upon a satisfactory verification thereof.<sup>570</sup>

Alterations to a drone subsequent to production or after registration relegate the drone into a category classified as 'privately built' and result in loss of confirmatory status and associated privileges.<sup>571</sup>

### **Information Privacy focused specifications**

The DR mandates that all new drones made available for purchase in the EU must be endowed with *inter alia* a direct remote identification (DRI) system, that permits the live transmission of the operator's ID, the drone's serial number (registration number) and other telemetry information about the drone operation, via various available communications networks within the vicinity of the drone operation.

Drones manufactured without this functionality are expected to procure a separate DRI add-on.<sup>572</sup> In terms of Chapter II of the DR, the DRI functionality is compulsory for operations in the open and specific categories.

The DR also insists that drones should be embedded with location geofencing software to enable drones to be geo-fenced or geo-caged, within geographic zones reserved for information privacy reasons under Article 15 of thereof.<sup>573</sup>

It is also a requirement that the drone must be embedded with a Return to Home (RTH) communication link to avoid it getting lost.

The latest amendments to the IR and DR, further provide that in order to enhance the visibility of drones and to distinguish them from conventional aircrafts, all drones must emit a green flashing light when operating at night.<sup>574</sup>

---

<sup>569</sup> Article 13 of the DR.

<sup>570</sup> EASA, 'Guidelines on Design verification of UAS operated in the 'specific' category and classified in SAIL III and IV' (EASA, Issue 31 March 2021) <<https://www.easa.europa.eu/downloads/126318/en>> accessed 10 July 2022

<sup>571</sup> BMF Administrator 'CAA Publishes CAP1789–Outlining the EU regulations for Unmanned Aircraft '(British Model Flying Association, May 20, 2022)< <https://bmfa.org/caa-publishes-cap1789-outlining-the-eu-regulations-for-unmanned-aircraft>> accessed 20 June 2022.

<sup>572</sup> Part 6 of the DR.

<sup>573</sup> Geo-fencing vs geo-caging; geo-fencing refers to software which hinders a drone from entering a certain geographical location whereas geo-caging software restricts a drone to a specific geographical location.

<sup>574</sup>The fitment of a green flashing light was incorporated as a new product standard for unmanned aircraft in Classes C1, C2 and C3.

All drones embedded with these mandatory features are certified under the C1-C4 drone groupings.<sup>575</sup> As of 1 January 2023, all drones that do not meet the technical requirements outlined in the DR (referred to as legacy drones) will be prohibited from operating in the open category.<sup>576</sup>

Unlike the CARs that are mute on industrial specifications, the EU Regulations referred to above, enforce information privacy protection by prescribing product standards at the engineering and production stage and subjects the manufacturers and engineers to product-specific conformity assessments. These provisions sit well within Article 25 of the GDPR that embodies the PbD information privacy principle, as propounded by Ann Cavoukian.<sup>577</sup>

The mandatory design features further guarantee information privacy compliance, particularly within the open category, which is largely self-regulated and STS, PDRA or LUC operations. Additionally, it also lessens the scope for non-compliance on the part of drone operators and pilots whilst at the same time lightening the compliance and monitoring burden of the NAAs.

From an information privacy perspective, the production specifications like geo-awareness or geo-caging and remote identification<sup>578</sup> enable transparency and enable data subjects to exercise and enforce their rights under the information privacy laws.

## 5. Sale, Labelling and Market Surveillance

---


<sup>575</sup> Anna Konert and Tadeusz Dunin, 'A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 (3) *Advances in Science, Technology and Engineering Systems Journal* 93-99 <[www.astesj.com](http://www.astesj.com)> accessed 30 May 2022.

<sup>576</sup> Article 22 of the DR.

<sup>577</sup> Ann Cavoukian, *Privacy by Design: Take the Challenge* (Information and Privacy Commissioner of Ontario 2009); Ann Cavoukian and Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Canada: Office of the Privacy Commissioner, Ontario, Canada, 2011) and Ann Cavoukian, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011).

<sup>578</sup> This is similar to an existing system used by manned aircraft called Automatic Dependent Surveillance Broadcast (ADS-B). With ADS-B, manned aircraft transmit information about their own flight to other aircrafts, as well as to ATC on the ground. ADS-B tracking websites such as FlightRadar24 <<https://www.flightradar24.com>> accessed 20 July 2021, allow members of the public to see real-time information about aircraft, including their location and their destination; See also Bethany Whitfield, 'How It Works: ADS-B' (*Flying Magazine*, 8 February 2017) <<https://www.flyingmag.com/how-it-works-ads-b/>> accessed 7 January 2021.

In addition to prescribing mandatory production requirements, the DR prohibits the manufacture and sale of products that do not conform with the technical specifications recounted above.

To this end, the DR requires that all drones, associated parts or components and software must be produced in accordance with the prescribed mandatory specifications. It is further required that compliant drones must be endorsed with a Conformité Européenne (CE) marking (as the logo .

The (CE) mark is the European Union's (EU) mandatory conformity endorsement for regulating goods sold within the European Economic Area (EEA).<sup>579</sup> The CE marking represents a manufacturer's pronouncement that goods fulfil the prescribed EU production and supply laws.<sup>580</sup> It is a criminal offence to affix a CE mark to a product that does not comply with the prescribed production standards for sale.<sup>581</sup>

It perhaps deserves mention that the marking referred to above, does not necessarily reflect that the particular drone is information privacy compliant, as envisaged in Article 42 of the GDPR. Article 42 of the GDPR anticipates certification and endorsement by appending data protection seals and marks, to demonstrate that a product or service adheres to the GDPR.<sup>582</sup>

I am of the opinion that it would be judicious that the conformity marking mandated under the DR should additionally require that the drones must be endorsed with an Article 42 marking or that the assessment of conformity for drones should include adherence to the GDPR, within the context of Article 42 of the GDPR.<sup>583</sup>

---

<sup>579</sup> Parts 11& 12 of the Annexure to the DR.

<sup>580</sup>EU Commission, 'CE marking' (EU Commission, no date supplied) <[https://ec.europa.eu/growth/single-market/ce-marking\\_en](https://ec.europa.eu/growth/single-market/ce-marking_en)> accessed 3 July 2022.

<sup>581</sup> Chapter II; Section 3 [Article 14 (5)] of the DR.

<sup>582</sup> Recital 100 of the GDPR; Eric Lachaud, 'What GDPR tells about certification' (2020) 38 Computer Law & Security Review 105457 <<https://doi.org/10.1016/j.clsr.2020.105457>> accessed 1 August 2022.

<sup>583</sup>EDPB, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (EDPB, 22 February 2022) <[https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en)> accessed 1 June 2022.

Section 2 of Chapter II of the DR read with parts 7 to 12 of the annex thereto impose a duty<sup>584</sup> on manufacturers, authorised representatives, importers and distributors<sup>585</sup> (jointly referred to as economic operators) to ensure that the drones supplied by them, conform with the prescribed technical standards. The DR also sets out commitments that are to be observed by drone economic operators and enlists them to play an active role in market surveillance throughout the supply and distribution chain.<sup>586</sup>

The DR further mandates manufacturers to inform the market surveillance authorities of the affected States if a product does not conform with the mandatory specifications. These provisions are exacerbated by Regulation (EU) 2019/1020<sup>587</sup> which entered into force on 16 July 2022. This Regulation insists on continuous market surveillance to protect consumers and businesses across the EU in furtherance of the single EU market agenda. The non-compliant drones will thus be withdrawn or re-called and several penalties may be imposed for supplying drones that do not conform to the prescribed manufacturing standards.<sup>588</sup>

The DR obligates manufacturers of drones intended for operation in the open category, to include their contact information and the registered trade name and or mark on the label or packaging of the drone. As of 1 July 2022, the labelling and advertising of drones must unambiguously specify their registration, operator details, as well as the category of intended operation. Considering that these drones are self-regulated, access to the contact details of the manufacturers enhances accountability.

Unlike the CARs, in line with the co-regulatory governance model and in furtherance of the accountability and transparency information privacy principles stipulated under Article 5 of the GDPR, the EU legal framework on drones binds suppliers of drones as well and mandates them to play an active role in safeguarding information privacy within the civil aviation industry.

---

<sup>584</sup> Through the rapid alert system; See Recital 45 of the DR.

<sup>585</sup> Distributors and Importers are presumed Manufacturers under Article 10 of the DR.

<sup>586</sup> Recital 16, 24 and Article 35 of the DR.

<sup>587</sup> Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance.)  
PE/45/2019/REV/1. OJ L 169, 25.6.2019, p.1–44. Available at <  
<http://data.europa.eu/eli/reg/2019/1020/oj>> accessed 1 August 2022.

<sup>588</sup> Chapter II; Section 5 Article 36 of

## 6. Registration

It is compulsory to register drones with the NAA of the EU country of their residence or principal place of business and to bear their registration numbers perceptibly on its surface,<sup>589</sup> except for drones operating within the open category without a camera or sensor capable of processing personal information, or those classified as a toy (with or without a camera or other sensor) in terms of in DR.<sup>590</sup>

Additionally, to ensure the answerability of operators in respect of the obligations imposed by law, including the GDPR, Article 14(5) of the IR mandates all drone operators to register with the NAA in which they have their principal place of business. Upon registration, the operator is issued with a unique Id code which must be exhibited on the peripheral of each drone belonging to the operator.<sup>592</sup>

Article 14 of the IR also allows the registration of a drone or operator under the umbrella of a model aircraft voluntary association(s).

The registration details are captured in a national register.<sup>593</sup> It is anticipated that by the end of 2024, the EU will have an interoperable centralised registration database in place which will permit database exchange between member states.<sup>594</sup>

NAA's are obliged to maintain a registration system that is information privacy compliant according to Article 18(m) of the DR. Article 18(e) of the DR provides that NAA's must

---

<sup>589</sup> The registration number consist of 16 alphanumeric characters, the first three (3) uppercase letters represent the code of the EU Member State of registration, and the remaining 13 are randomly generated displayed in lowercase.

<sup>590</sup> Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0048&from=EN>> accessed 10 July 2022.

<sup>592</sup> ASD-STAN, 'Direct Remote Id: Introduction To The European UAS Digital Remote Id Technical Standard' ( ASD-STAN, 2021) < [https://asd-stan.org/wp-content/uploads/ASD-STAN\\_DRI\\_Introduction\\_to\\_the\\_European\\_digital\\_RID\\_UAS\\_Standard.pdf](https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf)> accessed 31 May 2022.

<sup>593</sup> The Annex IX of the Regulation lays down the essential requirements for unmanned aircrafts, for the registration of devices and of operators and for the marking of unmanned aircraft, as well.

<sup>594</sup> EASA, 'EASA delivers broker solution to enable European-wide sharing of drone registration data', (EASA Press Release, 22 October 2020) <<https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-delivers-broker-solution-enable-european-wide-sharing-drone>> accessed 7 January 2022.

retain all their records for 3 years from the date of last entry and should update all successive changes thereto.

This obligation denotes that the NAAs should ensure that the storage of personal information in their registration records complies with Article 5(1)(e) of the GDPR which requires that personal information should be stored in a pseudonymised form and that there must be technical and organisational measures in place to prevent unauthorised processing of the data and allows archiving exclusively for journalistic, scientific or historical research or statistical purposes in accordance with Article 89(1) of the GDPR.

<sup>595</sup>

Caution should also be exercised when deleting records, as the GDPR requires deletion in an irrevocable way.<sup>596</sup> This may require much more than simply deleting personal data from the information communication system or server, but may require reformatting old drives and magnetic media including hard drives or audio tapes <sup>597</sup>

Registration and authorisation are welcome responses to the concern that drone operations are inconspicuous. If drone operators cannot be identified, it hampers the ability to hold those who infringe the information privacy rights of others accountable or to exercise the data subject rights provided by the GDPR and to facilitate the intervention of authorities.

## 7. Pilot Training

### Training

The minimum age for a drone pilot in the EU is 16 years, deviations in national legislation are however permissible.<sup>598</sup> Drone pilots are required to meet the competency

---

<sup>595</sup> Article 5 GDPR sets out data protection principles.

<sup>596</sup> F.G.Wilman, 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations' (2022) 46 *Computer Law & Security Review* 105728 < <https://doi.org/10.1016/j.clsr.2022.105728> > accessed 25 August 2022.

<sup>597</sup> Kayla Matthews, 'What you need to know about Data Destruction Post-GDPR' (Spiceworks, November 27, 2018) < <https://www.spiceworks.com/it-security/data-governance/guest-article/what-you-need-to-know-about-data-destruction-post-gdpr/> > accessed 31 July 2022.

<sup>598</sup> Article 9 of the IR.

requirements of the group of operations they intend to operate in. The STS, PDRA and LUC designate the competency pilots operating thereunder, must possess.<sup>599</sup>

Article 8 of the IR provides that any pilot who intends to fly a drone must be acquainted with the manufacturer's manual and receive a basic level of competency training and pass an online theoretical knowledge examination.<sup>600</sup> The theoretical online examination is foundational drone training and is mandatory for all drone pilots.<sup>601</sup>

I am pleased to learn that the curriculum of this rudimentary training includes training on privacy and information privacy protection.<sup>602</sup>

Pilots who envisage operations in specific and certified drone operation groupings must acquire a Remote Pilot Competency Certificate. Training to obtain a Remote Pilot Competency Certificate encompasses undergoing training with either an NAA or an approved external training organisation.<sup>604</sup> Competency assessment for the specific category range between the 'rudimentary' required in the open category to a staffed aircraft pilot's licence in proportion to the risk identified.<sup>605</sup>

Pilot licensing requirements for the specific drone sort are the same as that of the conventional aircraft pilot, which is stricter.<sup>606</sup>

It is creditable to note that, even at the entry-level (open category), emphasis is placed on the inclusion of information privacy protection within the syllabi of the drone personnel training. It is my opinion that this training complements the information privacy

---

<sup>599</sup> Damiano Taurino, 'Drones4Safety: Regulatory Gap/Barriers Analysis' (Drones4Safety, Version 1.0 14 September 2020) <<https://drones4safety.eu/wp-content/uploads/2021/01/D2.2-Regulatory-Gap-Barriers-Analysis.pdf>> accessed 2 June 2022.

<sup>600</sup>The full competency training requirements for all three subcategories in the Open category are included in Part A of the Annex to IR.

<sup>601</sup> This training is a pre-requisite for all other competency training and certifications.

<sup>602</sup> Damiano Taurino, 'Drones4Safety: Regulatory Gap/Barriers Analysis' (Drones4Safety, Version 1.0 14 September 2020) <<https://drones4safety.eu/wp-content/uploads/2021/01/D2.2-Regulatory-Gap-Barriers-Analysis.pdf>> accessed 2 June 2022.

<sup>604</sup> Mateusz Gregorski, 'Legislative changes regarding unmanned rights as an opportunity for professional empowerment of persons with disabilities' (2019) 4 *Przegląd Europejski* <doi: 10.5604/01.3001.0013.7888> accessed 21 June 2022.

<sup>605</sup>CAP 1789 - The EU UAS Regulation Package – Outline (June 2022 Update) <<https://uavacademy.co.uk/wp-content/uploads/2020/03/CAP1789-June-2022.pdf>> accessed 17 July 2022.

<sup>606</sup> Dublin City Council, 'Regulations: Drone User Handbook' (not supplied) <<https://smartdublin.ie/wp-content/uploads/2021/12/Regulations-Drone-User-Handbook-V1.pdf>> accessed 17 July 2022.



protection agenda in the drone arena well and will significantly contribute to developing an information privacy institutional culture within the drone industry.<sup>607</sup>

### **Obligations of the Pilot**

The obligation is to ensure that the drone operation is safe and lawful vests in the drone pilot. To this end, the recital of the IR accentuates that all drone operators and remote pilots are required to comply with European and national rules regarding information privacy protection. They are also required to familiarise themselves with the geographical zones demarcated pursuant to Article 15 of the IR on account of environmental, security or privacy reasons. They are also expressly mandated to assess whether the drone is fit for function and to cooperate with relevant air traffic service providers (ATS) and other relevant stakeholders.<sup>608</sup>

They are further responsible for executing their operations only if they are physically and psychologically fit to do so and to bear evidence of competency at all times.

Although the duty imposed on drone operators and pilots to respect information privacy laws is laudable, and while it should also be acknowledged that penalties for infringing the unauthorised processing of personal information by drones may be imposed under the GDPR, it is nevertheless a serious shortcoming that no sanctions are provided in the EU drone regulations, for failing to observe the provisions on information protection privacy in particular and non-compliance with regulations within the civil aviation regulatory environment.

Neither is there an obligation to at least notify the DPA of information privacy infringements that poses a risk to an individual's rights and freedoms as required under Article 33 and 34 of the GDPR and section 22 of POPIA.

## **8. Cross-Border and Third-Party Drone Operations**

---

<sup>607</sup> Pusztahegyi, Réka, *Recent EU Legislation relating to Drones in the light of right to Privacy* (International Multidisciplinary Scientific Conference University of Miskolc, 23-24 May, 2019) ISBN 978-963-358-177-3 < DOI: 10.26649/musci.2019.062> accessed 11 May 2022.

<sup>608</sup> Boris Galkin, *Spotlight No. 1 of 2021: Consumer and Commercial Drones* (Library & Research Service 10 February 2021) <[https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2021/2021-02-11\\_spotlight-consumer-and-commercial-drones-how-a-technological-revolution-is-impacting-irish-society\\_en.pdf](https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2021/2021-02-11_spotlight-consumer-and-commercial-drones-how-a-technological-revolution-is-impacting-irish-society_en.pdf)> accessed 26 May 2022; Ishveena Singh, 'Traveling across and outside Europe with a drone?' (DroneDJ, 17 December 2021) < <https://dronedj.com/2021/12/17/holiday-travel-europe-drone-rules/>> 1 January 2022.

As contemplated under SES, Article 41(3) of the DR contemplates the mutual recognition of civil aviation documents amongst EU member states.<sup>609</sup> Non-EU operators and pilots will however have to undergo all required assessments and certifications to operate in the EU.<sup>610</sup>

These provisions undoubtedly promote expediency and alleviates bureaucracy and red tape, rendering inter-country drone operations relatively seamless. However similar to the CARs that there has been an oversight regarding information privacy risks involved in cross-border drone operations. Mindful that a drone itself or its payloads may contain personal information that will be imported or exported in the course of cross-border operations. Operators and pilots must, therefore, adhere to Article 44 of the GDPR and section 72 of POPIA in such instances. Article 44 of the GDPR restricts the transfer of personal information outside the EU to jurisdictions that are unable to offer data subjects protection against unlawful processing of personal information equivalent to that under the GDPR. Section 72 of the POPIA contains a corresponding provision.

In light of the Court of Justice of the European Union (“CJEU”) judgement on 15 June 2021 in the *Facebook Ireland Limited, Facebook Inc; Facebook Belgium BVBA v. the Belgian Data Protection Authority* (“Belgian DPA”) case.<sup>611</sup> In this matter, the CJEU examined the question of whether a national supervisory authority that is not the lead supervisory authority under the GDPR one-stop-shop mechanism may bring legal proceedings against a company for GDPR violations before a court in its member state. The court ruled that a supervisory authority (DPA) of a member state which is not the ‘lead supervisory authority’ is permitted to assume jurisdiction in respect of a GDPR breach if the cooperation mechanisms under the GDPR are followed.

I am of the view that the IR should be amended to address the interplay between the information privacy risk posed by cross-border drone operations and the domestic information privacy legislation of the respective EU states.

---

<sup>609</sup>Drone registration and certifications, personnel qualifications and competency assessments.

<sup>610</sup> See Article 129 (Participation of European third countries) of the BR.

<sup>611</sup> C-645/19. < <https://www.dpcuria.eu/case?reference=C-645/19>> accessed 22 December 2022

## 9. Enforcement

Chapter IV of the BR delineates the oversight and enforcement mechanisms and power of the NAAs, in instances where it is delegated to the EASA. Article 62 of the BR provides that EU member states must establish a competent authority to exercise oversight and enforce the package of drone regulations regulation and associated implementing legislation, discussed above.

In instances where there is a shortage of expertise, member states are authorised to delegate their oversight and enforcement powers to the EASA or another EU member state.<sup>612</sup>

Article 63 of the BR further makes provision for the formation of a voluntary pool of inspectors and other experts for purposes of ensuring equal access to expertise and skills transfer within the EU.

Article 17 of the IR authorise EU states to designate a competent authority responsible for executing the task enumerated under Article 18 thereof.<sup>613</sup>

Article 18 of the IR enumerates the registration of drones, technical, security and personnel assessments and confirmation, and the gathering and publication of important safety and security statistics as the major enforcement activities to be performed by the NAAs. It is noted with concern that analogous to the CARS, the task listed under Article 18 excludes reference to privacy and information privacy protection and is mute on which institution and how the information privacy obligations introduced under the regulations will be monitored and enforced.

Notwithstanding the progressive pro-information privacy protections introduced by the laws discussed in this chapter, it is axiomatic that the efficacy of these laws and policies depends on the efficiency of the implementation and enforcement methodology adopted and requires specialised enforcement technology and infrastructure, as well as imperative upskilling of the civil aviation personnel's consciousness and expertise.

---

<sup>612</sup> Article 62(2) of the Basic Regulation.

<sup>613</sup>The Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947 informs that Member States are at liberty to designate several Institutions and not necessarily just their National Aviation Authorities.

Notwithstanding the above, the EU drone regulations do not offer insight into the enforcement and monitoring methodologies, infrastructure and technologies which will be employed to monitor and enforce the information privacy provisions introduced.

It is my view that in the absence of insight into the enforcement methodology and technologies, the information privacy provisions introduced by the regulations discussed above simply constitute formal compliance with the GDPR.

Arguably, the implementation and enforcement of the pro-information privacy laws deliberated above vest in the supervisory authorities designated under Article 51 of the GDPR. However, as evident from the foregoing discussion, the observance of information privacy within the context of drones is intricately linked to the overall technical and operational requirements across the entire drone regulatory spectrum. Moreover, bearing in mind the exceedingly specialised and methodological nature of the aviation industry in general, and the complexity of the rules on drones in particular, which are foundational to ensuring information privacy protection across the drone regulatory spectrum. It would therefore be a challenge for any DPA to effectively monitor and enforce the information privacy protection principles without having technical civil aviation expertise and vice-versa.

I am therefore of the considered view that, placing the mandate to promote, monitor and enforce information privacy protection within the drone industry (or the greater civil aviation industry) external to the regulatory jurisdiction of the civil aviation authorities would hamper the efficacious implementation of the information privacy focused drone regulations.

For example, to determine whether or not a violation of the GDPR (or POPIA) has occurred, the DPA will inevitably have to assess the technical and operational requirements under the BR, DR and IR. It is therefore my view that vesting the implementation and enforcement mandate and functions of the pro-information privacy drone regulations in the DPAs established under Article 51 of the GDPR (instead of the civil aviation authorities) would be a duplication of resources and functions and will give rise to ambiguity in the jurisdictional roles of the relevant authorities.

I am of the opinion that it is temerarious to isolate the enforcement of information privacy protection within the context of drones, from the technical and operational regulatory oversight thereof. Accordingly, I recommend that the civil aviation authority must assume the mandate to implement, monitor and enforce information privacy protection within the drone industry.

However, in line with the co-regulatory governance model, the above-mentioned mandate should be exercised in collaboration with the DPA in accordance with the principle of subsidiarity. In addition to this, there is a need for ongoing training and cross-training to develop competencies and expertise on both the information privacy and civil aviation regulatory ends, as well.

Another possible intervention to avoid blurring jurisdictional roles in ensuring the enforcement and implementation of information privacy in the drone industry (or the greater civil aviation industry) is to develop and submit a civil aviation (drone) industry code of conduct, as contemplated under Article 40 of the GDPR.

The GDPR industry codes of conduct are approved frameworks setting out industry-focused strategies and procedures, as well as voluntary accountability mechanisms to comply with the GDPR.<sup>616</sup>

Article 40(2) (i) -(k) of the GDPR, provides that a code of conduct must provide for an avenue to exercise and or enforce data subject rights.<sup>617</sup> Chapter 3 of the GDPR also requires that a code must specify out-of-court dispute resolution mechanisms to enable data subjects' rights to enforce their rights under the GDPR and the code of conduct.

Article 40(4) of the GDPR provides that a code of conduct may stipulate methodologies that empower an approved entity to carry out the mandatory monitoring of compliance

---

<sup>616</sup> Articles 40, 41 46 98, and 99 of the GDPR are applicable to Codes of Conduct; Anneliese Roos, 'Data Privacy Law': In Dana Van der Merwe (Med), *Information and Communications Technology Law* (3rd ed, LexisNexis, 2021) 520. Krzysztof Grabowski, 'GDPR industry codes of conduct' (Crowe, 12/11/2021) <<https://www.crowe.com/pl/en-us/insights/gdpr-industry-codes-of-conduct>> accessed 17 July 2022.

<sup>617</sup> Articles 12-23 of the GDPR; - 'The GDPR Data Subject Rights' (OneTrust, 24 May, 2021) <[https://www.onetrust.com/blog/the-gdpr-data-subject-rights/#:~:text=Right%20to%20object%20\(GDPR%20Article,automated%20decision%20making%20or%20profiling](https://www.onetrust.com/blog/the-gdpr-data-subject-rights/#:~:text=Right%20to%20object%20(GDPR%20Article,automated%20decision%20making%20or%20profiling)> accessed 12 July 2022; Bob Swanson, 'Understanding the Fundamental Rights of the Data Subject and establishing your Data Privacy Program with SOAR' (Swimlane, 20 Aug 2020) <[https://swimlane.com/blog/establishing-your-data-privacy-program-with-soar?gclid=Cj0KCQjwidSWBhDdARIsAloTVb1Z5Mm1QXF5SIMIDz0tILAsWE0wv8mji0omM6f4ojDGinksiGEECRZYaAqOTEALw\\_wcB](https://swimlane.com/blog/establishing-your-data-privacy-program-with-soar?gclid=Cj0KCQjwidSWBhDdARIsAloTVb1Z5Mm1QXF5SIMIDz0tILAsWE0wv8mji0omM6f4ojDGinksiGEECRZYaAqOTEALw_wcB)> accessed 12 July 2022.

with its provisions by the controllers or processors which undertake to apply it,<sup>618</sup> without prejudice to the tasks and powers of the data protection supervisory authorities.<sup>619</sup>

In the course of my research, I came across a draft *EU Privacy Code of Conduct: A Practical Guide for Privacy and Data Operators and Pilots*<sup>620</sup>. Paragraph 4.5.2 of the draft code<sup>621</sup> indicates that this is being reviewed by industry representatives, in preparation for legal recognition under Article 40 of the GDPR.

It is however my opinion that owing to the absence of mechanisms to facilitate the exercise and enforcement of data subject rights, as well as specifications on the consequences of non-adherence to the rules under the code; in its present form the code does not comply with all requirements of Article 40 of the GDPR and still requires a lot of work.

My final thoughts in this regard are that the civil aviation authorities should assume accountability to monitor and enforce information privacy compliance within the drone industry. These authorities must adopt a drone industry code of conduct through the prescribed procedures<sup>622</sup> to properly contextualise the implementation, monitoring and enforcement of the information privacy protection agenda within the industry. The code should most importantly set out mechanisms to enable data subjects to exercise and enforce their information privacy protection rights. In order to give the information privacy agenda a bite, the code should impose administrative penalties such as withholding or suspending or revoking civil aviation documents and authorisations, for contraventions of the code or the information privacy laws (in this case the GDPR).

## 10. Safety, Security and Maintenance

---

<sup>618</sup>EDPB, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (EDPB, 02 April 2019) < [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring_en) > accessed 1 June 2022 EDPB; 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (EDPB, 22 February 2022) < [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en) > accessed 1 June 2022.

<sup>619</sup> Article 55 or 56 of the GDPR.

<sup>620</sup> Available at < [https://dronerules.eu/assets/files/PCC\\_DR\\_final-for-printing\\_9-November-2018.pdf](https://dronerules.eu/assets/files/PCC_DR_final-for-printing_9-November-2018.pdf) > accessed 13 December 2022.

<sup>621</sup> Page 34.

<sup>622</sup> Article 40 of the GDPR.

In line with Regulation (EU) 376/2014,<sup>623</sup> drone operators are duty-bound to report safety-related occurrences. Regulation (EU) No 376/2014 aims to improve aviation safety in the EU and globally by ensuring that relevant safety information relating to civil aviation is reported, collected, stored, protected, exchanged, disseminated and analysed.<sup>624</sup>

Article 19 of the IR stipulates that the NAA is *inter alia* responsible for submitting all serious safety and security occurrences to the European central repository (ECR) managed by the EC, within 72 hours thereof or any such period reasonably thereafter. A comprehensive list of mandatory reportable occurrences are detailed in the IR.<sup>625</sup>

The requirement to report serious safety and security occurrences offers the aviation industry a tool to maintain a perspective on safety and security and informs ongoing reforms. Save for reference to report cybersecurity drone occurrences,<sup>626</sup> the regulations does not impose an obligation for mandatory reporting of information privacy contraventions, as contemplated in terms of section 72 of POPIA and Articles 33 and 34 of the GDPR.

It is my opinion that it will be prudent to put in place a similar reporting mechanism to monitor the number of information privacy violations occasioned by drones and to develop a corresponding occurrence reporting mechanism in respect of information privacy violations, to inform future reform initiatives, and will encourage greater compliance with the drone regulations and hopefully a more information privacy-consciousness in the industry.

---

<sup>623</sup> Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007. OJ L 122, 24.4.2014, p. 18–43. Available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0376>> accessed 17 July 2022.

<sup>624</sup> Andrija Vidović and Others, 'Operations of Drones in Controlled Airspace in Europe' 2019, 9(1) International Journal for Traffic and Transport Engineering 38-52 < DOI: [http://dx.doi.org/10.7708/ijtte.2019.9\(1\).04](http://dx.doi.org/10.7708/ijtte.2019.9(1).04)> accessed 1 June 2022.

<sup>625</sup> Commission Implementing Regulation (EU) 2015/1018 of 29 June 2015 laying down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 of the European Parliament and of the Council (Text with EEA relevance) OJ L 163, 30.6.2015, p. 1–17 Available at < <https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-20151018>> accessed 17 July 2022.

<sup>626</sup> Article 19 of the IR.

## 11. Insurance

Aviation insurance in the EU is delimited under Regulation (EC) 785/2004.<sup>627</sup> This Regulation requires all unmanned aircrafts, other than those with a maximum takeoff mass of less than 20kg which is being used for sporting or recreational purposes, to be insured for third-party risks for at least 1 million euros, proof of insurance is a pre-requisite for registration.<sup>628</sup>

Mindful that Article 83(5) of the GDPR imposes fines of twenty million euros, or in the case of an undertaking, up to 4% of their total global turnover of the preceding fiscal year, whichever is higher. Article 83(4) of the GDPR (which deals with less severe violations) contemplates fines of up to ten million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding financial year, whichever is higher.<sup>629</sup>

Considering the fact that the GDPR contemplates the award of ten million Euros for loss and damages suffered for contravening any of its provisions. The insured amount of one million Euros required under Regulation 785/2004 may not be sufficient to reimburse aggrieved data subjects for loss and damages suffered that were occasioned by drones. up to make allowance for information privacy violations, I recommend that the mandatory drone insurance must be scaled-up to an amount proportional to the penalties imposed under GDPR.<sup>630</sup> In the absence of proportional insurance, the

---

<sup>627</sup> Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators  
Select: 1 OJ L 138, 30.4.2004, p.1–6 Available at < <http://data.europa.eu/eli/reg/2004/785/2020-07-30>> accessed 17 July 2022.

<sup>628</sup> Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators  
OJ L 138, 30.4.2004, p. 1–6 Available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0785&from=EN>> accessed 20 June 2022.

<sup>629</sup> Compared to Article 13 (Fines and periodic penalty payments and maximum amounts) of Commission Implementing Regulation (EU) No 646/2012 of 16 July 2012 laying down detailed rules on fines and periodic penalty payments pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council Text with EEA relevance  
OJ L 187, 17.7.2012, p. 29–35 Available at < <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32012R0646>> accessed 31 July 2022.

<sup>630</sup> Lorenzo Dalla Corte, 'On proportionality in the data protection jurisprudence of the CJEU Get access Arrow' [2022] International Data Privacy Law Journal <<https://doi.org/10.1093/idpl/ipac014>> accessed 29 July 2022.



information privacy protection contemplated is merely academic, as the likelihood that data subjects will obtain effective redress is nominal.<sup>631</sup>

Furthermore, it may also be necessary to amend the aforesaid regulation to expressly stipulate that the insurance can be used for information privacy violations under the GDPR or domestic laws of the EU member states. This should include the administrative fines that can be imposed under Article 84 of the GDPR or the civil aviation code of conduct.<sup>632</sup>

## 12. Evaluation of the EU Legal Framework on Drones

The information privacy mandate regarding drones was infused into the civil aviation regulatory framework by Article 132 of the BR. Article 132 of the BR enjoins EU member states to accord due respect to the GDPR and all national laws on privacy and information privacy in the implementation of the BR and its implementing legislation.<sup>633</sup>

The EU legal framework on drones also incorporates the DPD and DPIA principles contained under Articles 25 and 35 of the GDPR in commendably pragmatic ways, by prescribing product specifications and imposing mandatory information privacy functionalities, in respect of the design and manufacturing of drones.<sup>634</sup>

Moreover, the mandatory safety features, particularly the RDI, geo-fencing and greenlights, marking and labelling requirements allay the information privacy concerns raised in the preceding chapters excellently.

---

<sup>631</sup> Dr. Sebastian Golla, 'Is Data Protection Law Growing Teeth? The current lack of sanctions in Data Protection Law and Administrative Fines under the GDPR' (2017) 8 (1) *Journal of Intellectual Property, Information Technology and E-Commerce Law* < urn: nbn:de:0009-29-45332> accessed 20 May 2022; See also '30 Biggest GDPR Fines So Far 2020, 2021, 2022 (Tessian, 05 May 2022) < <https://www.tessian.com/blog/biggest-gdpr-fines-2020/>> accessed 17 July 2022 ; CMS.Law 'GDPR Enforcement Tracker' (CMS.Law, no date supplied)< <https://www.enforcementtracker.com/>> accessed 17 July 2022.

<sup>632</sup> See Article 83 GDPR (General conditions for imposing administrative fines) and Art. 84 GDPR (Penalties).

<sup>633</sup> Nehaluddin Ahmad and Others, 'Unregulated drones and an emerging threat to right to privacy: A critical overview' (2021) 4(2) *Journal of Data Protection and Privacy* 124-145 <<https://hstalks.com/article/6238/unregulated-drones-and-an-emerging-threat-to-right/>> accessed 1 Jan 2022.

<sup>634</sup> Article 14 (5)(a) (iii) of the IR; Eleonora Bassi and Ugo Pagall, 'The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human Rights, and the Free Movement of Data in the EU' (2020) 30 *Minds and Machines* 439–455 < <https://doi.org/10.1007/s11023-020-09541-8>> accessed 1 April 2022.

Through the inclusion of the mandatory safety features, the EU legal framework on drones implements the proportionality principle, whilst simultaneously eliminating voluntary compliance; narrowing the scope for non-compliance and regulatory inefficiencies that may have otherwise occurred in absence of the mandatory features.<sup>635</sup>

Moreover, the EU regulation package embrace the co-regulatory information privacy protection model and entrenched the accountability and the third-generation information privacy principles such as PbD through mandatory technical design and manufacturing requirements.<sup>637</sup>

Information privacy is also promoted through the requirement that all drones embedded with a payload with information privacy intruding functionalities, must be registered. As a consequence, all drones with privacy intruding potential are rendered individually identifiable. The compulsory registration, classification and labelling requirements further enable holding persons contravening the information privacy of others by means of drones accountable across the drone regulatory spectrum.<sup>638</sup>

Enlisting suppliers of drones to undertake conformity assessments, requiring confirmatory endorsement for the sale of drones and imposing a duty on drone suppliers to actively participate in market surveillance are further amiable information privacy provisions.

---

<sup>635</sup> Mario Sabatino Riontino. 'Drones, UAV and Data Protection in the EU'(Celantur, 09 February 2021) <<https://www.celantur.com/blog/drones-uav-data-protection-eu/>> accessed 26 June 2022.

<sup>637</sup> Ludovica Mosci, 'EU rules on drones on the launching pad'(DLA Piper, 4 July 2018)<<https://blogs.dlapiper.com/iptitaly/2018/07/eu-rules-on-drones-on-the-launching-pad-%F0%9F%9A%80/>>1 June 2022; Ann Cavoukian, Privacy by Design and the Emerging Personal Data Ecosystem ( Canada: Office of the Privacy Commissioner, Ontario, Canada, 2012); Cavoukian A, Privacy by Design The 7 Foundational Principles (Information and Privacy Commissioner, Ontario, Canada, 2009, revised January 2011) 106.

<sup>638</sup> Eleonora Bassi and Ugo Pagall, 'The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human Rights, and the Free Movement of Data in the EU' (2020) 30 Minds and Machines 439–455 < <https://doi.org/10.1007/s11023-020-09541-8>> accessed 1 April 2022.

<sup>638</sup> Eleonora Bassi et al, 'The Design of GDPR-Abiding Drones through Flight Operation Maps: A Win-Win Approach to Data Protection. Aerospace Engineering, and Risk Management (2019) 29 (4). Minds and Machines 579–601.

Outstandingly, the inclusion of privacy and information privacy protection in the syllabi of drone pilots also goes a long way in sensitizing the industry and avoiding information privacy violations occasioned by drones.

Other pertinent information privacy enablers include the leeway to impose restrictions in respect of information privacy-prone geographical locations (geo-fencing and geo-caging), as a measure to protect *inter alia* information privacy under Article 15 of the DR. The envisaged U-Space flight map requirements which will permit geo-fencing or geo-caging from areas where the probability of processing personal and sensitive information is high is also a welcome information privacy protection consideration under the EU drone regulations.

For purposes of the GDPR, a drone operator may be regarded as a data controller in terms of the GDPR, if they capture personal information in the course of their operations.<sup>639</sup>

Being a data controller or processor,<sup>640</sup> Article 6 of the GDPR permits the processing of personal information in the absence of consent, provided that it is in the public interest or as part of the official authority or legal obligation of the drone operator stipulated under the law. Processing personal information is also justifiable if it is to protect the vital interests of an individual or in pursuit of the legitimate interests of the operator or a third party. Therefore, save for instances where the exemption for a purely personal or household activity justifies it, or when the operator is processing pseudonymized or anonymised personal information, the drone operator must adhere to the GDPR.

---

<sup>639</sup>Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (Clarus Press, 2017) 107; Anton McNulty, 'No privacy legislation on drones flying over homes' (Mayo News, 3 March 2020) <<https://www.mayonews.ie/news/35028-no-privacy-legislation-on-drones-flying-over-homes>> accessed 30 June 2022. Dr. Boris Galkin, 'Spotlight: Consumer and Commercial Drones' (Library & Research Service 10 February 2021) <[https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2021/2021-02-11\\_spotlight-consumer-and-commercial-drones-how-a-technological-revolution-is-impacting-irish-society\\_en.pdf](https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2021/2021-02-11_spotlight-consumer-and-commercial-drones-how-a-technological-revolution-is-impacting-irish-society_en.pdf)> 26 May 2022.

<sup>640</sup> DPC, 'Guidance Note: Legal Bases for Processing Personal Data' (Ireland Data Protection Commission, December 2019) 16 <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>> accessed 7 January 2022.

The parameters of the exemption for a purely personal or household activity were deliberated on by the Court of Justice of the European Union in the case of *František Rynes v Úřad pro ochranu osobních údajů* which held that a video recording by an individual of his family home to protect the property, but which also monitored an adjacent public space, did not fall within this exemption.<sup>641</sup>

Similarly, in *Tietosuoja- ja valtuutettu v Jehovan todistajat*<sup>647</sup> the CJEU had to evaluate whether the collection of personal data by members of the Jehovah's Witness community was covered under the purely personal or household activity exemption. The court concluded that:

an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner [...].<sup>648</sup>

In compliance with Article 25 of the GDPR, drone operators are also responsible to put in place technical and organisational measures to safeguard personal data processed by the drones during the flight and when storing and transporting the drone across borders, to avert unauthorised processing of data.<sup>649</sup>

The PbD and DPIA requirements set out in Articles 25 and 35 of the GDPR also find expression through the SORA, STA and PRDA methodologies.

The duty imposed on drone operators and pilots to respect privacy and information privacy protection laws also greatly amplifies information privacy protection in the industry if strictly enforced.

Regrettably, there is still a lot of ambiguity regarding the monitoring and enforcement methodologies that will be employed to translate these commendable substantive pro-

---

<sup>641</sup>Rynes v Úřad pro ochranu osobních údajů (Case C-212/13) EU:C:2014:2428 [Judgment of 11 December 2014]. C-212/13 [2014] All ER (D) 124 (May).

<sup>647</sup> (Case C-25/17); Edward S. Dove and Jiahong Chen, 'To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices?' [2020] *Journal of Law, Medicine & Ethics* < <https://doi.org/10.1177/1073110520917046> > accessed 28 April 2022.

<sup>648</sup> Tietosuoja- ja valtuutettu v Jehovan todistajat (CJEU, Case C-25/17), paras 42, 44-45.

<sup>649</sup> Jeremiah Karpowicz, 'How has GDPR reshaped the way drone stakeholders should approach data privacy?' (Commercial Drone News, 17 July 2019) < <https://www.commercialuavnews.com/europe/gdpr-drone-data-privacy> > accessed 31 May 2022.

information privacy drone laws into actual information privacy protections within the drone industry.

It is also a perceptible challenge to invest in the infrastructure and technologies to enforce the information privacy protection contemplated in the EU Regulations on drones.

### **13. Chapter Conclusion**

As acclaimed by Alamouri and co-authors, although cumbersome and embedded with application hiccups, the EU legal framework on drones epitomizes a momentous stride towards harmonising the laws regulating drones in the EU.

In addition to harmonising, the EU drone regulatory package discussed in this chapter is an amiable template to address the information privacy challenges of the drone industry and offers light to the regulatory darkness that has loomed around this subject, all this while.

Notwithstanding, the concerns regarding the lack of monitoring and enforcement infrastructure and the lack of expertise to monitor and enforce information privacy within the drone industry, the EU drone regulatory legal framework propositions solid lessons, on how to address the information privacy risk posed by drones, to glean from.

From a substantive law point of view, the EU legal framework on drones is significantly information privacy protection responsive. It demonstrates enthusiasm to protect the right to information privacy within the drone regulatory landscape.

However, the information privacy protection monitoring and enforcement mechanisms are indeterminate at this stage and are likely to be undermined by the lack of enforcement infrastructure and the expertise to implement monitor and enforce the regulations.

It is my finding that similar to CARs the drone industry leaders in the EU divested themselves from the accountability to implement, monitor and enforce information privacy protection within the drone regulatory spectrum, but instead delegated their responsibility to unspecified persons, possibly DPAs, that will invariably lack the

technical capability to effectively give utterance to the information privacy aspirations in the legal instruments discussed.

Consequently, time will tell whether the drone laws adopted in the EU will translate into the intended practicable information privacy protection within the drone industry

## Chapter Six

# Information Privacy within the Global Drone Civil Aviation Regulatory Regime

---

*This chapter investigates the place of information privacy within the scope of the global civil aviation regulatory regime. It investigates the methodology adopted by ICAO to address the information privacy challenges highlighted in this thesis, as well as the avenue(s) available within the regulatory spectrum of the ICAO to address the information privacy implications of drones, if any.*

### 1. Introduction

The development of drone technologies dawned on the civil aviation industry worldwide like a bombshell.<sup>652</sup> Resultantly, the aerospace industry is still grappling with finding an appropriate methodology to efficiently integrate drones into the civil aviation industry.

In the words of Abeyratne, 'the Chicago Convention is the *Magna Carta*<sup>653</sup> of the international civil aviation industry'.<sup>654</sup> The ICAO was constituted under the Chicago Convention and is primarily responsible for implementing the Chicago Convention.

The Manual on Remotely Piloted Aircraft Systems (RPAS Manual)<sup>655</sup> maintains that ICAO's role in relation to drones is to coordinate the establishment of an international regulatory framework on drones through adopting Standards and Recommended

---

<sup>652</sup> Michael Ashkenazi, 'The Future of UAVs: Lessons from the "Great War' (2016) 34 (4) *Sicherheit und Frieden (S+F) / Security and Peace* 257-262 < <https://www.jstor.org/stable/26429020>> accessed 1 December 2022; Sarah Jane Fox, 'The 'risk of disruptive technology today (A case study of aviation enter the drone') [2020] *Technology in Society* < [https://repository.uel.ac.uk/download/feb8ef6abb4dd5c58cc91faf902bfb1c9499a358d18ea9018e049b088b90b371/705566/Policing%20Drones%202.05.2020\\_3-ACCEPTED.pdf](https://repository.uel.ac.uk/download/feb8ef6abb4dd5c58cc91faf902bfb1c9499a358d18ea9018e049b088b90b371/705566/Policing%20Drones%202.05.2020_3-ACCEPTED.pdf)> accessed 20 December 2022; Sarah Jane Fox, 'Policing challenges in the Cyber and Autonomous era ( Presentation at the International Conference on Cyberlaw, Cybercrime and Cyber Security. 14–16th November, 2018 New Delhi, India) < [https://repository.uel.ac.uk/download/feb8ef6abb4dd5c58cc91faf902bfb1c9499a358d18ea9018e049b088b90b371/705566/Policing%20Drones%202.05.2020\\_3-ACCEPTED.pdf](https://repository.uel.ac.uk/download/feb8ef6abb4dd5c58cc91faf902bfb1c9499a358d18ea9018e049b088b90b371/705566/Policing%20Drones%202.05.2020_3-ACCEPTED.pdf)< accessed 23 December 2022.

<sup>653</sup> *Magna Carta*, means the great charter and denotes that it is a fundamental document within the international civil aviation industry.

<sup>654</sup> Ruwantissa Abeyratne, 'Aviation and Intervention' [2015] *Public Health Emergency Collection* 63–158 <doi: 10.1007/978-3-319-17022-0\_2> accessed 3 August 2022; Brian F. Havel, *Beyond Open Skies: A New Regime for International Aviation* (2<sup>nd</sup> ed, Kluwer Law International, 2009)

<sup>655</sup> ICAO, *Manual on Remotely Piloted Aircraft Systems* (Doc 10019) (1st Edition, ICAO 2015).

Practices (SARPs), Procedures for Air Navigation Services (PANS) as well as guidance material to ensure the development of a synchronized global drone legal framework.<sup>656</sup>

In light of the aforementioned, this chapter briefly examines ICAO's response to the information privacy concerns levied in respect of the proliferation of drones, intending to borrow lessons and or a methodology to address the information privacy implications of drones.<sup>657</sup>

I do not intend to undertake a comprehensive content analysis of the ICAO Model UAS Regulations or the ICAO SARPs but will merely probe the avenue(s) available and the methodology adopted by ICAO, to address the information challenges highlighted in the former chapters of this thesis, if any.

## **2. Institutional Framework**

The following institutions spearhead the progression of drones on behalf of ICAO.<sup>658</sup> The ICAO is made up of three principal governing structures, namely the Assembly, Council, and the Secretariat, alongside several ad hoc and standing committees and panels of experts.<sup>659</sup>

### **ICAO Assembly**

The ICAO Assembly of state parties<sup>660</sup> (Assembly) is the sovereign body that convenes every three years and is responsible for reviewing the work of the organisation, setting policy, and passing a triennial budget.

### **The ICAO Council**

---

<sup>656</sup> Article 37 of the Chicago Convention provides that ICAO shall adopt and amend from time to time, as may be necessary, international standards and recommended practices and procedures'; Leslie Cary, 'International Civil Aviation Organization UAS Study Group; In UAS International (ed), *UAS Yearbook - UAS: The Global Perspective* (Blyenburgh and Co 2010) 51.

<sup>657</sup> Elie El Khoury, 'Remotely Piloted Aircraft Systems (RPAS)' (PowerPoint Presentation, ICAO Middle East Office-Cairo, 2016) <<https://www.icao.int/MID/Documents/2016/RASG-MID5/PPT3%20-%20RPAS%20Elie.pdf>> accessed 22 August 2022.

<sup>658</sup> L.J.P. Speijker and Others, *Study on the regulation of UAS in Hong Kong Final Report* (Netherlands Aerospace Centre 2018).

<sup>659</sup> David McClean and Others, *Shawcross and Beaumont: Air Law* (Issue 159, LexisNexis 2018) 1; Michael Milde, *International Air Law and ICAO* (11<sup>th</sup> ed, International Publishing 2008).

<sup>660</sup> Comprising of representatives from all 191 Contracting States.



The ICAO's executive functions of the ICAO vest in the Council. The Council is the only permanent UN governing body and is headed by a Secretary General. The Council consists of government representatives across three categories of states.<sup>661</sup>

Council decisions are reached via consensus or popular vote.<sup>662</sup> The Chicago Convention accords Council several quasi-legislative<sup>663</sup> and judicial functions,<sup>664</sup> pursuant to which the Council adopts SARPS and resolves disputes stemming from or connected to the Chicago Convention.<sup>665</sup> Council also issues PANS and Regional Supplementary Procedures (SUPPS).<sup>666</sup>

According to the ICAO Secretary General, Dr. Fang Liu, the 'ICAO Council focus on five strategic areas: aviation safety; air navigation capacity and efficiency; security and facilitation; the economic development of air transport and environmental protection'.<sup>667</sup>

---

<sup>661</sup> States of chief importance in air transport; states not otherwise included but which make the largest contribution to the provision of facilities for international civil air navigation; and states not otherwise included whose designation will ensure that all major geographic areas of the world are represented on the Council.

<sup>662</sup> Article 52 of the Chicago Convention stipulates that '[d]ecisions by the Council shall require approval by a majority of its members; Melvin Lum, 'ICJ judgment on jurisdiction of the ICAO Council: 'off chocks', but will it take off?' (International Bar Association, no date supplied) <<https://www.ibanet.org/article/3E25F8E8-0105-4531-B502-F38C27C54C4C>> accessed 19 August 2022.

<sup>663</sup> See Articles 37 and 54 of the Chicago Convention (ICAO Standards and Recommended Practices (SARPs)).

<sup>664</sup> Dispute settlement mechanisms are set out under Chapter XVIII of the Chicago Convention and ICAO, Rules for the Settlement of Differences, ICAO Doc 7782/2 (adopted in 1957, and revised in 1975); to date Council has only dealt with five cases, none of which were resolved on the merits. Several academics criticise the impartiality of the judicial functions of the ICAO Council; See Mathieu Vaugeois, 'Settlement of Disputes at ICAO and Sustainable Development' : In Occasional Paper Series: Sustainable International Civil Aviation (Centre for Research in Air and Space Law, McGill University 2016) <[https://www.mcgill.ca/iasl/files/iasl/occasional\\_paper\\_iv\\_settlement\\_of\\_disputes.pdf](https://www.mcgill.ca/iasl/files/iasl/occasional_paper_iv_settlement_of_disputes.pdf)> accessed 19 August 2022; Richard N Gariepy and David L Botsford, 'The Effectiveness of the International Civil Aviation Organization's Adjudicatory Machinery' (1976) 42 *Journal of Air Law and Commerce* 351, 357-58; Daniel Goedhuis, 'Question of Public International Air Law' (Rec des Cours 1952) 81 201, 223-24; Richard N Gariepy and David L Botsford, 'The Effectiveness of the International Civil Aviation Organization's Adjudicatory Machinery' (1976) 42 *Journal of Air Law and Commerce* 351, 357-58; Cecily Rose, 'Appeal Relating to the Jurisdiction of the ICAO Council' (2021) 115 (2) *American Journal of International Law* 301-308; Anna Ventouratou, 'Defences and indispensable incidental issues: the limits of subject-matter jurisdiction in view of the recent ICJ ICAO Council judgments' (*EJIL: Talk! Blog of the European Journal of International Law*, 23 July 2020) <<https://www.ejiltalk.org/defences-and-indispensable-incidental-issues-the-limits-of-subject-matter-jurisdiction-in-view-of-the-recent-icj-icao-council-judgments/>> accessed 22 August 2022.

<sup>665</sup> Article 84 (Dispute Resolution) and Article 54(n) of the Chicago Convention.

<sup>666</sup> Paul Stephen Dempsey, 'The Chicago Convention as the Constitution of an International Civil Aviation Organization' (PowerPoint Presentation McGill University, 2014) <[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8ntUodr5AhXHYcAKHULrBSQQFnoECAkQAQ&url=https%3A%2F%2Fwww.mcgill.ca%2Fiasl%2Ffiles%2Fiasl%2Faspl\\_633\\_dempsey\\_chicago\\_icao.ppt&usq=AOvVaw2dKw0-WmOhysK-hEPE5onc](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8ntUodr5AhXHYcAKHULrBSQQFnoECAkQAQ&url=https%3A%2F%2Fwww.mcgill.ca%2Fiasl%2Ffiles%2Fiasl%2Faspl_633_dempsey_chicago_icao.ppt&usq=AOvVaw2dKw0-WmOhysK-hEPE5onc)> accessed 1 August 2022.

<sup>667</sup> Fang Liu, 'Lecture Remarks by the Secretary General of the International Civil Aviation Organization (ICAO) to the Uruguay Foreign Ministry's Diplomatic Academy (Montevideo, Uruguay 3 April

## Unmanned Aircraft Systems Study Group

During its 175<sup>th</sup> ICAO Session in April 2005, the Unmanned Aircraft Systems Study Group (UASSG) was constituted as the ICAO focal point for all drone-related issues. It comprised of experts availed by member states and organisations to support the ICAO Secretariat in an advisory capacity on selected technical matters on drones. The UASSG first convened in April 2008.<sup>668</sup> The UASSG was succeeded by the Remotely Piloted Aircraft Systems Panel (RPASP) in 2014.<sup>669</sup>

## Remotely Piloted Aircraft Systems Panel

The Remotely Piloted Aircraft Systems Panel (RPASP) was appointed by the ICAO Air Navigation Commission on 6 May 2014 and is at present the focal point and coordinating body of all ICAO drone-related work. To guarantee geographical representation and multiplicity of considerations and consideration of various socio-economic statuses, the panel includes representatives of 26 states from all seven continents. The RPASP is supported by seven working groups.

### 3. General Overview of the ICAO Regulatory Framework on Drones

Annex 6 to the Chicago Convention defines an aircraft as '[a]ny machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface'.<sup>670</sup>

---

2017)< [https://www.icao.int/Documents/secretary-general/fliu/20170403\\_URUGUAY-LECTURE.pdf](https://www.icao.int/Documents/secretary-general/fliu/20170403_URUGUAY-LECTURE.pdf)> accessed 18 August 2022

<sup>668</sup> Membership: Australia, Austria, Brazil, China, Czech Republic, France, Germany, Italy, Netherlands, New Zealand, Russian Federation, Singapore, South Africa, Sweden, U.K., U.S., CANSO, EASA, EUROCAE, EUROCONTROL, IAOPA, ICCAIA, IFALPA, IFATCA, UVS Intl.

<sup>669</sup> EURNAT Office – ICAO, 'CIVIL AVIATION AND UAS –RPAS –DRONES' (ICAO, 1 Oct 2017) <<https://unitingaviation.com/regions/eurnat/civil-aviation-and-uas-rpas-drones/>> accessed 19 May 2022; George Thomas Black, Catherine Nadaud and Ronflé-Nadaud, 'Integration in the National Airspace (Europe and USA) – UAV Classification and Associated Missions, Regulation and Safety, Certification and Air Traffic Management; (2020) Multi-Rotor Platform-based UAV System <<https://doi.org/10.1016/B978-1-78548-251-9.50001-7>> accessed 12 July 2022; Philip Dawson, 'Developing a global framework for unmanned aviation'(Coordinates, April 2018) <<https://mycoordinates.org/developing-a-global-framework-for-unmanned-aviation/>> accessed 11 June 2022.

<sup>670</sup> ICAO, *Annex 6 to the Chicago Convention; Part 1 (Operation of an Aircraft)* (9<sup>th</sup>ed, ICAO 2010) Available at <[https://www.verifavia.com/bases/ressource\\_pdf/299/icao-annex-6-part-i.pdf](https://www.verifavia.com/bases/ressource_pdf/299/icao-annex-6-part-i.pdf)> accessed 18 July 2022.

Owing to this definition, the ICAO classified drones as an aircraft. Article 8 of the Chicago Convention provides that '[n]o aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting state without special authorisation by that state and in accordance with the terms of such authorization.' On account of this, drones fell within the jurisdictional scope of ICAO.

More specifically, the Global Air Traffic Management Operational Concept (Doc 9854)<sup>671</sup> defines 'an unmanned aerial vehicle' as:

[a] pilotless aircraft, in the sense of Article 8 of the Convention on International Civil Aviation, which is flown without a pilot-in-command on-board and is either remotely and fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous.

Being classified as an aircraft, all the provisions of the Chicago Convention apply to drones, *mutatis mutandis*.<sup>672</sup> The provisions of the Chicago Convention thus govern among others the safety, security, air navigation procedures, personnel licensing, airport development, aircraft airworthiness, and accident investigation of drones on an international level.<sup>673</sup>

On the strength of the quasi-legislative powers conferred on the ICAO under Article 37 of the Chicago Convention, the ICAO from time to time adopts, revises or amends <sup>674</sup>SARPs<sup>675</sup> as annexes to the Chicago Convention.<sup>676</sup>

To date, the ICAO adopted 12,000 SARPs relating to drones. These are arranged across 19 annexes to the Chicago Convention. Eighteen of the 19 annexes (with the

---

<sup>671</sup>ICAO, *Global Air Traffic Management Operational Concept* (Doc 9854 AN/458) (1<sup>st</sup> ed, ICAO 2005 (revised 2017)) <[https://www.icao.int/Meetings/anconf12/Document%20Archive/9854\\_cons\\_en\[1\].pdf](https://www.icao.int/Meetings/anconf12/Document%20Archive/9854_cons_en[1].pdf)> accessed 18 July 2022.

<sup>672</sup>Michael Milde, *International Air Law and ICAO* (11<sup>th</sup> ed, International Publishing 2008).

<sup>673</sup>Fang Liu, 'Lecture Remarks by the Secretary General of the International Civil Aviation Organization (ICAO) to the Uruguay Foreign Ministry's Diplomatic Academy (Montevideo, Uruguay 3 April 2017)' <[https://www.icao.int/Documents/secretary-general/fliu/20170403\\_URUGUAY-LECTURE.pdf](https://www.icao.int/Documents/secretary-general/fliu/20170403_URUGUAY-LECTURE.pdf)> accessed 18 August 2022.

<sup>674</sup>An International Standard is defined as '[a]ny specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as necessary for the safety or regularity of international air navigation and to which contracting States will conform in accordance with the Convention' (Articles 37, 38 and 54 of the Chicago Convention).

<sup>675</sup>A Recommended Practice is defined as '[a]ny specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as desirable in the interest of safety, regularity or efficiency of international air navigation and to which contracting States will endeavour to conform in accordance with the Convention' (Articles 37 and 54 of the Chicago Convention).

<sup>676</sup>Benoît Verhaegen, 'ICAO Legal Seminar (Bangul, The Gambia, 24-25 February 2020)' <<https://www.icao.int/Meetings/GambiaSeminar2020/Documents/2.3%20Benoit%20Verhaegen%20-%20International%20Framework%20for%20Air%20Navigation%20Safety.pdf>> accessed 18 August 2022.

exception of annex 5 (Units of Measurement to be used in Air and Ground Operations), have been amended to accommodate drones.<sup>677</sup>

Article 90 of the Chicago Convention sets out the procedure to be followed leading to the adoption of a SARP.<sup>678 679</sup> The process for the formal adoption of a SARP requires a two-thirds majority vote by the Assembly and classically spans over two years and is subject to amendment from time to time and becomes due for domestication 5 years after adoption by the Assembly.<sup>680</sup>

The Assembly endorsed SARPs on the international safety and interoperability of remotely piloted aircraft systems (RPAS) at its 222<sup>nd</sup> Session on the 19 of March 2021. These SARPS must be transposed in the domestic law of member states by 26 November 2026.<sup>681</sup>

The International Organization for Standardization (ISO) is in the process of developing standards for the classification, design, manufacture, operation (including maintenance), and safety management of drone operations.<sup>682</sup> Although the contents of the ISO standards are not publicly available at this juncture, I am delighted to note

---

<sup>677</sup>Anna Masutti and Filippo Tomasello, *International Regulation of Non-Military Drones* (1<sup>st</sup> ed, Edward Elgar Publishing 2018).

<sup>678</sup>Chahinez Dib, 'The ICAO Annexes to the Convention on International Civil Aviation' (ICAO, 28 Feb, 2022) <<https://unitingaviation.com/news/safety/publication-spotlight-the-icao-annexes-to-the-convention-on-international-civil-aviation/>> accessed 19 August 2022.

<sup>679</sup>David Hodgkinson and Rebecca Johnston, 'Guiding principles for drones: A starting point for international regulation' (2018) 3 Perth International Law Journal 158-184; Muhammad Nadeem Mirza et al, 'Unmanned Aerial Vehicles: A Revolution in the Making' (2016) 31 Research Journal of South Asian Studies 625, 627.

<sup>680</sup>ICAO, Manual on Notification and Publication of Differences (Doc 10055 AN/518-) (1st ed, ICAO 2019) <http://www.icscc.org.cn/upload/file/20190102/Doc.10055EN%20Manual%20on%20Protection%20of%20Safety%20Information.pdf>> accessed 19 August 2022; Jenny Beechener, 'ICAO proposes legal framework for international RPAS design, type certification and operations' (February 9, 2021) <<https://www.icao.int/Newsroom/Pages/ICAO-Council-makes-progress-on-new-remotely-piloted-aircraft-system-RPAS-standards.aspx>> accessed 21 June 2022; ICAO, 'Making an ICAO Standard' (ICAO, 1 November 2011).

<sup>681</sup> Zieliński, Tadeusz and Marud, Wiesław, 'Challenges for Integration of Remotely Piloted Aircraft Systems into the European Sky' (2019) 102 Scientific Journal of Silesian University of Technology Transport Series 217-229<DO-10.20858/sjsutst.2019.102.18> accessed 10 August 2022; ICAO, 'Council makes progress on new remotely piloted aircraft system (RPAS) standards' (ICAO, 19 March 2021)> <https://www.icao.int/Newsroom/NewsDoc2021fix/COM.10.21.EN.pdf>> accessed 19 August 2022; Declan Fitzpatrick, 'UAS a new paradigm for aviation regulators' (European Civil Aviation Conference Magazine 73,2021)<[https://www.ecac-ceac.org/images/news/ecac-news/ECAC\\_News\\_73\\_Unmanned\\_Aircraft\\_Systems.pdf](https://www.ecac-ceac.org/images/news/ecac-news/ECAC_News_73_Unmanned_Aircraft_Systems.pdf)> accessed 19 August 2022.

<sup>682</sup>International Standards Organisation (ISO), 'Unmanned aircraft systems Part 3: Operational procedures' (ISO, November 2019)<<https://www.iso.org/obp/ui/#iso:std:iso:21384:-3:ed-1:v1:en>>accessed 19 August 2022.

from the table contents that is publicly available that Part 6 will address information privacy.<sup>683</sup>

Since ICAO follows the principle of international consensus, the dominant academic opinion is that the standards are binding upon all member states. Articles 37 and 38 of the Chicago Convention requires states to supplant all SARPS within their domestic law or file a notification, if it digresses from the SARPS adopted by ICAO. Therefore, following the adoption of SARPS, member states to the Chicago Convention who have not filed a notification of divergence, are obligated to supplant the SARPs, as part of their domestic law.<sup>684</sup>

In order to monitor and enforce the domestication and compliance with the SARPs, the ICAO introduced the Universal Safety Oversight Audit Programme (USOAP) in 1999 and the Universal Security Audit Programme (USAP) in 2002.<sup>685</sup>

In 2011, the ICAO issued its first drone-specific document; Circular 328-AN/190,<sup>686</sup> delineating its vision of incorporating drones into the international regulatory framework. It further dispensed the Manual on Remotely Piloted Aircraft Systems in 2015, which offered guidance on technical and operational drone matters.<sup>687</sup>

---

<sup>683</sup> Douglas M. Marshall, *UAS Integration into Civil Airspace: Policy, Regulations and Strategy* (John Wiley and Sons, 2022)140; Next Practice, 'ISO Publishes Draft of New Standards for Drones' (Next Practice, 7 Aug, 2019)<<https://www.nextpractice.education/iso-publishes-draft-of-new-standards-for-drones>> accessed 19 August 2022.

<sup>684</sup> Article 12 of the Chicago Convention provides that, '[s]tates must ensure that aircraft flying over their territory or carrying their nationality mark complies with the rules and regulations governing flight there in force'.

<sup>685</sup> ICAO, *Manual on Notification and Publication of Differences* (Doc 10055 AN/518) (1st ed, ICAO 2019) <<http://www.icscc.org.cn/upload/file/20190102/Doc.10055EN%20Manual%20on%20Protection%20of%20Safety%20Information.pdf>> accessed 19 August 2022; Fang Liu, 'Lecture Remarks by the Secretary General of the International Civil Aviation Organization (ICAO) to the Uruguay Foreign Ministry's Diplomatic Academy (Montevideo, Uruguay 3 April 2017)' <[https://www.icao.int/Documents/secretary-general/fliu/20170403\\_URUGUAY-LECTURE.pdf](https://www.icao.int/Documents/secretary-general/fliu/20170403_URUGUAY-LECTURE.pdf)> accessed 18 August 2022.

<sup>686</sup> ICAO, Unmanned Aircraft Systems (UAS) (Circular 328 AN/190-/ Doc 10019) (ICAO, 2011) <[https://www.icao.int/Meetings/UAS/Pages/UAS\\_Documents.aspx](https://www.icao.int/Meetings/UAS/Pages/UAS_Documents.aspx)> accessed 18 August 2022.

<sup>687</sup> Milan A. Plücker, 'The regulatory approach of ICAO, the United States and Canada to Civil Unmanned Aircraft Systems, in particular to Certification and Licensing' (Master's Thesis, University Montreal, 2015).

After having complied with the prescribed processes,<sup>688</sup> which include allowing member states to provide comments,<sup>689</sup> the ICAO promulgated Model Regulations, titled Parts 101, 102, and 149, amidst the challenges presented by the Covid-19 pandemic.<sup>690</sup>

It is claimed that the ICAO Model Regulations have strong undertones of Vanuatu, New Zealand, Australia, Canada, and the United States drone regulations.<sup>691</sup> Guidance for the implementation of the ICAO Model UAS Regulations is provided through Advisory Circulars (ACS).<sup>692</sup>

#### 4. ICAO's approach to Information Privacy

In line with the golden principle of state sovereignty enshrined in Article 1 of the Chicago Convention, which vests the unrestricted exclusive control over their national airspace in member states, the ICAO Model UAS Regulations are in principal discretionary and overtly serve as a legislative prototype and omits sovereign domestic considerations.<sup>693</sup>

---

<sup>688</sup>The process involved analyzing the drone regulations in force in various Member States and identifying commonalities and best practices that aligns with the Chicago Convention. Current State Regulations' represents a UAS Toolkit and is available at <<https://www.icao.int/safety/UA/UAStoolkit>> accessed 19 August 2022.

<sup>689</sup> Comments on the Model Drone Regulations were due on 23 June 2020.

<sup>690</sup> ICAO Model UAS Regulations: Part 101 and Part 102. Available at <<https://www.icao.int/safety/UA/UAID/Documents/Final%20Model%20UAS%20Regulations%200-%20Parts%20101%20and%20102.pdf>> accessed 1 August 2022 .

<sup>691</sup> ICAO Model Regulations are available at <<https://www.icao.int/safety/UA/>> accessed 1 August 2022.

<sup>692</sup> ICAO 'UAS Related Activities: Update on ICAO UAS Advisory Group' (PowerPoint presentation 28 September 2021) <<https://www.icao.int/NACC/Documents/Meetings/2021/UASRPAS/P05-UASRPASW2-Update-ICAO-UAS-Advisory-Group-Wuennenberg.pdf>> accessed 3 August 2022. On 10 September 2020 (ICAO) published its latest UAS guidance materials electronic bulletin Electronic Bulletins and State Letters – ICAO(EB2020/43) <<https://www.icao.int/safety/CAPSCA/Pages/Electronic-Bulletins-and-State-Letters.aspx>> accessed 19 August 2022; ICAO UAS Study Group, 'ICAO UAS Study Group resources' (ICAO, date not supplied) <<https://liye.info/doc-viewer>> accessed 22 August 2022; ICAO, 'UAS Documents' (ICAO, no date supplied) <[https://www.icao.int/Meetings/UAS/Pages/UAS\\_Documents.aspx](https://www.icao.int/Meetings/UAS/Pages/UAS_Documents.aspx)> accessed 23 August 2022.

<sup>693</sup> Appeal relating to the Jurisdiction of the ICAO Council under Article 84 of the Convention on International Civil Aviation (Bahrain, Egypt, Saudi Arabia and United Arab Emirates v. Qatar), Judgment, I.C.J. Reports 2020, p. 81693 (International Court of Justice Reports of Judgments, Advisory Opinions And Orders, 2020) <<https://www.icj-cij.org/public/files/case-related/173/173-20200714-JUD-01-00-EN.pdf>> accessed 19 July 2022; Saulo Da Silva, 'ICAO UAS-Update from the UASSG (NPF/SIP/2010-WP/14)' (Workshop Presentation: International Civil Aviation Organization Eastern and Southern African Office Workshop on the Development of national performance framework for Air Navigation Systems Nairobi, 6-10 December 2010) <[https://www.icao.int/ESAF/Documents/meetings/2010/wdnpf\\_ans/docs/wp\\_02.pdf](https://www.icao.int/ESAF/Documents/meetings/2010/wdnpf_ans/docs/wp_02.pdf)> accessed 17 August 2022; Rutwantissa Abeyratne, 'Law Making and Decision Making Powers of the ICAO Council - A Critical Analysis' (1992) 41 Zeitschrift für Luft <<https://lawexplores.com/legal-legitimacy-of-icao-and-direction-to-be-taken/>> access 17 August 2022; Ruwantissa Abeyratne, 'Legal Legitimacy of ICAO and Direction to Be Taken' (Law Explorer, 10 Jan, 2016) <<https://lawexplores.com/legal-legitimacy-of-icao-and-direction-to-be-taken/>> access 17 August 2022.

For this reason, the preface to the Model ICAO Regulations unambiguously stipulates that:

[t]hese model regulations are limited to the certification and safe operations of UAS and do not address sanctions against violations of these provisions or discretionary topics specific to national consideration such as, for example, *privacy*, insurance, or economic authority.<sup>694</sup>

To this end, member states have the unfettered regulatory prerogative in respect of dealing with the (information) privacy implications of drones within their domestic regulations.

It is inopportune that notwithstanding the universal lament regarding the information privacy threats of drones, the ICAO offers no guidance on how to address the information privacy challenges of drones.

This stance is justified by alleging that (information) privacy is beyond the scope of ICAO's mandate.<sup>695</sup> Moreover, the ICAO contends that even if it was within ICAO's mandate to address (information) privacy, as an international organisation dealing with multiple countries with differing, conceptualisation, dogmas, and ethos on (information) privacy and its parameters, it would be a great challenge or ill-advised to promulgate a universally acceptable legal framework on information privacy.<sup>696</sup>

Even though I acknowledge the historical opprobrium regarding conceptualising an all-encompassing determinant of privacy, as well as information privacy, I respectfully disagree that it is impossible to obtain commonality among the ICAO member states to address the information privacy risk posed by drones. This is evident from the compromise in this regard among the twenty-five EU member states.<sup>697</sup>

---

<sup>694</sup>ICAO Model UAS Regulations: Part 101,102 and 149 <<https://www.icao.int/safety/UA/UAID/Documents/Final%20Model%20UAS%20Regulations2%20-%20Parts%20101%20and%20102.pdf>> accessed 1 August 2022; Leslie Cary, "International Civil Aviation Organization UAS Study Group", ICAO, UAS Yearbook - UAS: The Global Perspective (Blyenburgh & Co, 2010) at 51.

<sup>695</sup>K Kirthan Shenoy and Divya Tyagi, 'Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky' (2022) 9 (1) International Journal of Aviation, Aeronautics, and Aerospace <<https://commons.erau.edu/ijaaa/vol9/iss1/7>> accessed 10 April 2022; Rodgers Wanyonyi Manana and Nelson Otieno, 'Drones Operations in Kenya: Perspectives on Privacy Challenges and Prospects' (2022) 1 (47) Air and Space Law 75–92.

<sup>696</sup> Brian F. Havel and John Q. Mulligan, 'Unmanned Aircraft Systems: A Challenge to Global Regulators' (2015) 65 DePaul Law Review 107, 112-113.

<sup>697</sup> Discussed in Chapter Five of this thesis.

## 5. Chapter Summary and Evaluation

ICAO's standpoint to leave the regulation of information privacy of implications of drones to the prerogative of the member states proves the assertions made by Gary Marchant that, the 'existing regulatory authorities lack the legal authority, expertise, and resources to regulate emerging technologies', true.<sup>699</sup>

I hold the opinion that by virtue of Article 36 of the Chicago Convention, information privacy, as it relates to photographic apparatus, falls within the rubric of ICAO's mandate. Article 36 of the Chicago Convention (Photographic apparatus) provides that 'each contracting State may prohibit or regulate the use of photographic apparatus in aircraft over its territory'.<sup>700</sup>

Although the Chicago Convention does not define the phrase photographic apparatus,<sup>701</sup> I am convinced that most of the information communication technology intruding payloads a drone can be amassed with,<sup>702</sup> can invariably be accommodated under this reference.

It is therefore my opinion that Article 36 of the Convention offers sufficient ambit for the ICAO to assume accountability to address the information privacy challenges presented by drones in order to allay the myriad of information privacy concerns that is associated with drones or to have placed (information) privacy implications of drones on ICAO's agenda, in the least.

Moreover, I am further inclined to endorse Dhananga Pathirana's contention that the 'inimitable challenges presented by the civil application of drones warrant a pressing

---

<sup>699</sup>Gary E. Marchant, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 (6) *Vanderbilt Law Review* 1861,1866; See discussion on Paragraph 4 of Chapter 1 of this thesis.

<sup>700</sup>Masutti A, Tomasello F, *International regulation of non-military drones* (Edward Elgar, 2018); Ruwantissa Abeyratne (ed), 'Convention on International Civil Aviation': *In Convention on International Civil Aviation: A Commentary* (Springer International Publishing, 2014).

<sup>701</sup> Benjamyn I. Scott, 'Key Provisions in Current Aviation Law': In Bart Custers (ed), *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives* (Springer 2016) 241, 249–256; Ruwantissa Abeyratne, *International Convention on Civil Aviation: A Commentary* (Springer 2014), 516.

<sup>702</sup> See the discussion in this regard under Paragraph 4 of Chapter 1.



intervention by governments worldwide, in a manner unlike any other in the history of civil aviation'.<sup>703</sup>

To this end, I am further of the considered opinion that the ICAO is the best forum for an intervention to address the information privacy implications of drones by incorporating pro-information privacy considerations in the ICAO Model Regulations and SARPs.

I draw support for the above-mentioned, by drawing an analogy to the expansion of the ICAO's mandate to include environmental protection, shortly after the United Nations Framework Convention on Climate Change (Kyoto Protocol) entered into force on 21 March 1994, notwithstanding the fact that the constitutive text of the Chicago Convention is mute on the subject matter.<sup>704</sup>

Following the operationalisation of the Kyoto Protocol,<sup>705</sup> the Assembly resolved to moderate environmental protection within the civil aviation industry and mandated Council to spearhead policy guidance on environmental matters within the civil aviation industry.<sup>706</sup> To strengthen this resolve, the ICAO Committee on International Aviation Environmental Protection (CAEP) was established in 1998. CAEP advise the Council and Assembly on technical, economic, social, and policy aspects of fostering environmental protection in the global civil aviation industry.<sup>707</sup> Since then, the ICAO has been consistent in its role in respect of promoting environmental protection within its quasi-legislative functions.<sup>708</sup> An analysis of the ICAO Assembly resolutions since 1998, depicts sound political will toward fostering environmental protection within the

---

<sup>703</sup> Dhananga Pathirana, 'Towards Better Regulation of Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of Selected National Regulations' (Master's Thesis, University of Montreal 2019), 38.

<sup>704</sup> Protocol to the United Nations Framework Convention on Climate Change, adopted on 11 December 1997, (UN Doc FCCC/CP/1997/7/Add.1) entered into force 16 February 2005. Available at <<https://unfccc.int/resource/docs/convkp/kpeng.pdf>> accessed 1 August 2022.

<sup>705</sup> Article 2 (2) of the Kyoto Protocol provides that, States shall pursue limitation of greenhouse gases emission (GHG) by working through ICAO.

<sup>706</sup> ICAO Assembly resolutions: A32-8; A33-7; A35-5; A36-22; A37-19 and A38-18. Available at <<https://www.icao.int/Meetings/AMC/MA/Assembly%2032nd%20Session/resolutions.pdf>> accessed 21 August 2022.

<sup>707</sup> Alejandro Piera, *Greenhouse Gas Emissions from International Aviation: Legal and Policy Challenges* (11<sup>th</sup> ed, International Publishing 2015) 86.

<sup>708</sup> Baine P Kerr, 'Clear skies or turbulence ahead? The international civil aviation organization's obligation to mitigate climate change (2020) 16(1) Utrecht Law Review 101–116 <DOI: <http://doi.org/10.36633/ulr.551>> 18 August 2022.

civil aviation industry, which at this point qualifies as a rule of state practice or customary international law.<sup>709 710</sup>

There are diverging academic sentiments regarding the legal justification for the expansion of the ICAO's mandate to include environmental protection. Scholars like Piera contend that 'the Chicago Convention's lack of reference to the environment or climate change is problematic and suggests the it should (have) be (een) amended to legitimize the inclusion of environmental protection'.<sup>711</sup> He is supported by Romera<sup>712</sup> who posits that the 'legal status of the ICAO's environmental objective is certainly beneath the ones established by the Chicago Convention, since those are, at most, soft law, while the Chicago Convention is a hard law'.

I am however persuaded by the argument advanced by Abeyratne<sup>713</sup> and Kerr,<sup>714</sup> who are of the opinion that a liberal interpretation of Article 44 of the Chicago Convention is sufficient to legitimise the expansion of the ICAO's mandate to include environmental protection, and if I may contest it a step further, (information) privacy. Further, in terms of Article 44 of the Chicago Convention, the ICAO's objectives are to:

- Ensure the safe and orderly growth of international civil aviation throughout the world.
- Encourage the arts of aircraft design and operation for peaceful purposes;
- Encourage the development of airways, airports and air navigation facilities for international civil aviation;

---

<sup>709</sup> State practice is creative, or expressive, of rules of customary international law, but only in so far as it is undertaken with the conviction that a legal right or obligation is involved (acceptance as law, or *opinio iuris*) (Max Planck Encyclopedia of Public International Law (MPEPIL) <<https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1107>> accessed 20 August 2022; Harmen Van der Wilt, 'State Practice as Element of Customary International Law: A White Knight in International Criminal Law?' (2022) (1) International Criminal Law Review (online) <[https://brill.com/view/journals/icla/20/5/article-p784\\_784.xml?language=en](https://brill.com/view/journals/icla/20/5/article-p784_784.xml?language=en)> accessed 20 August 2022.

<sup>710</sup> Mathieu Vaugeois, 'Settlement of Disputes at ICAO and Sustainable Development': In Occasional Paper Series: Sustainable International Civil Aviation (Centre for Research in Air and Space Law, McGill University 2016) (*Paragraph VII. The consideration of Environment and Sustainable Development by the ICAO Council*, 13) <[https://www.mcgill.ca/iasl/files/iasl/occasional\\_paper\\_iv\\_settlement\\_of\\_disputes.pdf](https://www.mcgill.ca/iasl/files/iasl/occasional_paper_iv_settlement_of_disputes.pdf)> accessed 19 August 2022; Brian F Havel and Gabriel S Sanchez, 'The International Law Regime for Aviation and the Environment': In *The Principles and Practice of International Aviation Law* (Cambridge University Press 2014) at 228.

<sup>711</sup> Alejandro Piera, *Greenhouse Gas Emissions from International Aviation: Legal and Policy Challenges* (11th ed, International Publishing 2015) 116,117.

<sup>712</sup> Beatriz Martinez Romera, *Regime Interaction and Climate Change* (Routledge 2018),41.

<sup>713</sup> Rutwantissa Abeyratne, *International Convention on Civil Aviation: A Commentary* (Springer 2014), 516.

<sup>714</sup> Baine P Kerr, 'Clear skies or turbulence ahead? The international civil aviation organization's obligation to mitigate climate change (2020) 16(1) Utrecht Law Review 101–116 <DOI:<http://doi.org/10.36633/ulr.551>> 18 August 2022.

- Meet the needs of the people of the world for safe, regular, efficient, and economical air transport;
- Prevent economic waste caused by unreasonable competition;
- Ensure that the rights of the Contracting States are fully respected and that every Contracting State has a fair opportunity to operate international airlines;
- Avoid discrimination between Contracting States;
- Promote the safety of flight in international air navigation;
- Promote generally the development of all aspects of international civil aeronautics;
- and such other matters concerned with the safety, regularity, and efficiency of air navigation as may from time to time appear appropriate. (Underlined for Emphasis)

Bearing in mind the information privacy risks posed by drones as canvassed in earlier chapters, I am adamant that the absence of information privacy considerations from the ICAO regulations, undoubtedly undermines the need of people globally to have their human right to (information) and privacy protected. Additionally, it holds the potential to undercut aviation security and safety and consequently the growth of civil aviation worldwide. It is thus reasonable to conclude that, omitting information privacy from the mandate and strategic focus of the ICAO is inconsistent with the objectives of the Chicago Convention, as espoused under Article 44 of the Chicago Convention.<sup>715</sup>

In conclusion, banking on the analogy from the practice in respect of environmental protection within the civil aviation industry, I am optimistic that the established significance of ensuring information privacy protection within the drone industry, will give rise to an expansion of the ICAO's mandate and the Council's strategic objectives, to include the (information) privacy implications of drones in order to avert the information privacy challenges posed by drones on an international front which will inevitably trickle down to all its member states.

The literature is unanimous that international organisations have the competence to contribute to the formulation of international state practice and rules of customary international law.<sup>716</sup> Therefore, provided that the ICAO internalises the information

---

<sup>715</sup>Jan Klabbbers, 'Reflections on Role Responsibility: The Responsibility of International Organizations for failing to Act,' (2017) 28 (4) *European Journal of International Law*, 1137.

<sup>716</sup>Jan Klabbbers, *An Advanced Introduction to the Law of International Organizations* (4<sup>th</sup> ed, Cambridge University Press 2022) 14,115; Jan Klabbbers, 'Notes on the Ideology of International Organizations Law: The International Organization for Migration, State-making, and the Market for Migration' (2019) 32 (2) *Leiden Journal of International Law* 383-400 <<https://doi.org/10.1017/S092>> accessed 25 August 2022; Ellen Campbell and Others, 'Due Diligence Obligations of International Organizations under International Law' (2018) 50 *New York University Journal of International Law and Politics* 558, See also Andrew Clapham, *Human Rights Obligations of Non-State Actors* (Oxford University Press 2006) 151.

privacy agenda connected to drones and garners sufficient support from member states,<sup>717</sup> the ICAO can effortlessly contribute to the development of novel rules of customary international law<sup>718</sup> on information privacy protection of drones.<sup>719</sup>

The commentary on the Statute of the International Court of Justice (ICJ),<sup>720</sup> stipulates that customary international law encompass two elements: consistent and general international practice by states coupled with a subjective acceptance of the practice as law by the international community (*opinio juris*).

Article 38(1)(b) of the Statute of the International Court of Justice (ICJ)<sup>721</sup> provides that the formation of a rule of 'international custom' requires a general practice by States which is accepted as law. Patrick Dumberry<sup>722</sup> holds that any uniform, consistent, extensive and representative state practice will undoubtedly be adopted as a rule of customary international law and that customary international law finds commonplace within international organisations like the ICAO.

Given that Articles 36 and 44 of the Chicago Convention, the ICAO must first, reconsider its stance regarding the privacy implications of drones and take accountability, as it did in respect of environmental protection to spearhead the formulation of pro-information privacy customary international rules, guidelines and best practices to ensure that data subjects are protected from the unlawful processing of their personal information by drones.

---

<sup>717</sup> Based on the Chapter Five, there is guaranteed support from the EU already. According to Baine P Kerr, 'Clear skies or turbulence ahead? The international civil aviation organization's obligation to mitigate climate change' (2020) 16(1) Utrecht Law Review 101–116 <DOI: <http://doi.org/10.36633/ulr.551>> 18 August 2022, the EU was also spearheaded the civil aviation environmental protection agenda.

<sup>718</sup> Customary international law is comprised of two elements: (1) consistent and general international practice by states, and (2) a subjective acceptance of the practice as law by the international community (*opinio juris*).

<sup>719</sup> James D. Fry, 'Rights, Functions, and International Legal Personality of International Organizations' (2018) 32 Boston University International Law Journal 221.

<sup>720</sup> United Nations, Statute of the International Court of Justice, adopted on 18 April 1946 and entered into force on 24 October 1945 (1179, 59 Stat 1055, TS No 993). Available at <<https://www.refworld.org/docid/3deb4b9c0.html>> accessed 25 August 2022.

<sup>721</sup> United Nations, Statute of the International Court of Justice, adopted on 18 April 1946 and entered into force on 24 October 1945 (1179, 59 Stat 1055, TS No 993). Available at <<https://www.refworld.org/docid/3deb4b9c0.html>> accessed 25 August 2022.

<sup>722</sup> Patrick Dumberry, 'State practice': In *The Formation and Identification of Rules of Customary International Law in International Investment Law* (Cambridge University Press, 2016), 116, 291 See also Andreas Zimmermann and Others, *The Statute of the International Court of Justice: a commentary* (3rd ed, Oxford University Press 2019).

# Chapter Seven

## Conclusion

---

*This chapter offers a synopsis of the research undertaken throughout this thesis. It sets out the main conclusions of my scholarly investigation, informed by the main conclusions it advance policy and legal suggestions for reform and sets out future areas of academic focus.*

### 1. Introduction

The progression of drone technologies gave rise to what is commonly referred to as ‘innovation shock’.<sup>723</sup> Despite being formerly overtly utilised in military operations, advancements in artificial intelligence, image processing, and robotics have transmuted drones to civilian usage; enabling them to be employed for innumerable civil applications across several industries, as well as purely for amusement.

Drone technologies are designated as nascent technology and scholars anticipate that they will undergo an ascending evolution in forthcoming years.<sup>724</sup> Despite being classified as an embryonic industry, it is projected that the commercial drone industry will be worth US\$ 279 Billion by 2032.<sup>725</sup>

### 2. Synopsis of the Research

Scholars unanimously concede that the propagation of civilian drones embedded with technological hardware and software that can process personal information leaves room for unlawful violations of the constitutional right to privacy guaranteed under section 14 and article 13 of the RSA and Namibian constitutions, respectively.

---

<sup>723</sup> Ferran Gionesa and Alexander Brema, ‘From toys to tools: The co-evolution of technological and entrepreneurial developments in the drone industry’ (2017) 60 (6) *Business Horizons* 875-884. < <https://doi.org/10.1016/j.bushor.2017.08.001> accessed 20 September 2022

<sup>724</sup> Kristina Vaarst Andersen and Other, ‘The strategic responses of start-ups to regulatory constraints in the nascent drone market’ (2021) 49 (1) *Research Policy* 104055 <<https://doi.org/10.1016/j.respol.2020>> accessed 22 September 2022; Sarah Jane Fox, ‘The ‘risk’ of disruptive technology today (A case study of aviation – Enter the drone)’ (2020) 62 *Technology in Society* 101304.

<sup>725</sup> Fact.Mr, ‘Global Drones Market Outlook (2022-2032)’ (Fact.MR no date supplied) <<https://www.factmr.com/report/62/drone-market>> accessed 1 September 2022; Himanashu Joshi and Sonja Mutreja, ‘Micro Drone Market Statistics’ (Alliedmarketresearch, September 2021) <<https://www.alliedmarketresearch.com/micro-drone-market-A13679>> accessed 1 September 2022.

This is the reason one of the drafters of the EU Charter Rodotà argues that the 4IR demands that the inviolability of the person must be reconfirmed in the electronic dimension.<sup>726</sup>

Being considered the 'new oil or new currency of the digital world' all academics and jurists agree that personal information must be protected against unauthorised processing by governments, natural and juristic persons.<sup>727</sup>

The overriding academic opinion is that the popularisation of commercial drones is at friction with the right to information privacy.

This research established that inadequately regulated drone usage infringes several internationally recognised fair information privacy principles, particularly transparency, accountability, purpose specification, processing limitation, information quality and the duty to put in place security safeguards.

Moreover, data subjects whose personal information was unlawfully processed by drones are also left without a forum to exercise the rights accorded to them under the various international and national information privacy protection frameworks.<sup>728</sup>

This friction is aggravated by the fact that drones are classified as aircrafts under Article 8 of the Chicago Convention. Resultantly, drones fall within the regulatory jurisdiction of the national and international civil aviation regulators. The civil aviation industry is conventionally exclusively regulated in respect of safety and security and since 1997, environmental protection.<sup>729</sup>

---

<sup>726</sup> S Rodotà, 'Data Protection as Fundamental Human Right': In Serge Gutwirth and Others (eds) *Reinventing Data Protection?* (Springer, 2009) 77-82;

<sup>727</sup> A May, 'Data is the new oil, the New Gold of the Digital Era!' (LinkedIn: 16 March, 2021) < <https://www.linkedin.com/pulse/data-new-oil-gold-digital-era-dr-may-alobaiddy/> accessed 14 February 2022; Agnes Budzyn, 'Data is the oil of the digital world. What if tech giants had to buy it from us?' (World Economic Forum, 30 April Apr 30, 2019) < <https://www.weforum.org/agenda/2019/04/data-oil-digital-world-asset-tech-giants-buy-it/> accessed 7 January 2023; The Economist, 'The world's most valuable resource is no longer oil, but data' (The Economist, 6 May 2017) < <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 7 January 2023.

<sup>728</sup> Nehaluddin Ahmad and Others, 'Unregulated drones and an emerging threat to right to privacy: A critical overview' (2021) 4(2) *Journal of Data Protection and Privacy* 124-145,130 <<https://hstalks.com/article/6238/unregulated-drones-and-an-emerging-threat-to-right/>> accessed 1 Jan 2022

<sup>729</sup> For purposes of this thesis safety denotes safeguards to avert unforeseen and inadvertent events, whilst security refers to managing anticipated operational risk.

In addition to the preoccupation with safety and security, the civil aviation industry has limited human resources with expertise outside the named strategic focus areas.

Furthermore, the research established that the civil aviation regulators on both the domestic and international fronts presently lack political commitment and (allegedly) the legal mandate to regulate information privacy.<sup>730</sup>

To offer perspective on the friction between drone technologies and information privacy, I conducted a conceptual analysis of statutes, policies, laws and their associated, procedures and industry practices, as well as jurisprudence on information privacy and drones in the RSA and Namibia and compared these findings to those in the EU.

The research process followed a qualitative, content analysis and comparative study methodology.

My overarching initial supposition was that the legal framework on civilian drones administered by the civil aviation regulators in the RSA and Namibia and by the ICAO inadequately addresses the information privacy risks associated with civilian drone operations.

Considering that information privacy is an enabler of the comprehensive inalienable universal human right to privacy, this thesis proceeds from the assumption that as state actors, the RSA and Namibia (through their national civil aviation regulators) and the ICAO as an international organisation are enjoined in terms of several binding international and national human rights law instruments, to exercise due diligence to protect the right to information privacy within the international drone industry.

Human rights due diligence is a term coined in 2008 by John Ruggie, the UN Secretary General's special representative for business and human rights. The term denotes a rule of customary international law that requires international actors and business enterprises to proactively manage and mitigate potential and actual human rights impacts within the scope of their mandate.<sup>731</sup>

---

<sup>730</sup> It is my finding that Article 44 of the Chicago Convention offers scope to include information privacy. See discussion in chapter 6 in this regard.

<sup>731</sup>Tineke Lambooy, 'Corporate Due Diligence as a tool to respect Human Rights' <<https://www.jus.uio.no/ifp/english/research/areas/companylaw/events/lunches/Lambooy.pdf>> accessed 19 June 2022; Summary of the Report of the Working Group on Business and Human Rights to the General Assembly, October 2018 (A/73/163) <<https://www.ohchr.org/sites/default/files/Documents/Issues/Business/ExecutiveSummaryA73163.pdf>> Jonathan Bonnitcha and Robert McCorquodale, 'The Concept of 'Due Diligence' in the UN

**The core assignment of this thesis was to investigate whether, compared to the newly reformed cocktail of drone regulations on civilian drones in the EU, the civilian drone regulations in the RSA and Namibia extend an acceptable level of protection to the constitutional right to information privacy within the parameters of the information privacy principles espoused under POPIA and the Namibian Data Protection Bill.**

The academic enquiry commenced with an expose of the determinants of privacy as a comprehensive right guaranteed under several national and international human rights instruments and interrogated the interplay between the comprehensive right to privacy and information privacy.

Scholarly focus has been devoted to the interplay of technology and information privacy by Brandeis and Warren as far back as 1890. Countless other academics offered theories over the decades to conceptualise the right of privacy and its relationship to information privacy.<sup>732</sup> This paper affirms the assertions by several authors that owing to various competing socio-political paradigms, it is a challenge to extract all-encompassing definitional elements for privacy.

However, with the aid of various scholarly reviews and case law, the working delineation for privacy employed for this paper is the right of persons to conduct their personal affairs without unjustifiable and disproportionate intrusions, as permitted in terms of section 36 of the RSA and article 21(2) and 22 of the Namibian Constitutions.

In terms of Section 8(1) and article 5 of the RSA and Namibian constitutions, all-natural and juristic persons are enjoined to uphold and protect the right to privacy which is guaranteed under section 14 and article 13 of the aforementioned constitutions.

The right to privacy may only be restricted in accordance with legislative stipulations setting out reasonable public interest justifications under section 14(2) and articles 21(2) and 22 of the respective constitutions.

---

Guiding Principles on Business and Human Right (2017) 28 (3) *European Journal of International Law* 899–919 <<https://doi.org/10.1093/ejil/chx042>> accessed 16 June 2022.

<sup>732</sup> Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 (5) *Harvard Review* 193.



Privacy and information privacy are often convoluted by many EU academics, particularly in scholarly works that pre-date the operationalisation of the EU Charter which occurred on 1 December 2009.<sup>733</sup>

Whilst there are divergent perspectives regarding the proximity between privacy and information privacy, this paper established that privacy (in a wide sense) and information privacy are not identical phenomena, but are nonetheless intricately intertwined and are co-dependent phenomena. Moreover, I have found that information privacy (an aspect of information privacy) is an enabler of the right to privacy.

Having established the above, I analysed the parameters of information privacy which presently includes all personally identifiable information of a living natural person. There is nevertheless jurisprudence that shows that the scope of personal information has expanded to online identifiers and there is a lot of unresolved debate on whether or not it should be stretched, to encapsulate the personal data of deceased individuals.

Following a study of the current academic appraisal on the subject matter of this thesis, primarily the work of Samantha Huneburg and Namalanga Mashinini<sup>734</sup> I was swayed to test the assertions of the aforementioned authors that the current drone regulations in RSA offend the POPIA.

This paper purposed to augment the current literature which predates the full operationalisation of the POPIA and the GDPR. In light of the regulatory developments within the drone industry, particularly the ICAO's regulations adopted on 23 June 2020 and the compendium of EU drone regulations which become fully operational in January 2024. Moreover, the paper is exclusive in so far as it proposes recommendations in response to the research questions instead of being simply explorative.

---

<sup>733</sup>The right to information privacy is recognize as an independent human right under Article 8 of the EU Charter of Fundamental Rights which entered into force together with the Treaty of Lisbon, which was signed by the EU member states on 13 December 2007, and entered into force on 1 December 2009. The entry into force of the Lisbon Treaty in 2009, gave the Charter of Fundamental Rights the same legal value as the constitutional treaties of the EU. Treaty amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (OJ C 306, 17.12.2007, p. 1–271) Available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT>> accessed 20 September 2022.

<sup>734</sup> Samantha Huneburg, 'The Rise of the drone: Privacy concerns' (2017) THRHR 586; Nomalanga Mashinini, 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) 53 De Jure Law Journal 140-158.

With this goal in mind, this paper examined the POPIA and the Namibian Data Protection Bill, 2019 in light of the provisions of the GDPR.

I found that despite their nuances and generational relativity and notwithstanding the absence of third-generation information privacy protection features in the POPIA. The POPIA and the Namibian Data Protection Bill complies with the minimum standards of information protection and thus pass the litmus test for an adequate information privacy legal framework. This finding is also supported by Roos and Warikanda in their recent evaluation of the POPIA and the GDPR.<sup>735</sup>

Although informed by unique domestic veracities and implemented and enforced via diverging mechanisms, it also emerged that these laws hold a strong asymmetry with regional and international information privacy instruments.<sup>736</sup>

After interrogating the information privacy legislation in the RSA and the envisaged law in Namibia, I established that the civil aviation regulators, drone operators and pilots are constitutionally and legislatively charged to pro-actively protect the information privacy of data subjects within the drone industry. Resultantly, data subjects whose personal information is unlawfully processed during a drone operation, have the right to be informed when their personal information is being processed and to be compensated for any loss and damage that ensues in consequence thereto, as provided for under POPIA.

Notwithstanding the extensive academic lamentation of the information privacy risks associated with drones, as well as the constitutional and international human rights due diligence call on the RSA and the SACAA, the SACAA has no legislative mandate to regulate the information privacy challenges presented by drones.

---

<sup>735</sup>Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53 (3) Comparative and International Law Journal of Southern Africa 8-9< <https://doi.org/10.25159/2522-3062/7985>> accessed 16 November 2022; Tapiwa Warikandwa, 'Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared' 2021(24) Potchefstroom Electronic Law Journal <DOI <http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727>> accessed 14 December 2022.

<sup>736</sup>G Gunasekara 'Paddling in unison or just paddling? International trends in reforming Information Privacy Law' (2014) 22 (2) International Journal of Law and Information Technology 141; Koliwe Majama, Janny Montinat and Anriette Esterhuysen (Coordinators), *Privacy and Personal Data Protection in Africa: A Rights-based Survey of Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021); See also OECD, 'Thirty years After the OECD Privacy Guidelines', (DDPR.EU, no date supplied)< <https://gdpr.eu/what-is-gdpr/>> accessed 14 February 2022.

In a recent decision of the Gauteng Province High Court, *Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others*,<sup>737</sup> the court rejected a purported refusal by the Johannesburg Roads Agency (JRA) to grant a private Electronic Communications Network Service (ECNS) that installs several CCTV cameras on public roads within Johannesburg and makes the footage available to security companies, on the ground that the companies operations constitute an infringement of the right to privacy guaranteed under the RSA constitution, although the bylaws did not permit refusal on this ground. The court held that, although the JRA had valorous intents, the absence of provisions empowering it to consider the privacy protection implications for purposes of issuing the authorization, rendered their refusal *ultra-vires*.<sup>738</sup>

Therefore, in the absence of an express mandate to address the towering information privacy implications of drones, the SACAA may be entirely precluded from asserting regulatory power with respect to information privacy, which will effectively leave data subjects without protection and a right of recourse for information privacy violations. It is therefore recommended that the CAA must be amended to empower the SACAA to assume responsibility to regulate the information privacy challenges of drones.

Furthermore, measured against the provisions of POPIA, apart from the stand-alone single reference that, pilots must respect the privacy of people in the course of deploying drones, the SACAR does not address the myriad information privacy challenges presented by drones.<sup>740</sup>

To form a comparative perspective, the drone regulations in the EU were analysed. The EU is unanimously considered an information privacy imperialist and has historically been a dominant influencer in the international civil aviation industry community. It also has a prevalent drone manufacturing base and is a pioneer in regional drone integration. The EU GDPR is selected as the benchmark for assessment, as it is acclaimed to be the toughest information privacy law worldwide.

---

<sup>737</sup>(14867/20) [2020] ZAGPJHC 186 Available at <  
<http://www.saflii.org/za/cases/ZAGPJHC/2020/186.pdf>> access 18 August 2022.

<sup>738</sup> See also Ciffe Dekker Hofmeyer Incorporated, 'Administrative bodies: - 'Stay in your lane!' (Ciffe Dekker Hofmeyer Incorporated, 20 October 2020) <  
<https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/dispute/Dispute-Resolution-Alert-20-October-2020-Administrative-bodies-Stay-in-your-lane-.html>> accessed 18 August 2022; Stefano de Gouveia, 'Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others' (Schindlers, 01 SEP 2020) <<https://www.schindlers.co.za/2020/vumacam-pty-ltd-v-johannesburg-roads-agency-and-others/>> accessed 18 August 2022.

<sup>740</sup> RSA Civil Aviation Technical Standards SA-CATS 101: 101.01.07 (d). Available at <[caa.mylexis.co.za](http://caa.mylexis.co.za)>

The comparative analysis of the drone regulations in the EU revealed that there is a definite inverse proportioned consideration of information privacy within the RSA and Namibia drone industry. Moreover, the EU recently adopted a bundle of drone regulations that offers a stencil from which lessons can be gleaned to improve the information privacy responsiveness of the drone regulations in the RSA, Namibia as well as at the ICAO level.

To generate a more wholesome understanding, the paper also examined the ICAO's stance on information privacy within the drone industry. I found that similar to the national civil aviation regulators, the ICAO denounces accountability for information privacy and left all information privacy interventions to individual member states, instead.

The ICAO justifies its reservation by asserting that privacy is beyond the scope of its mandate. The ICAO argues that even if it was within ICAO's mandate to do so, as an international organisation dealing with multiple countries with differing dogmas and ethos on information privacy and its parameters, it would be ill-advised to adopt a universally acceptable position on how to deal with information privacy within the International drone industry.

The research however illustrates that there are avenues to assume accountability for information privacy within the civil aviation industry, at least within the purview of Article 36 and a purposive interpretation of Article 44 of the Chicago Convention.<sup>741</sup>

In normatively justifying the right to information privacy within the drone industry, the paper draws a correlation to ICAO's history of expanding its mandate to accommodate environmental protection alongside safety and security, following the operationalisation of the Kyoto Protocol in 1977, which subsequently became an area of strategic focus and is presently supported by various dedicated institutional structures.

Moreover, as an international organisation, the ICAO can champion the incorporation of the protection of information privacy within the drone industry, by building on the template afforded by the EU which is a pioneer in this regard, after achieving a regional consensus on drones and privacy will certainly spearhead and support the agenda to

---

<sup>741</sup> Article 36 of the Chicago Convention (Photographic apparatus) provides that: '(e)ach contracting State may prohibit or regulate the use of photographic apparatus in aircraft over its territory'.

protect the right to information privacy within in the international drone industry and consequently accord this agenda the status of a rule of customary international law.

### 3. Main Conclusions

**Based on the research conducted the main conclusions of this study are that:**

- incontrovertibly to the hypothesis of this thesis, the drone regulations in the RSA and Namibia offer meagre, weak and ineffective information privacy protection to the information privacy challenges presented by drones;
- there are insufficient oversight, implementation and enforcement mechanisms for data subjects whose right to information privacy is infringed in the course of drone operations to seek and obtain recourse within the civil aviation industry;
- this paper affirms the assertions made by Marchant<sup>742</sup> that the existing civil aviation regulatory authorities lack the legal authority, expertise and resources to regulate emerging technologies, true;
- as advanced by Pathirana the 'inimitable challenges presented by the civil application of drones warrant a pressing intervention by governments worldwide;
- the RSA and Namibia as well as all-natural and legal persons are beholden to protect the right to information privacy, as an enabler of the constitutional right to privacy guaranteed under section 14 and article 13 of their respective constitutions through a due diligence human rights approach;
- POPIA offers mechanisms that if embraced by the leaders of the civil aviation industry and all relevant stakeholders, will offer adequate internationally aligned protection from the information privacy risks presented by drone operations;
- on an international level the ICAO is the best forum to spearhead an intervention to address the information privacy implications of drones through the promulgation of pro-information privacy model drone regulations and SARPs which will over time become a rule of customary international law;

---

<sup>742</sup>Gary E. Marchant, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 (6) *Vanderbilt Law Review* 1861; See discussion on Paragraph 4 of Chapter 1 of this thesis.

- an effective response to the information privacy implications of drones will require measures across the lifespan of a drone;
- the aviation industry is highly specialised and technical and the adherence to information privacy within the context of drones is intricately linked to the overall technical and operational requirements across the drone regulatory spectrum, therefore to avoid the duplication of resources and invariably functions and to forestall ambiguity regarding the jurisdictional roles of the respective regulatory authorities. I am of the considered opinion that the responsibility to protect and promote information privacy within the drone industry will be most effectively enforced by the civil aviation regulators, whilst the IRSA will retain overall oversight;
- there is a need to develop progressive information privacy responsive drone regulations, a code of conduct for the civil aviation drone industry and to overhaul the drone regulatory policies and practices both at an international and national level, by using the EU legal framework on drones, as a reference point.

#### **4. Recommendations**

**Informed by the conclusions synopated above, the paper recommends that;**

- the mandate and strategic focus of the ICAO, SACAA and NACAA must be expanded to include the regulation, monitoring and enforcement of privacy and information privacy within the drone industry;
- in line with the PbD information privacy principle, optimal use of PETs must be ensured and information privacy protection must be weaved in at the design and development stage as compulsory production standards;
- the drone regulations should detail compulsory information privacy-focused manufacturing standards and functionalities ;
- all drones, regardless of whether employed for commercial or personal amusement, must be registered to ensure accountability and transparency and to enable aggrieved data subjects to obtain recourse for violations of their right to information privacy;
- leeway must be granted in the regulation of drone operations to permit drone operations for purely household purposes from the regulatory ambit of civil aviation regulators;

- the unique registration details of drones must be palpable at all times through a suitable form of DRI and must include details that will enable aggrieved data subjects to bring pilots and drone operators that infringe their right to information privacy to book with relative ease;
- the civil aviation regulators in the RSA and Namibia must develop and seek the approval of a civil aviation code of conduct in line with chapter 7 of the POPIA. Consequently, this code of conduct must:
  - ✓ delineate and translate the information privacy principles set out in POPIA into practical measures and standards that all stakeholders within the drone industry must adhere to;
  - ✓ set out policies and internal systems across the regulatory spectrum to avert information privacy infringements by drone operators and pilots;
  - ✓ include dispute resolution mechanisms and avenues for data subjects to enforce and seek recourse for any violations similar to that accorded by the POPIA;<sup>743</sup>
  - ✓ include suitable aviation-focused enforcement and monitoring mechanisms;
  - ✓ contain penalties aligned with chapter 11 of the POPIA, which must include compensation for corporeal and incorporeal loss and damage;
  - ✓ require compulsory notification of information privacy violations within the drone industry, which will offer intelligence for future policy and legal reforms;
- financial support must be secured and prioritised to invest in infrastructure and technology to aid the efficient monitoring, enforcement and investigation of drone information privacy laws;
- financial resources must be committed to harnessing knowledge, skills and expertise on information privacy and POPIA in the civil aviation regulator's personnel in order to develop capacity for the enforcement and monitoring of pro-information privacy drone laws;
- considering that the enforcement of the information privacy-focused drone regulations is complex and technical, cooperation initiatives (perhaps a memorandum of understanding) to facilitate the cross-pollination of skills and

---

<sup>743</sup> Section 68 of POPIA the definition of Code of Conduct includes the Regulations and Codes and Conduct issued thereunder.

expertise within both the IRSA and the SACAA, as envisaged in terms of section 40(1) (a)(i)-(ii) of the POPIA, must be established and maintained;

- the rules regarding mandatory drone insurance which is a pre-requisite for the registration of drones must be amended to cover information privacy violations as an insurable risk and to permit drone insurance to be employed to compensate data subjects for information privacy violations under the POPIA or the civil aviation code of conduct;
- it must be compulsory that all drone operators must designate a DPO who will be responsible to spearhead the information privacy agenda in-house and will be responsible to liaise with the SACAA and the IRSA for purposes of giving effect to POPIA or the code of conduct;
- the 2C command communications link of all drones must be end-to-end encrypted and secured to protect personal information from unlawful access;
- drones must be embedded with a return to home and encryption default settings to avert the occasion of a drone getting lost and personal information falling into the hands of unauthorised persons;
- a general requirement that all pilots and drone operators are obligated to undertake a DPIA (or the alternatives introduced in the EU SORA, STS, LUC PRDA) must be introduced, to avert and mitigate information privacy damage as required under section 19(2) of the POPIA;
- the requirements in respect of approving an operation manual must be modified, to provide that an operator must stipulate the measures that will be undertaken to avert, manage, control or mitigate the information privacy risk of their envisaged drone operations;
- drone pilots and operators must be required to keep a compliance portfolio, to evidence compliance with the POPIA or the code of conduct as required in section 17 of the POPIA;
- the training circular for drone pilots or operators and approved remote pilot training institutions must be revised to incorporate compulsory modules on information privacy protection;
- safeguards to avoid the unlawful processing of personal information at the point of import or export into and from the national territory or when undertaking cross-border operations must be introduced;



- the scope of the Universal Safety Oversight Audit Programme (USOAP) must be extended to include measures to evaluate the implementation of measures to promote and protect information privacy within the drone industry;
- drone manufacturers and other relevant economic operators and stakeholders must be engaged before the development and implementation of compulsory standards for the manufacturing, sale and deployment of drones<sup>744</sup> and to regularly review and update procedures and practices;
- drone manufacturers and suppliers should be enlisted to perform market surveillance and undertake conformity assessments with independent standards institutions and endorse drones with privacy compliance endorsements on the products they place on the market.

## 5. Suggestions for Future Research

Moreover, I await with bated breath to see whether the prophecy of this thesis, that ICAO will expand its mandate and strategic focus to incorporate information privacy protection of drones, will indeed be fulfilled and that the same will be recognized as an international customary international law rule.

In closing, it is my considered opinion that future studies should investigate the enfolding compendium of EU drone regulations and examine its effectiveness in promoting and protecting information privacy within the drone industry, as well as how the EU will resolve the challenges around cross-border information privacy enforcement of information privacy infringements occasioned by drones.

I could drone on and on, and on and on, but this is the end for now...

Finally, remember privacy is precious. In my considered opinion privacy is the last true luxury.

---

<sup>744</sup>See <[https://mcusercontent.com/a65f41dee96b4db9179ffb7ba/files/0f949ddd-f72e-e7e3-e3d9-1b1297edc810/SACAA\\_ILF\\_Presentation\\_2\\_September\\_2022.pdf](https://mcusercontent.com/a65f41dee96b4db9179ffb7ba/files/0f949ddd-f72e-e7e3-e3d9-1b1297edc810/SACAA_ILF_Presentation_2_September_2022.pdf)> accessed 23 September 2022.

---

## Bibliography

### Books

Abeyratne R (ed), 'Convention on International Civil Aviation': *In Convention on International Civil Aviation: A Commentary* (Springer International Publishing 2014)

Albers M, Leenes R and De Hert Paul, 'Realising the Complexity of Data Protection': In Gurtwith S and Others (eds), *Reloading data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Miller A R, *The Assault on Privacy* (Michigan University Press 1971)

Bennett C and Raab C, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006)

Blokker N, 'Constituent Instruments': In Cogan Katz J, Ian H and Ian J (eds): In *The Oxford Handbook of International* (Oxford University Press 2016)

Boshe P, 'Data Privacy Law Reforms in Tanzania': In. Makulilo A B (ed), *African Data Privacy Laws* (Springer 2016)

Bracken-Roche C and Others, *Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada* (Office of the Privacy Commissioner of Canada 2014)

Brin D, *The Transparent Society: Will technology force us to choose between Privacy and Freedom* (1998 MIT Press)

Bulin R, 'The European Organisation for the Safety of Air Navigation - Eurocontrol': In Robertson A H (eds), *European Yearbook / Annuaire Europeen* (Springer 1976)

Burns Y and Burger-Smidt, *A Commentary on the Protection of Personal* (LexisNexis, 2018)

Bygrave L A, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer 2002)

Bygrave Lee Andrew, *Data Privacy Law: An International Perspective* (1st Edition, Oxford University Press 2014)

Cary L, 'International Civil Aviation Organization UAS Study Group': In UAS International (eds), *UAS Yearbook - UAS: The Global Perspective* (Blyenburgh and Co 2010)

Cavoukian A, *Privacy by Design The 7 Foundational Principles* (Information and Privacy Commissioner, Ontario, Canada, 2009)

Cavoukian A, *Privacy by Design: Take the Challenge* (Information and Privacy Commissioner of Ontario 2009)

---

Cavoukian A, *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario, Canada, 2011)

Cavoukian A, and Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Canada: Office of the Privacy Commissioner, 2011)

Cavoukian A, 'Privacy and Drones: Unmanned Aerial Vehicles; (Information and Privacy Commissioner Ontario, Canada Office 13 August 2012)

Cavoukian A, 'Operationalising Privacy by Design: a Guide to Implementing Strong privacy Practices' (Privacy Commissioner of Ontario 2013)

Cavoukin A, 'Privacy by Design Leadership Methods': In Gutwirths S and Others(eds), *European Data Protection: Coming of Age* (Springer Heidelberg 2013)

Chetty P and Alkalay A, 'Namibia': In Majama K, Montinat J and Esterhuysen A (Coordinators), *Privacy and Personal Data Protection in Africa: A Rights-based Survey of Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021)

Clapham A, *Human Rights Obligations of Non-State Actors* (Oxford University Press 2006)

Costello R A, 'The Impacts of AdTech on Privacy Rights and the Rule of Law': In Leenes R and Martin A (eds), *Technology and Regulation 2020* (Open Press Tilburg University 2021)

Currie I and De Waal J, *The Bill of Rights Handbook* (6th edition, Juta 2013)

Custers B, 'Drones Here, There and Everywhere: Introduction and Overview': In Custers B (ed), *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives* (Springer 2016)

Dalamagkidis K, 'Aviation History and Unmanned Flight': In Valavanis K P and Vachtsevanos G J (eds), *Handbook of Unmanned Aerial Vehicles* (Springer 2015)

Dalamagkidis, K. Valavanis K, and Piegl L (eds), On Integrating Unmanned Aircraft Systems into the National Airspace System: In Issues, Challenges, Operational Restrictions, Certification, and Recommendations, Intelligent Systems, Control and Automation: Science and Engineering (Vol. 36, 2nd ed. Springer, 2012)

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action': In Gutwirth S and Others (eds), *Reinventing Data Protection* (Springer 2009)

De Miguel M M and Campos S V (eds), 'The Drone Sector in Europe': In *Ethics and Civil Drones European Policies and Proposals for the Industry* (Springer 2018)

De Stadler and Esselaar P, *A guide to the Protection of Personal Information Act* (Juta 2015)

De Terwange C, 'Is a Global Data Protection Regulatory Model possible': In Gutwirth S and Others(eds) *Reinventing data Protection* (Springer 2009)

---

Dempsey P S and Jakhu R (eds), *Handbook of Public Aviation Law* (1st ed, Routledge 2019)

Diederiks-Verschoor I H P; Philepina I H and Butler MA, *An Introduction to Air Law* (8th revised edition, Kluwer 2012)

Donna A Dulo (ed), 'Aeronautical Foundations of the Unmanned Aircraft': *In Unmanned Aircraft: In the National Airspace: in Critical Issues, Technology, and the Law* (Illinois American Bar Association 2015)

Dumberry P, 'State practice': In *The Formation and Identification of Rules of Customary International Law in International Investment Law* (Cambridge University Press, 2016)

Elaine F, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity* (Bloomsbury Publishing 2022)

European Union, *Agency for Fundamental Rights Handbook on European Data Protection Law* (Luxembourg Publications Office 2018)

Fernando L and Pazmiño F, *The International Civil Operations of Unmanned Aircraft Systems under Air Law* (Kluwer 2020)

Fiallos F, 'The Applicability of Public International Air Law Regime to the Operation of UAS', In Benjamin Ian Scott (ed.) *The Law of Unmanned Aircraft Systems: An Introduction to the Current and Future Regulation under National, Regional and International Law* (Kluwer 2016)

Finn R and Others, *Study on Privacy, Data Protection and Ethical Risks in Civil RPAS Operations* (Luxembourg: Publications Office of the European Union 2014)

Fry J D, 'Rights, Functions, and International Legal Personality of International Organizations' (2018) 32 *Boston University International Law Journal* 221

Fuster G G, *The Emergence of Data Protection Law as a Fundamental Human Right of the EU* (Springer Heidelberg 2014)

Galkin B, 'Consumer and Commercial Drones' (Library & Research Service 10 February 2021)

Gerstein R S, 'Intimacy and Privacy': In Schoeman F D (eds), *Philosophical Dimensions of Privacy* (Cambridge University Press 1984)

Goitom H, 'South Africa': In *Regulation of Drones* (The Law Library of Congress, Global Legal Research Center, 2016)

Grayling A C, *Liberty in the Age of Terror. A Defence of Civil Liberties and Enlightenment Values* (Bloomsbury 2009)

Hallinan D et al, *Data Protection and Privacy* (Volume 12, Hart Publishing 2021)

Hartzog W, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018)

Havel B F and Sanchez G S, *The Principles and Practice of International Aviation Law* (Cambridge University Press 2014)

---

Hodgkinson D and Johnston R, *International Commercial Drone Regulation and Drone Delivery Services* (Routledge 2018)

Hofstee E, *Constructing a Good Dissertation: A practical Guide to Finishing a Master's, MBA or Phd on Schedule* (EPE Publishers 2006 [2018 reprint])

Huang J, *Aviation safety through the rule of law: ICAO's mechanisms and practices*. (Kluwer Law International 2009)

Huges T P, *American Genesis; A Century of Innovation and Technological Enthusiasm* (Edward Elgar Publishing 2006)

ICAO, *Annex 6 to the Chicago Convention: Part 1 (Operation of an Aircraft)* (9th ed, ICAO 2010)

ICAO, *Circular No. 328-AN/190: Unmanned Aircraft Systems* (ICAO, 2011)

ICAO, *Global Air Traffic Management Operational Concept* (Doc 9854 AN/458) (1<sup>st</sup> ed, ICAO, 2005 (revised 2017))

ICAO, *Manual on Notification and Publication of Differences* (Doc 10055 AN/518) (1st ed, ICAO 2019)

ICAO, *Manual on Remotely Piloted Aircraft Systems* (Doc 10019) (ICAO, 1st ed, 2015).

Inness J C, *Privacy, Intimacy and Isolation* (Oxford University 1992)

Jakhu R and Dempsey PS (eds), *Handbook of Public aviation law* (Routledge 2017)

Kennedy R and Murphy M H, *Information and Communications Technology Law in Ireland* (Clarus Press 2017)

Kim D H, 'Regulations and Laws Pertaining to the use of Unmanned Aircraft Systems (UAS) by ICAO, USA, China, Japan, Australia, India, and Korea': In Tarryn K, and Others (eds), In *Global Issues Surrounding Aviation Law and Policy* (IGI 2019)

Klabbers J, *An Advanced Introduction to the Law of International Organisations* (4<sup>th</sup> ed, Cambridge University Press 2022)

Konstantinos D, Piegl L A and Valavanis K P (eds), *On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification and Recommendations* (Springer 2009)

Kreps S E, *Drones: What Everyone Needs to Know* (Oxford University Press 2016)

Lloyd I, *Information Tchnology Law* (Oxford University Press 2017)

Majama K, Montinat J and Esterhuysen A (Cordinators), *Privacy and Personal Data Protection in Africa: A Rights- based Survey of Legislation in Eight Countries* (African Declaration on Internet Rights and Freedoms Coalition 2021)

---

Marsden C T (eds), *Internet, Co-Regulation: European Law, Regulatory Governance and Legitimacy*: In *Cyberspace* (Cambridge University Press 2011)

Marshall D M, *UAS Integration into Civil Airspace: Policy, Regulations and Strategy* (John Wiley and Sons 2022)

Masutti A and Tomasello F, *International Regulation of Non-Military Drones* (1<sup>st</sup> ed, Edward Elgar Publishing 2018)

McClellan D and Others, *Shawcross and Beaumont: Air Law* (Issue 159, LexisNexis 2018)

McQuoid-Mason D, 'Privacy'; In Woolman S and Others (eds), *Constitutional Law of South Africa* (2<sup>nd</sup> ed, Juta [Revised 2011] 2014)

Milde M, *International Air Law and ICAO* (11<sup>th</sup> ed, International Publishing 2008)

Neethling J, Potgieter J M and Visser P J, *Neethling's Law of Personality* (2<sup>nd</sup> ed, LexisNexis 2007 [revised edition])

Office of the Privacy Commissioner of Canada, *Drones in Canada Report Will the Proliferation of Domestic Drone use: in Canada raise new concerns for Privacy* (Office of the Privacy Commissioner of Canada 2013)

Oppenheim C (eds), *Data Protection: In the Regulatory Environment for Electronic Information* (4<sup>th</sup> edition, Infonortics Ltd Wiltshire 2001)

Ottavio M, *Privacy and Data Protection Implications of the Civil Use of Drones: In-depth Analysis* (4<sup>th</sup> ed, European Parliament Publications, 2015)

Papadopoulos S and Ka Mtuze S (eds), 'Privacy and Data Protection'; In *Cyberlaw @SA IV: The law of the internet in South Africa* (Van Schaik 2022)

Piera A, *Greenhouse Gas Emissions from International Aviation: Legal and Policy Challenges* (11<sup>th</sup> ed, International Publishing 2015)

Réka P, *Recent EU Legislation relating to Drones in the Light of Right to Privacy* (International Multidisciplinary Scientific Conference University of Miskolc, 23-24 May, 2019)

Romera B M, *Regime Interaction and Climate Change* (Routledge 2018)

Roos A, 'Data Privacy Law': In Van der Merwe D and Others, *Information and Communication Technology Law* (3<sup>rd</sup>, LexisNexis 2021)

Schonberger V M, *Delete: the Virtue of Forgetting in the Digital Age* (Princeton University Press 2009)

Scott B I (ed), 'Terminology, Definitions and Classifications': In *The Law of Unmanned Aircraft Systems: An Introduction to the Current and Future Regulation under National, Regional and International Law* (Wolters Kluwer 2016)

Scott B I (ed), *The Law of Unmanned Aircraft Systems: An Introduction to the Current and Future Regulation under National, Regional and International Law* (Kluwer Law International 2016)

---

Scott B I, 'Key Provisions in Current Aviation Law': In Custers B (ed), *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives* (Springer 2016)

Sepulveda M et al, 'International supervisory mechanisms for Human Rights': In *Human Rights Reference Handbook* (3<sup>rd</sup> Revised, University for Peace Press 2004)

Speijker LJP and Others, *Study on the regulation of UAS in Hong Kong Final Report* (Netherlands Aerospace Centre 2018)

Vaugeois M, 'Settlement of Disputes at ICAO and Sustainable Development': In *Occasional Paper Series: Sustainable International Civil Aviation* (Centre for Research in Air and Space Law, McGill University 2016)

Woolman S and Botha H, 'Limitations': In Roux T and Bishop M (eds), *Constitutional Law of South Africa* (2<sup>nd</sup> ed, Juta 2008)

Zimmermann A and Others, *The Statute of the International Court of Justice: A Commentary* (3<sup>rd</sup> ed, Oxford University Press, 2019)

## Journal Articles

Abeyratne R, 'Law Making and Decision Making Powers of the ICAO Council - A Critical Analysis (1992) 41 Zeitschrift für Luft-> <https://lawexplores.com/legal-legitimacy-of-icao-and-direction-to-be-taken/>> access 17 August 2022

Abeyratne R, 'Aviation and Intervention' [2015] Public Health Emergency Collection 63–158 <doi: 10.1007/978-3-319-17022-0\_2> accessed 3 August 2022

Adam Warren, James Dearnly and Charles Oppenheim, 'Sources on Data Protection and Human Rights' (2002) 2 Journal of information, Law and Technology <<http://elj.warwick.ac.uk/01-2/warren.html>>accessed 28 April 2020

Ahmad N and Others, 'Unregulated drones and an emerging threat to right to Privacy: A critical overview' (2021) 4(2) Journal of Data Protection and Privacy 124-145 <<https://hstalks.com/article/6238/unregulated-drones-and-an-emerging-threat-to-right/>>

Alamouri A, Lampert A and Gerke M, 'An Exploratory Investigation of UAS Regulations in Europe and the Impact on Effective Use and Economic Potential' (2021) 5 MDPI Drones 63 <<https://doi.org/10.3390/drones5030063>>

Ashman C R, 'The Assault on Privacy by Arthur R. Miller' (1971) 20 DePaul Law Review 1062

Ayamga M and Others, 'Developing a policy framework for adoption and management of drones for agriculture in Africa' (2021) 33 (8) Technology Analysis & Strategic Management 970 <DOI: 10.1080/09537325.2020.1858047>accessed 28 March 2022

Banisar D and Davies SG, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (2012) 18 (1) John Marshall Journal of Computer & Information Law 3

---

Bassi E, 'European Drones Regulation: Today's Legal Challenges' [2019] International Conference on Unmanned Aircraft Systems (ICUAS) 443–450 < DOI:10.1109/ICUAS.2019.8798173>

Bassi E and Others, 'The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win-Win Approach to Data Protection. Aerospace Engineering, and Risk Management (2019) 29 (4). Minds and Machines 579–601

Bassi E, 'Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance' (2019b) 36 (2) Law in Context. A Socio-legal Journal < <https://doi.org/10.26826/law-in-context.v36i2.114>>

Bassi E and Pagall U, 'The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human Rights, and the Free Movement of Data in the EU' (2020) 30 Minds and Machines 439–455 < <https://doi.org/10.1007/s11023-020-09541-8>>

Bassi E, 'From Here to 2023: Civil Drones Operations and the Setting of New Legal Rules for the European Single Sky' (2020) 100 (2) Journal of Intelligent & Robotic Systems 493- 503

Bergelson V, 'It is Personal, but it is Mine? Towards Property Rights' (2004) 37 (2) University of California, Davis Law Review <<https://doi.org/10.7282/00000015>>accessed 14 July 2021

Bentley J M, 'Policing the Police: Balancing the Right to Privacy against the Beneficial Use of Drone Technology' (2019) 70 Hastings Law Journal 249 <[Avhttps://repository.uchastings.edu/hastings\\_law\\_journal/vol70/iss1/6](https://repository.uchastings.edu/hastings_law_journal/vol70/iss1/6)> accessed 12 February 2022

Bhana D, 'The Horizontal Application of the Bill of Rights: A Reconciliation of Sections 8 and 39 of the Constitution' (2013) 29 (2) South African Journal on Human Rights 351

Black W J III, 'A No-Drones Home: Solving the Home Airspace Dilemma'[2018] J Marshall Law Journal 1

Blitz M J et al, 'Regulating Drones Under the First and Fourth Amendments ' (2015) 57 (1) William & Mary Law Review 49< <https://scholarship.law.wm.edu/wmlr/vol57/iss1/3> > accessed 1 March 2022

Bonnitcha J and McCorquodale R, 'The Concept of 'Due Diligence in the UN Guiding Principles on Business and Human Right (2017) 28 (3) European Journal of International Law 899–919

Bratman B E, 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2002) 69 Tennessee Law Review 344

Burchell J, 'The Legal Protection of Privacy in South Africa: A transplantable hybrid' (2009) 13 (1) European Journal of Comparative Law and Governance 1

Butler D, 'The Dawn of the Age of the Drones: An Australian Privacy Law Perspective' (2014) 37(2) University of New South Wales Law Journal 434

Bygrave L A, 'Data Protection pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 (3) International Journal of Law and Information Technology 250



---

Bygrave L A, 'The Place of Privacy in Data Protection' (2001) 24 (1) University of Wales Law Journal 277

Bygrave L A, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 Oslo Law Review 105

Calandrillo S and Oh J, 'Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety' (2020) 23 Stanford Technical Law Review 182

Calo R, 'The Drone as Privacy Catalyst' [2011] Stanford Law Review 64

Calvo M, 'Uncertainty and Innovation: The need for effective Regulations to foster successful Integration of Personal and Commercial Drones' (2016) 22 Southwestern Journal of International 189

Campbell E and Others, 'Due Diligence Obligations of International Organizations under International Law' (2018) 50 New York University Journal of International Law and Politics 558

Cavoukian A, 'Staying one step ahead of the GDPR: embed Privacy and Security by Design' (2018) 2 (2) Cyber Security: A Peer-Reviewed Journal 173-180

Cavoukian A and Jolly N, 'Embedding Privacy and Security to gain a Competitive Advantage' (2018) 1 (4) Journal of Data Protection & Privacy 400-409

Charles R, 'The Assault on Privacy by Arthur R. Miller' (1971) 20 DePaul Law Review 1062

Chu N, 'Protecting Privacy after death' (2015) 13 (2) Northwestern Journal of Technology and Intellectual Property 225

Clarke R, 'Understanding the Drone Pandemic' (2014) 30 Computer Law & Security Review 240

Clarke R, 'The Regulation of Civilian Drones' Impacts on Behavioral Privacy' (2014) 30 (3) Computer Law & Security Review 286

Currie I and Allan K, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa' [2007] South African Journal on Human Rights 23

Danielle C and Henry L M, 'Visionary Pragmatism and the Value of Privacy in the Twenty-One Century' (2010) 108 Michigan Law Review 1107

Daugirdas K, 'International Organizations as Creators of International Law: A Good Thing? A Reply to Klabbers J' (EJIL: Talk! Blog of the European Journal of International Law 10 September 2020) <<https://www.ejiltalk.org/international-organizations-as-creators-of-international-law-a-good-thing-a-reply-to-jan-klabbers/>> accessed 22 August 2022

De Hert P and Papakonstantiniou E, 'Three scenarios for International Governance of Data Privacy: Towards an international data privacy Organisation, preferably a UN Agency?' (2013) 9 (2) Journal of Law and Policy for the Information Society 276

Denning D E and MacDoran PF, 'Location-based authentication: Grounding cyberspace for better security' (1996) 2 Computer Fraud & Security 12

Dove E S and Chen J, 'To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices?' [2020] Journal of Law, Medicine & Ethics < <https://doi.org/10.1177/1073110520917046>>

---

Dunlap T 'We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search' (2009) 51 (1) South Texas Law Review 173

Finn R L and Wright D, 'Privacy, Data Protection and Ethics for Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organisations' (2016) 32 Computer Law & Security Review 577

Florczyk K L, 'Privacy: An Elusive Concept' (2021) 34 (2) SAGE Journals: Nursing Science Quarterly 113

Floridi L, 'Four Challenges for a Theory of Informational Privacy' (2006) 8 (3) Ethics and Information Technology Journal 109

Forde A, 'The conceptual Relationship between Privacy and Data Protection' (2016) (1) Cambridge Law Review 135

Fox S J, 'The Rise of the Drones: Framework and Governance –Why Risk It!' (2017) 82 Journal of Air Law and Commerce 683

Fox S J, 'Policing: Monitoring, Investigating and Prosecuting: Drones' (2019) 6(1) European Journal of Comparative Law and Governance 78

Fox S J, 'Policing the Technological Revolution: Opportunities & Challenges!' [2019] Journal of the American Society for Information Science and Technology 56

Fox S J, 'The 'risk' of disruptive technology today (A case study of aviation – Enter the drone)' (2020) 62 Technology in Society 101304

Fox S J, 'Past Attacks, Future Risks: Where Are We 20-years After 9/11?' (2021) 14 (3) Journal of Strategic Security 112

Fry J D, 'Rights, Functions, and International Legal Personality of International Organizations (2018) 32 Boston University International Law Journal 221

Fuchs C, 'Towards an Alternative Concept of Privacy' (2011) 9 (4) Journal of Information, Communication and Ethics in Society 220

Garipey R N and Botsford D L, 'The Effectiveness of the International Civil Aviation Organization's Adjudicatory Machinery' (1976) 42 Journal of Air Law and Commerce 351

Gary E Marchant, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 Vanderbilt Law Review 1861

Gavison R, 'Privacy and the Limits of the Law' (1980) 89 (3) Yale Law Journal 421

Gionesa F and Brema A, 'From toys to tools: The Co-evolution of Technological and Entrepreneurial Developments in the Drone Industry' (2017) 60 (6) Business Horizons 875-884.

Glancy D J, 'The Invention of the Right to Privacy' (1979) 21 Arizona Law Review < <https://law.scu.edu/wp-content/uploads/Privacy.pdf>> accessed 30 June 2020

Goedhuis D, 'Question of Public International Air Law' (1952) 81 Rec des Cours 201

---

Golla S J, 'Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR' (2017) 8 (1) Journal of Intellectual Property, Information Technology and E-Commerce Law < urn: nbn:de:0009-29-45332>

Gosh Y, 'Data Protection: 'A Different Dimension under Human Rights and Intellectual Property Law' (2015) (1) International Journal of Justice and Legal Studies 39

Greenleaf G, 'An endnote on Regulating Cyberspace: Code vs Law?' [1998] University of New South Wales Law Journal 1

Greenleaf G, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) International Data Privacy Law < https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1960299> accessed 26 January 2022

Greenleaf G, 'Independence of Data Privacy Authorities (Part 1): International Standards' (2012) 3 (13) Computer Law & Security Review 28

Greenleaf G, 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?' (2013) 29 Computer Law and Security Review 430

Greenleaf G, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23 (1) Journal of Law, Information & Science 4

Greenleaf G & Georges M, 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' Privacy Laws & International Business Journal Report [2014] 18 (21) < https://ssrn.com/abstract=2546652> accessed 5 October 2021

Greenleaf G and Cottier B, 'International and Regional Commitments in Africa Data Privacy Law: A Comparative Analysis [2022] Computer & Security Law Review<https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3582478> accessed 7 January 2022

Gregorski M, 'Legislative changes regarding unmanned rights as an opportunity for professional empowerment of persons with disabilities' (2019) 4 Przegląd Europejski 45< doi: 10.5604/01.3001.0013.7888>

Gross H, 'The Concept of Privacy' [1967] New York University Law Review 34

Gunasekara G, 'Paddling in unison or just paddling? International trends in reforming Information Privacy Law' (2014) 22 (2) International Journal of Law and Information Technology 141

Harbinja E, 'Does the EU Data Protection Regime Protection, Post-Mortem Privacy and What could be the Potential Alternatives?' (2013) 10(1) Scripted 19

Havel B F and Mulligan J Q, 'Unmanned Aircraft Systems: A Challenge to Global Regulators' (2015) 65 DePaul Law Review 107

Hazel D R, 'Litigating with Class: Considering a potential framework for Class actions in Namibia' (2014) 1 (6) Namibia Law Journal 3

Hodgkinson D, and Johnston R, 'Guiding Principles Integrating RPAS into Airspace' (2015) 70(2) ICAO Journal 4

---

Hodgkinson D and Johnston R, 'Guiding principles for drones: A starting point for international regulation' (2018) 3 Perth International Law Journal 158

Huffman G M, 'Video-streaming Records and the Video Privacy Protection Act: Broadening the Scope of Personally Identifiable Information to Include Unique Device Identifiers Disclosed with Video Titles' (2016) 91 Chicago Kent Law Review 737

Huneberg S, 'The Rise of the Drone: Privacy Concerns' (2017) 81 (2) THRHR 263

Hustinx P, 'Privacy by Design: Delivering the Promises' (2010) 3 (2) Identity in the Information Society 253-255

Huttunen M, 'Unmanned, remotely piloted, or something else? Analyzing the terminological dogfight' (2017) 42(3) Air and Space Law review 349

Huttunen M, 'Drone operations in the specific category: A unique approach to aviation safety' (2019) 13 (2) Aviation & Space Journal 2–21

Ingham L A, Jones T and Maneschijn A, 'Certification of Unmanned Aerial Vehicles in South African' (2006) 22 (1) Airspace Research & Development Journal 21

Jasmontaite L and Others, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4 European Data Protection Law Review 168

Jiniuzashvili N, 'To what extent does the current EU Regulatory Framework for Civilian Drones address Privacy Issues?' (2021) 1(2) Vectors of Social Science <<https://openjournals.ge/index.php/vss/article/view/3635/3870>>

Kaiser S A, 'UAVs and their Integration into non-segregated Airspace' (2011) 36 (2) Air & Space Law Journal 161

Kamara I, 'Co-regulation in EU Personal Data Protection: the case of Technical Standards and the Privacy by Design Standardisation Mandate' (2017) 8 (1) European Journal of Law and Technology <<<https://ejlt.org/index.php/ejlt/article/view/545>>

Kartzog W, 'What is Privacy? That's the Wrong Question' (2021) 88 The University of Chicago Law Review 1677

Kellermann R, Biehle T and Fischer L, 'Drones for Parcel and Passenger Transport: A Literature Review' (2020) 4 Transportation Research Interdisciplinary Perspectives 100088

Kerr BP, 'Clear Skies or Turbulence ahead? The International Civil Aviation Organization's Obligation to mitigate Climate Change (2020)16(1) Utrecht Law Review 101<DOI:<http://doi.org/10.36633/ulr.551>>18 August 2022

Klabbers J, 'Reflections on Role Responsibility: The Responsibility of International Organizations for Failing to Act,' (2017) 28(4) European Journal of International Law 1137

Klabbers J, 'Notes on the Ideology of International Organizations Law: The International Organization for Migration, State-making, and the Market for Migration' (2019) 32 (2) Leiden Journal of International Law 383

---

Konert A and Dunin T, 'A Harmonized European Drone Market? – New EU Rules on Unmanned Aircraft Systems' (2020) 5 (3) *Advances in Science, Technology and Engineering Systems Journal* 93-99

Koops B and Leenes R 'Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law' (2014) 28 (2) *International Review of Law, Computers & Technology* 159

Koops B J, 'The trouble with European Data Protection Law' (2014) 4 (4) *International Comparative Law Quarterly* 250 <<https://doi.org/10.1093/idpl/ipu023>> accessed 14 February 2022

Koops B J, 'The Concept of Function Creep' (2021) 13 (1) *Law, Innovation and Technology* 29

Krebs D, 'Privacy by Design: Nice-to-have or a Necessary Principle of Data Protection Law?' (2013) 4 *Journal of Intellectual Property, Information Technology and Electronic Commerce* 2

Kuner C, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 *Computer Law & Security Review* 307

Lachaud E, 'What GDPR tells about certification' (2020) 38 *Computer Law & Security Review* 105457 <<https://doi.org/10.1016/j.clsr.2020.105457>>

Loideain N N, 'Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy: in Cyberspace by Christopher T. Marsden' (2012) *Cambridge Law Journal* 71

Lynskey Orla, 'Deconstructing Data Protection: The Added Value of a Right to a Data in the EU Legal order' [2014] *International and Comparative Law Quarterly* 569

Lukacs A, 'What Is Privacy? The History and Definition of Privacy' (2017) 25 (1) *Computer Law and Security Review* 84

Luppicini R and So A, 'A Techno Ethical Review of Commercial Drone use in the context of Governance, Ethics and Privacy' (2016) 46 *Technology in Society* 109

Makulilo A B, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) *International Data Privacy Law* 163

Makulilo A B, 'Data Protection Regimes in Africa: too far from the European 'adequacy' standard?' [2013] *International Data Privacy Law Journal* 42

Makulilo A B, 'A Person Is a Person through Other Persons - A Critical Analysis of Privacy and Culture in Africa' (2016) 7 (3) *Beijing Law Review* 720

Malgerie G, 'RIP: Rest in Privacy or Rest in (Quasi) Property Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions' (SSRN, 22 June 2018) <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3185249](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185249)> accessed may 2020

Manana R W and Otieno N, 'Drones Operations in Kenya: Perspectives on Privacy challenges and Prospects' (2022) 47 (1) *Air and Space Law* 75

Mantelero A, 'The future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 *Computer Law & Security Review* 105500

---

Marchant G E, 'Governance of Emerging Technologies as a Wicked Problem' (2020) 73 (6) Vanderbilt Law Review 1861

Martinez C and Others, 'SORA Methodology for Multi-UAS Airframe Inspections in an Airport' 2021 5 (4) Drones 141 <<https://doi.org/10.3390/drones5040141>>

Mashinini N, 'The processing of Personal Information using Remotely Piloted Aircraft systems in South Africa' [2020] De Jure Law Journal 140

McKelvey N, Diver C and Curran K, 'Drones and Privacy' (2015) 6 International Journal of Handheld Computing Research 44

Melissa B 'Uncharted Territory: The FAA and the Regulation of Privacy via Rulemaking for Domestic Drones' [2014] 66 (2) Administrative Law Review 484

Merket R and Bushell J, 'Managing the Drone Revolution: A systematic Literature Review into the current use of Airborne Drones and future strategic directions for their effective control' (2020) 89 Journal of Air Transport Management 101929

Michel G and Strohmeier M, 'Flying in Private Mode: Understanding and Improving the Privacy ICAO Address Program' (2020) 18 (8) Journal of Aerospace Computing, Information and Communication 1 <DOI:10.2514/1.1010938> accessed 1 June 2022

Mirza M N et al, 'Unmanned Aerial Vehicles: A Revolution in the Making' (2016) 31 Research Journal of South Asian Studies 625

Moor J H, 'The Ethics of Privacy Protection, Library trends' (1991) 39 (1-2) Intellectual Freedom 69 <<http://www.hdl.handle.net/1242/7714>> accessed 10 March 2018

Nandar M, 'Thein,' Nature of Air Law' (not supplied) 9 (1) Dagon University Commemoration of 25th Anniversary Silver Jubilee Research Journal <<https://www.dagonuniversity.edu.mm/wp-content/uploads/2019/08/Myint-Nandar-Thein-1.pdf>> accessed 14 March 2022

Naude A and Papadopoulos S, 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments' (2016) (1) THRHR 51

Ncube C B, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems' (2004) (2) 4 Journal of Information, Law and Technology 1

Nehaluddin N, Saurabh C and Ahmad M, 'Unregulated Drones and an Emerging threat to the Right to Privacy: A critical overview' (2021) 4 (2) Journal of Data Protection & Privacy 124-145(22)

Neethling J, 'The concept of Privacy in South Africa' (2005) 122 (1) The South African Law Journal 18

Neethling J, 'Features of the Protection of Personal Information Bill, 2009 and the law of Delict' (2012) 75 THRHR 245

Osrin N S C, 'South Africa's new Drone Regulations take off: Aviation Law' [2015] Sabinet African Journals <<https://hdl.handle.net/10520/EJC175197>> accessed 12 March 2022

Pagallo U, Casanovas P and Madelin R, 'The Middle-out Approach: Assessing Models of legal Governance in Data Protection, Artificial Intelligence, and the

---

Web of Data' (2019) 7(1) *The Theory and Practice of Legislation* 1–25 < <https://doi.org/10.1080/20508840.2019.1664543>>

Parker R R, 'Definition of Privacy' (1974) 27(2) *Rutgers Law Review* 275

Paterson M and McDonagh M, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 1 *Monash University Law Review* 44

Patti F P and Bartolini F, 'Digital inheritance and Post Mortem Data Protection: The Italian Reform' [2019] *European Review of Private Law* 1183

Pauletto C, 'Options towards a global standard for the protection of individuals concerning the processing of personal data' (2021) 40 *Computer Law & Security Review*

Pazdej A P, 'The proportionality principle in Privacy and Data Protection Law' (2021) 4(3) *Journal of Data Protection & Privacy* 322-331

Peekhaus W, 'South Africa's Promotion of Access to Information Act: An Analysis of Relevant Jurisprudence' (2014) 4 *Journal of Information Policy* 570-96 <<https://doi.org/10.5325/jinfopoli.4.2014.0570>> accessed 28 January 2021

Peikoff A L, 'Beyond Reductionism: Reconsidering the right to Privacy' (2008) 3 (1) *New York University Journal of Law and Liberty* <<http://www.migration.nyulaw.me/default/files>> accessed 15 April 2021

Post R C, 'Three Concepts of Privacy' (2001) 89 *Georgetown Law Journal* 2087

Pūraitė A, 'Privacy Protection In The New Eu Regulations on the use of Unmanned Aerial Systems Public Security and Public Order' 2020 (24) *Public Security and Public Order Research Journal* <<https://ojs.mruni.eu/ojs/vsvt/article/view/5539>>

Purtova N, 'Property in Personal Data: A European Perspectives on the Instrumentalist Theory of Propertisation' (2010) 2 (3) *European Journal of Legal Studies* 18

Purtova N, 'The Illusion of Personal Data as No One's Property' (2015) 7 (1) *Law, Innovation, and Technology* <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2346693](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346693)> accessed 26 December 2021

Raab C, 'Information Privacy: Networks of Regulation at the Subglobal Level' (2010) 1 (3) *Global Policy* October 2

Rautenbach I M, 'The conduct and interests protected by the right to privacy in section 14 of the Constitution' [2001] *Journal of South African Law* 115

Roos A, 'Core principles of Data Protection Law' (2006) 39(1) *Comparative International Law South Africa* 102

Roos A, 'Personal Data Protection: Explaining the International backdrop and Evaluating the current South African position' [2007] *South African Law Journal* 400 (2007) 124(2) *South African Law Journal* 421

Roos A, 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 11 (4) *Potchefstroom Electronic Law Journal* 62

---

Roos A, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53 (3) Comparative and International Law Journal of Southern Africa 8-9 <<https://doi.org/10.25159/2522-3062/7985>> accessed 16 November 2022;

Rose C, 'Appeal Relating to the Jurisdiction of the ICAO Council' (2021) 115 (2) American Journal of International Law 301-308 <<https://doi.org/10.1017/ajil.2021.8>> accessed 22 August 2022

Scharf R L, 'Game of Drones: Rolling the Dice with Unmanned Aerial Vehicles and Privacy' [2017] Scholarly Works University of Nevada, Las Vegas-William S. Boyd School of Law 1006

Scharf R L, 'Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy' (2019) 94 (3) Indiana Law Journal <<https://www.repository.law.indiana.edu/ilj/vol94/iss3/6/>> accessed 28 April 2021

Schlag C, 'New privacy battle: How the expanding use of drones continues to erode our concept of Privacy and Privacy Rights' (2013) 13 (2) Pittsburgh Journal of Technology Law & Policy 9–12

Shenoy K K and Tyagi D, 'Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky' (2022) 9 (1) International Journal of Aviation, Aeronautics, and Aerospace <<https://commons.erau.edu/ijaaa/vol9/iss1/7>> accessed 10 April 2022

Semantha F H, 'A Systematic Literature Review on Privacy by Design in the Healthcare Sector' (2020) (9) (3) MDPI Electronics <<https://doi.org/10.3390/electronics9030452>> accessed 1 April 2022

Shapiro F R, 'The Most-cited Articles' (1985) 73 (5) California Law Review 1545

Smolensky K R, 'Rights of the dead' (2009) 37 (3) Hofstra Law Review 763

Solove D J, 'Conceptualising Privacy' (2002) 90 California Law Review 1087

Solove D J, 'A Taxonomy of Privacy' (2006) 154 (3) University of Pennsylvania Law Review 477

Solove D J, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 4 San Diego Law Review 745

Staunton C and Others 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) (4) South African Medical Journal 232

Stopforth R, 'Drone Licenses-Necessities and Requirements' (2017) 73 (1) International Journal of Sciences and Research 149

Stöcker C et al, 'Review of the Current State of UAV Regulations' (2017) 9 MDPI: Remote Sens 459 <<https://www.mdpi.com/2072-4292/9/5/459#cite>> accessed 1 January 2022

Suh J, 'Drones: How They Work, Applications, and Legal Issues' [2019] Georgia Law Technology Review 502 <<https://georgetownlawtechreview.org/wpcontent/uploads/2019/05/3.1-Suh-pp-502-514c.pdf>> accessed 21 March 2022

Swales L, 'The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock?' (2022) (25)



---

Potchefstroom Electronic Law Journal < DOI <http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11180>> accessed 15 March 2022

Sweeney M, 'Book Review on Understanding Privacy by Daniel J Solove' (2012) 28 (5) International Journal of the Information Society 1

Taborda A, 'Privacy & Drone Surveillance: The Illusive Remedy' [2017] Canadian Journal of Law and Technology 379

Tadeusz Z and Wiesław M, 'Challenges for Integration of Remotely Piloted Aircraft Systems into the European Sky' (2019) 102 Scientific Journal of Silesian University of Technology Transport Series 217-229 <DOI:10.20858/sjsutst.2019.102.18> accessed 10 August 2022

Taplin K, 'South Africa's PNR regime: Privacy and Data Protection' [2021] Computer Law & Security Review < DOI:10.1016/j.clsr.2020.105524> accessed 12 March 2022

Thomasen K, 'Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation' (2018) 16 (2) Canadian Journal of Law and Technology 307

Timothy Takahashi, 'Drones and Privacy' [2012] Columbia Science and Technology Law Review <10.2139/ssrn.2035575> accessed 27 July 2021

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? Reconstructing a not So New Right' (2013) 3 International Data Privacy Law 88

Vaarst Andersen K and Others, 'The strategic responses of start-ups to regulatory constraints in the nascent drone market' (2021) 49 (1) Research Policy 104055 <<https://doi.org/10.1016/j.respol.2020>> accessed 22 September 2022

Van der Merwe D, 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda (2014) 17 (1) Potchefstroom Electronic Law Journal 298

Van der Wilt H, 'State Practice as Element of Customary International Law: A White Knight in International Criminal Law?' (2022) (1) International Criminal Law Review < [https://brill.com/view/journals/icla/20/5/article-p784\\_784.xml?language=en](https://brill.com/view/journals/icla/20/5/article-p784_784.xml?language=en)> accessed 20 August 2022

Ventouratou A, 'Defences and indispensable incidental issues: the limits of subject-matter jurisdiction in view of the recent ICJ ICAO Council judgments' (EJIL: Talk! Blog of the European Journal of International Law, 23 July 2020) <<https://www.ejiltalk.org/defences-and-indispensable-incidental-issues-the-limits-of-subject-matter-jurisdiction-in-view-of-the-recent-icj-icao-council-judgments/>> accessed 22 August 2022

Vidović A and Others, 'Operations of Drones in Controlled Airspace in Europe' (2019) 9(1) International Journal for Traffic and Transport Engineering 38 – 52 < DOI: [http://dx.doi.org/10.7708/ijtte.2019.9\(1\).04](http://dx.doi.org/10.7708/ijtte.2019.9(1).04)>

Voss G, 'Obstacles to Transatlantic Harmonization of Data Privacy Law in Context' 2019 (2) Journal of Law, Technology & Policy <405-463 < fhal-02482174f <<https://ssrn.com/abstract=2280877>> accessed 20 February 2022

Warikandwa T, 'Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared' 2021(24) Potchefstroom

---

Electronic Law Journal <DOI <http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727>> accessed 14 December 2022

Warren S D and Brandeis L D, 'The Right to Privacy' (1890) 4 (5) Harvard Law Review 193

Warren A, Dearnly J and Oppenheim C, 'Sources on Data Protection and Human Rights' (2002) 2 Journal of information, Law and Technology <<http://elj.warwick.ac.uk/01-2/warren.html>>accessed 28 April 2020

Weber R H, 'The right to be forgotten more than a Pandora's Box' [2011] Journal of Intellectual Property, Information Technology and E-commerce 12

Wilman F G, 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations' (2022) 46 Computer Law & Security Review 105728 <<https://doi.org/10.1016/j.clsr.2022.105728>>

Winter S, 'Against Posthumous Rights' (2010) 27 (2) Journal of Applied Philosophy 186

Yaacoub J P and Others, 'Security Analysis of Drones systems: Attacks, Limitations, and Recommendations' (2020) 11 Internet of Things <[10.1016/j.iot.2020.100218](https://doi.org/10.1016/j.iot.2020.100218)> accessed 12 December 2021

Zalnieruite M, 'An International Constitutional moment for Data Privacy in the times of Mass Surveillance' (2015) 23 (2) International Journal of Law and Information Technology 199

Zieliński T and Marud W, 'Challenges for integration of remotely piloted aircraft systems into the European sky (2019) 102 Scientific Journal of Silesian University of Technology. Series Transport 217-229 <DOI: <https://doi.org/10.20858/sjsutst.2019.102.18>>

## Internet Resources

Abeyratne R, 'Legal Legitimacy of ICAO and Direction to Be Taken' (Law Explorer, 10 Jan 2016) <<https://lawexplores.com/legal-legitimacy-of-icao-and-direction-to-be-taken/>> access 17 August 2022

Aerospace and Defence Industries Association of Europe Standardization (ASD-STAN) 'Introduction to the European UAS Digital Remote Id Technical Standard' (not supplied, 2021) <[https://asd-stan.org/wp-content/uploads/ASD-STAN\\_DRI\\_Introduction\\_to\\_the\\_European\\_digital\\_RID\\_UAS\\_Standard.pdf](https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf)> accessed 31 May 2022

Ashimwe E, 'Rwanda hosts Africa's first drone flying competition next month' (Observer Research Foundation, 30 Jan 2020) <<https://www.newtimes.co.rw/news/rwanda-hosts-africasfirst-drone-flying-competition-next-month>> accessed 30 January 2020

Appeal relating to the Jurisdiction of the ICAO Council under Article 84 of the Convention on International Civil Aviation (Bahrain, Egypt, Saudi Arabia and United Arab Emirates v. Qatar), Judgment, I.C.J. Reports 2020, p. 81

---

(International Court of Justice Reports of Judgments, Advisory Opinions and Orders, 2020) <<https://www.icj-cij.org/public/files/case-related/173/173-20200714-JUD-01-00-EN.pdf>> accessed 19 July 2022

Banisar D and Davies S, 'Global Internet Liability Campaign, Report on Privacy and Human rights: An International Survey of Privacy Laws and Practice' (Privacy International, no date supplied) <<http://gilc.org/privacy/survey/intro.html#defining>> accessed 21 March 2020

Barr A and Albergotti R, 'Google to buy Titan as Web Giants battle for Air Superiority' (Wall Street Journal, 14 April 2014) <<https://www.wsj.com/articles/SB10001424052702304117904579501701702936522>> accessed 19 January 2021

Beechener J, EASA, 'Updated EU Regulation 2022/425 postpones transition dates for some BVLOS unmanned operations' (Unmanned Airspace, March 16, 2022) < <https://www.unmannedairspace.info/emerging-regulations/updated-eu-regulation-2022-425-postpones-transition-dates-for-some-bvlos-unmanned-operations/>> accessed 17 July 2022

Beechener J, 'ICAO proposes legal framework for international RPAS design, type certification and operations' (ICAO, 9 February 2021) <<https://www.icao.int/Newsroom/Pages/ICAO-Council-makes-progress-on-new-remotely-piloted-aircraft-system-RPAS-standards.aspx>> accessed 21 August 2022

Bracken-Roche C et al, 'Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada: Report to the Office of the Privacy Commissioner of Canada, under the 2013-2014 Contributions Program' (Surveillance Study Centre April 30, 2014) <[https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance\\_Drones\\_Report.pdf](https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance_Drones_Report.pdf)> accessed 16 June 2021

BMF Administrator, 'CAA Publishes CAP1789 - Outlining the EU regulations for Unmanned Aircraft' (British Model Flying Association, 20 May 2022) < <https://bmfa.org/caa-publishes-cap1789-outlining-the-eu-regulations-for-unmanned-aircraft>> accessed 20 June 2022

CAP 1789 - The EU UAS Regulation Package – Outline (June 2022 Update) <<https://uavacademy.co.uk/wp-content/uploads/2020/03/CAP1789-June-2020.pdf>> accessed 17 July 2022

CMS.Law, 'GDPR Enforcement Tracker' (CMS.Law, no date supplied) < <https://www.enforcementtracker.com/>> accessed 17 July 2022

Cliffe Dekker Hofmeyer Incorporated, 'Administrative bodies: - 'Stay in your lane!'' (Cliffe Dekker Hofmeyer Incorporated, 20 October 2020) < <https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/dispute/Dispute-Resolution-Alert-20-October-2020-Administrative-bodies-Stay-in-your-lane-.html>> accessed 18 August 2022

Dawson P, 'Developing a global framework for unmanned aviation' (Coordinates, April 2018) < <https://mycoordinates.org/developing-a-global-framework-for-unmanned-aviation/>> accessed 11 June 2022

DeGarmo M T, 'Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace' (MITRE, 2004) 4 <[https://www.mitre.org/sites/default/files/pdf/04\\_1232.pdf](https://www.mitre.org/sites/default/files/pdf/04_1232.pdf)> accessed 20 August 2022

---

De Gouveia S, 'Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others' (Schindlers, 01 SEP 2020) <<https://www.schindlers.co.za/2020/vumacam-pty-ltd-v-johannesburg-roads-agency-and-others/>> accessed 18 August 2022

De Jager W, 'DRONAMICS First Cargo Drone Airline to obtain Light UAS Operator Certificate' (Drone Watch EU, May 25, 2022) <<https://www.dronewatch.eu/dronamics-first-drone-cargo-company-to-obtain-light-uas-operator-certificate/>> accessed 7 July 2022

Dempsey P S, 'The Chicago Convention as the Constitution of an International Civil Aviation Organization' (PowerPoint Presentation McGill University, 2014) <[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8ntUodr5AhXHcAKHULrBSQQFnoECAkQAQ&url=https%3A%2F%2Fwww.mcgill.ca%2Fiasl%2Ffiles%2Fiasl%2Faspl\\_633\\_dempsey\\_chicago\\_icao.ppt&usg=AOvVaw2dKw0-WmOhysK-hEPE5onc](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8ntUodr5AhXHcAKHULrBSQQFnoECAkQAQ&url=https%3A%2F%2Fwww.mcgill.ca%2Fiasl%2Ffiles%2Fiasl%2Faspl_633_dempsey_chicago_icao.ppt&usg=AOvVaw2dKw0-WmOhysK-hEPE5onc)> accessed 1 August 2022

Dib C, 'The ICAO Annexes to the Convention on International Civil Aviation (ICAO, 28 Feb 2022) <<https://unitingaviation.com/news/safety/publication-spotlight-the-icao-annexes-to-the-convention-on-international-civil-aviation/>> accessed 19 August 2022

DPC, 'Guidance Note: Legal Bases for Processing Personal Data' (Ireland Data Protection Commission, December 2019) 16 <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>> accessed 7 January 2022

Drone Enable, Unmanned Aircraft Systems (UAS) Industry (Drone Enable 2022 Symposium) <<https://www.icao.int/Meetings/DRONEENABLE2022/Documents/RFI.pdf>> accessed 21 August 2022

Dublin City Council, 'Regulations: Drone User Handbook' (not supplied) <<https://smartdublin.ie/wp-content/uploads/2021/12/Regulations-Drone-User-Handbook-V1.pdf>> accessed 17 July 2022

European Civil Aviation Conference (ECAC), 'The new EU regulatory framework for U-space' (UAS Bulletin#2, December 2021) < <https://www.ecac-ceac.org/activities/unmanned-aircraft-systems/uas-bulletin/22-uas-bulletin/505-uas-bulletin-2-the-new-eu-regulatory-framework-for-u-space>> accessed 26 June 2022

European Commission- Proposal for a Council Decision on the position to be taken on behalf of the European Union in the 222nd session of the Council of the International Civil Aviation Organization (ICAO) as regards the envisaged adoption of Amendment 177 to Annex 1, Amendment 47 to Annex 2, Amendment 108 to Annex 8, Amendment 90 to Annex 10 and of the new volume VI to Annex 10 the Convention on International Civil Aviation' Brussels, 5.2.2021 COM(2021) 48 final 2021/0027 (NLE) < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0048&rid=1>> accessed 20 June 2022

EASA, 'EASA Delivers Broker solution to enable European-wide sharing of drone registration Data', (EASA Press Release, 22 October 2020) <<https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-delivers-broker-solution-enable-european-wide-sharing-drone>> accessed 7 January 2022

EASA Opinion No 01/2018 Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories

---

EASA Opinion published on February 2018  
<<https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2001-2018.pdf>> accessed 26 June 2022

EASA Pro, 'FAQ: I would like to know about the light UAS operator certificate (LUC)' (EASA Pro, no date supplied) < <https://www.easa.europa.eu/the-agency/faqs/i-would-know-about-light-uas-operator-certificate-luc>> accessed 2 July 2022. May 2022

EASA, 'UAV Task Force Final Report: A concept for the European Regulations for Civil Unmanned Aerial Vehicles' (European Aviation Safety Agency (EASA), 11 May 2004)<[https://www.easa.europa.eu/sites/default/files/dfu/NPA\\_16\\_2005\\_Appendix.pdf](https://www.easa.europa.eu/sites/default/files/dfu/NPA_16_2005_Appendix.pdf)>accessed 14 October 2020

EDPB, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (EDPB, 02 April 2019) < [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring_en)> accessed 1 June 2022

EDPB, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (EDPB, 22 February 2022) <[https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en)> accessed 1 June 2022

EU Commission, 'CE marking' (EU Commission, no date supplied) <[https://ec.europa.eu/growth/single-market/ce-marking\\_en](https://ec.europa.eu/growth/single-market/ce-marking_en)> accessed 3 July 2022

EURNAT Office-CAO, 'Civil Aviation and UAS-RPAS -DRONES' (ICAO, 1 October 2017) <<https://unitingaviation.com/regions/eurnat/civil-aviation-and-uas-rpas-drones/>>accessed 19 May 2022

Fact.Mr, 'Global Drones Market Outlook (2022-2032)' (Fact.MR no date supplied) <<https://www.factmr.com/report/62/drone-market>> accessed 1 September 2022

Fang Liu, 'Lecture Remarks by the Secretary General of the International Civil Aviation Organization (ICAO) to the Uruguay Foreign Ministry's Diplomatic Academy (Montevideo, Uruguay 3 April 2017)' <[https://www.icao.int/Documents/secretary-general/fliu/20170403\\_URUGUAY-LECTURE.pdf](https://www.icao.int/Documents/secretary-general/fliu/20170403_URUGUAY-LECTURE.pdf)> accessed 18 August 2022

Fifth National Development Plan (NDP5) 2017/18 – 2021/2022 <<https://www.npc.gov.na/national-plans/national-plans-ndp-5/>> accessed 1 Jan 2022

Finn P, 'Domestic use of Aerial Drones by Law Enforcement likely to prompt Privacy debate' (Washington Post, 22 January 2011)<[https://www.washingtonpost.com/national/domestic-use-of-aerial-drones-by-law-enforcement-likely-to-prompt-privacy-debate/2011/01/22/ABLD0MR\\_story.html](https://www.washingtonpost.com/national/domestic-use-of-aerial-drones-by-law-enforcement-likely-to-prompt-privacy-debate/2011/01/22/ABLD0MR_story.html)> accessed 04 August 2020

Fitzpatrick D,' UAS – a new paradigm for aviation regulators' (European Civil Aviation Conference Magazine 73, 2021) < [https://www.ecac-ceac.org/images/news/ecac-news/ECAC-News\\_73\\_Unmanned\\_Aircraft\\_Systems.pdf](https://www.ecac-ceac.org/images/news/ecac-news/ECAC-News_73_Unmanned_Aircraft_Systems.pdf)> accessed 19 August 2022

Gervasius N, 'Data Protection and Privacy In Namibia: an Exploratory Study in the context of Covid-19' (Internet Society of Namibia, 2021) <

---

<https://isocnamibia.org/wp-content/uploads/2021/04/Data-Protection-During-COVID-19-Study-in-Namibia.pdf>> accessed 3 March 2022

Gianclaudio M, 'RIP: Rest in Privacy or Rest in (Quasi) Property Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions'(SSRN, 22 Jun 2018)<[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3185249](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3185249)> accessed may 2020

Giles J, 'GDPR vs POPIA: Compare the GDPR with the POPI Act?' (Michalsons,13 February 2020) <<https://www.michalsons.com/blog/gdpr-mean-popi-act/19959>> accessed 14 February 2021

Grabowski K, 'GDPR industry codes of conduct' (Crowe, 12 November 2021) <<https://www.crowe.com/pl/en-us/insights/gdpr-industry-codes-of-conduct->>accessed 17 July 2022

Grigorov Z, 'The Future of Unmanned Flight (Part 1)' (Kambourov and Partners Attorneys at Law, 21 April 2021) <<https://www.kambourov.biz/en/publications/the-future-of-flight-an-introduction-to-drone-regulations-in-the-eu-and-bulgaria>> accessed 30 May 2022

ICAO UAS Study Group, 'ICAO UAS Study Group resources' (ICAO, date not supplied) < <https://liye.info/doc-viewer>> accessed 22 August 2022

ICAO, 'Council makes progress on new remotely piloted aircraft system (RPAS) standards' (ICAO,19 March 2021)>  
<https://www.icao.int/Newsroom/NewsDoc2021fix/COM.10.21.EN.pdf>> accessed 19 August 2022

ICAO, 'ICAO RPAS SARPS' (DRONE ENABLE Webinar, 17 November 2020) <<https://www.icao.int/NACC/Documents/Meetings/2020/UAS/UASWeb-P05EN.pdf>> accessed 1 January 2022

ICAO, 'Making an ICAO Standard' (ICAO,1 November 2011) <<https://www.icao.int/safety/airnavigation/pages/standard.aspx>> accessed 17 August 2022

ICAO, 'UAS Documents' (ICAO, no date supplied) <[https://www.icao.int/Meetings/UAS/Pages/UAS\\_Documents.aspx](https://www.icao.int/Meetings/UAS/Pages/UAS_Documents.aspx)> accessed 23 August 2022

ICAO, 'UAS Related Activities: Update on ICAO UAS Advisory Group' (PowerPoint presentation 28 September 2021) <<https://www.icao.int/NACC/Documents/Meetings/2021/UASRPAS/P05-UASRPASW2-Update-ICAO-UAS-Advisory-Group-Wuennenberg.pdf>> accessed 3 August 2022

ICAO, 'Unmanned Aircraft Systems Advisory Group (UAS-AG)' (ICAO, no date supplied)< [https://www.icao.int/safety/UA/Pages/Unmanned-Aircraft-Systems-Advisory-Group-\(UAS-AG\).aspx](https://www.icao.int/safety/UA/Pages/Unmanned-Aircraft-Systems-Advisory-Group-(UAS-AG).aspx)> accessed 15 August 2022

ICAO, Model UAS Regulations: Part 101,102 and 149 <<https://www.icao.int/safety/UA/UAID/Documents/Final%20Model%20UAS%20Regulations2%20-%20Parts%20101%20and%20102.pdf>> accessed 1 August 2022

International Bar Association, 'The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa' ( IBA,2021) <

---

<https://www.lssa.org.za/wp-content/uploads/2021/07/Data-Protection-Privacy-Guide-Africa.pdf>> accessed 11 December 2021

International Conference of Data Protection and Privacy Commissioners, 'The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities' [Montreux Declaration] (27th International Conference of Data Protection and Privacy Commissioners, 6 September 2005) <<https://www.refworld.org/docid/435914f74.html>> accessed 9 October 2021

International Standards Organisation (ISO), 'Unmanned aircraft systems Part 3: Operational procedures' (ISO, November 2019) <<https://www.iso.org/obp/ui/#iso:std:iso:21384:-3:ed-1:v1:en>> accessed 19 August 2022

Joshi H and Mutreja S, 'Micro Drone Market Statistics' (Alliedmarketresearch, September 2021) <<https://www.alliedmarketresearch.com/micro-drone-market-A13679>> accessed 1 September 2022

Kariseb K, 'Namibian Supreme Court finds that National Security Concerns do not Automatically Trump Free Speech' (Oxford Human Rights Hub, May 24, 2019) < <https://ohrh.law.ox.ac.uk/namibian-supreme-court-finds-that-national-security-concerns-do-not-automatically-trump-free-speech/>> accessed 1 February 2022

Karpowicz J, 'How has GDPR reshaped the way drone stakeholders should approach data privacy?' (Commercial Drone News, 17 July 2019) <<https://www.commercialuavnews.com/europe/gdpr-drone-data-privacy>> accessed 31 May 2022

Khoury E E, 'Remotely Piloted Aircraft Systems (RPAS)' (PowerPoint Presentation, ICAO Middle East Office-Cairo, 2016) <<https://www.icao.int/MID/Documents/2016/RASG-MID5/PPT3%20-%20RPAS%20Elie.pdf>> accessed 22 August 2022

Kock S, 'An Overview of South African RPAS Regulations' (EE Publishers, February 13th, 2015) <<https://www.ee.co.za/wp-content/uploads/2015/08/Sonet-Kock.pdf>> accessed 21 June 2020

Konrad Adenauer Stiftung, 'Harambee Prosperity Plan' (KAS, no date supplied) <<https://www.kas.de/documents/279052/279101/Der+Harambee+Prosperity+Plan+II.pdf/7691d89b-2e35-20e9-86d4-cd9779a40f61?version=1.0&t=1624947238275>> accessed 1 Jan 2022

Law Reform Commission South Africa, 'Project 124: Privacy and Data Protection' (Law Reform Commission South Africa, 2009) <[https://www.justice.gov.za/salrc/reports/r\\_prj124\\_privacy%20and%20data%20protection2009.pdf](https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf)> accessed March 2021

Lawrenson T and De Oliveira R, 'South Africa: without Drone-ing On: A Legal Overview Of Drones In South Africa' (Clyde & Co, 17 October 2018) <<https://www.mondaq.com/southafrica/aviation/746350/without-drone-ing-on-a-legal-overview-of-drones-in-south-africa>> accessed 20 Jan 2021

Lum M, 'ICJ judgment on jurisdiction of the ICAO Council: off chocks, but will it take off?' (International Bar Association, no date supplied) <<https://www.ibanet.org/article/3E25F8E8-0105-4531-B502-F38C27C54C4C>> accessed 19 August 2022

Maslaton M, 'Drones and European Law Part I: Overview of Hobby and Commercial Drones' (Dedrone, no date supplied) <

---

<https://blog.dedrone.com/en/drones-and-european-law-part-i-what-hobby-and-commercial-pilots-need-to-know>> accessed 1 June 2022

Matanzima S and Gumede G, 'Drones and Delict: Robot Usage and Damage in South African Law' (Snail Attorneys @ Law Inc, 2019) < <http://www.lex-informatica.org/wp-content/uploads/2020/08/DRONES-AND-DELICT-Artificial-Intelligence-Robot-Usage-and-Damage-in-South-African-Law.pdf>>accessed 20 July 2020

Matthews K, 'What You Need to Know About Data Destruction Post-GDPR' (Spiceworks, November 27, 2018) <<https://www.spiceworks.com/it-security/data-governance/guest-article/what-you-need-to-know-about-data-destruction-post-gdpr/>> accessed 31 July 2022

McNabb M, 'Are Drones Ready to take Off in Africa?'(Dronelife,19 June 2018)<<https://dronelife.com/2018/06/19/are-drones-ready-to-take-off-in-africa-the-african-union-report/>>accessed 28 February 2020

McNulty A, 'No privacy legislation on drones flying over homes' (Mayo News, 3 March 2020) <<https://www.mayonews.ie/news/35028-no-privacy-legislation-on-drones-flying-over-homes>> accessed 30 June 2022

Mishra A, 'Ushering Drones for development Technology in Africa'(Observer Research Foundation,16 June 2019)<<https://www.orfonline.org/expert-speak/ushering-drones-for-development-technology-in-africa-51920/>> accessed 12 June 2019

Morier Y, 'Introduction of a regulatory framework for the operation of drones in the open and specific category (Presentation to ICAO 2nd RPAS Symposium 19 September 2021) <<https://www.icao.int/Meetings/RPAS17/Presentations/Yves%20Moirier.pdf>> accessed 20 May 2022

Morier Y, '2021's Key Changes in Drone Regulation Impacting International Organisations' (Dronetalks, 28 June 2021)<<https://dronetalks.online/blog/drone-regulation-international-organisations/>> accessed 20 May 2022

Mosci L, 'EU rules on drones on the launching pad'(DLA Piper, 4 July 2018)<<https://blogs.dlapiper.com/iptitaly/2018/07/eu-rules-on-drones-on-the-launching-pad-%F0%9F%9A%80/>>1 June 202

Naidoo S, 'Drone Laws South African Commercial Regulations' (Drone Laws, February2020)<[http://www.durban.gov.za/City\\_Services/engineering%20unit/Surveying\\_Land\\_Information/Documents/DroneLawsSouthAfricanCommercialRegulations.pdf](http://www.durban.gov.za/City_Services/engineering%20unit/Surveying_Land_Information/Documents/DroneLawsSouthAfricanCommercialRegulations.pdf)> accessed 21 March 2021

Namibian Legal Assistance Centre, 'Project 27: Locus Standi Discussion Paper' (LAC, no date supplied)<<https://media.namiblii.org/files/na/other/law-reform-report/NALRDC%2027/27%20LRDC%20-%20Locus%20Standi%20Discussion%20Paper.pdf>> accessed 14 February 2021

Nanfuka J, 'Data Privacy Still a neglected digital right in Africa' (Collaboration on International ICT Policy for East and Southern Africa (CIPESA, Jan 27, 2022) <<https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/>> accessed 27 January 2022

National Business Aviation Association, 'Privacy ICAO Address (PIA)' (National Business Aviation Association, 2 March 2022) < <https://nbaa.org/aircraft-operations/security/privacy/privacy-icao-address-pia/>> accessed 1 June 2022



---

New World Encyclopaedia contributors, 'Code of Hammurabi' (New World Encyclopedia February 8, 2021) <[http://www.newworldencyclopedia.org/p/index.php?title=Code\\_of\\_Hammurabi&oldid=1003616](http://www.newworldencyclopedia.org/p/index.php?title=Code_of_Hammurabi&oldid=1003616)> accessed 10 Jan 2021

Next Practice, 'ISO Publishes Draft of New Standards for Drones' (Next Practice, 7 August 2019) <<https://www.nextpractice.education/iso-publishes-draft-of-new-standards-for-drones>> accessed 19 August 2022

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980' (OECD, no date supplied) <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandtransborderflowsofpersonaldata.htm#background>> accessed 24 December 2021

OECD, 'Thirty years After the OECD Privacy Guidelines', (DDPR.EU, no date supplied) < [https://gdpr.eu/what-is-gdpr/.](https://gdpr.eu/what-is-gdpr/)> accessed 14 February 2022

Office of the President, 'Namibia Vision 2030 Policy Framework for long-term National Development' < <https://www.namfisa.com.na/wp-content/uploads/2017/10/Vision-2030.pdf>> accessed 12 February 2022

Osakwe S and Adeniran A, 'Strengthening Data Governance in Africa Project Inception Report' (CSEA, July 2021) <[https://media.africaportal.org/documents/Strengthening-Regional-Data-Governance-in-Africa-\\_Inception\\_Report.pdf](https://media.africaportal.org/documents/Strengthening-Regional-Data-Governance-in-Africa-_Inception_Report.pdf)> accessed 12 January 2022

Plaza J, 'What is the Value of the European Drone Market? (Commercial UAV News, OCTOBER 15, 2019) <<https://www.commercialuavnews.com/europe/value-european-drone-market>> accessed 20 May 2022

Raillant-Clark W, 'New Model Unmanned Aircraft Systems (UAS) Regulations to help countries set out globally-aligned civil UAS operations in domestic airspace' (ICAO, no date supplied) < <https://www.icao.int/Newsroom/Pages/New-Model-UAS-Regulations-to-help-countries-set-out-globallyaligned-civil-UAS-operations-in-domestic-airspace.aspx>> accessed 3 August 2022

Riontino M S, 'Drones, UAV and Data Protection in the EU' (Celantur, 09 February 2021) <<https://www.celantur.com/blog/drones-uav-data-protection-eu/>> accessed 26 June 2022

Sarma D and Quinn P, 'Data protection, Social, Ethical and Legal Frameworks Delivery' (not supplied, Feb 2018) < [http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN\\_D3.1\\_DataProtectionSoEL\\_Framework\\_V1\\_0\\_PU.pdf](http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN_D3.1_DataProtectionSoEL_Framework_V1_0_PU.pdf)> 31 May 2022

Savanna S and Monique J, 'Global Data Protection Laws of the World: Law in South Africa' (DLA Piper, no date supplied) <[www.dlapiperdataprotection.com/dex.html?t=law7c=ZA](http://www.dlapiperdataprotection.com/dex.html?t=law7c=ZA)> accessed 1 March 2021

Scott M, 'Europe's tech ambition: To be the World's Digital Policeman' (Politico, 20 Aug 2017) <<https://www.politico.eu/article/europe-tech-ambition-to-be-world-digital-policeman/>> accessed 15 January 2021

SESAR, European Drones Outlook Study Unlocking the value for Europe. (SESAR European Drones Outlook Study, November 2016) <[https://www.sesarju.eu/sites/default/files/documents/reports/European\\_Drones\\_Outlook\\_Study\\_2016.pdf](https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf)> accessed 28 April 2022

---

SESAR JU, 'U-Space Blueprint' (SESAR JU, 2017) 5 <<https://rpa-regulations.com/community-info/sesar-ju-u-space-blueprint-170616/>> accessed 7 January 2021

South African Law Reform Commission, 'Project 124 Privacy and Data Protection Report2009' <[https://www.justice.gov.za/salrc/reports/r\\_prj124\\_privacy%20and%20data%20protection2009.pdf](https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf)> accessed 9 January 2022

Stanley J and Crump C, 'Protecting Privacy from Aerial Surveillance: Recommendations for Government use of Drone Aircraft' (American Civil Liberties Union, December 2011) <<http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>> accessed 28 April 2020

Stein S & Bright J 'African experiments with Drone Technologies could Leapfrog decades of infrastructure' <<https://www.lexology.com/library/detail.aspx?g=c8a92220-c406-483f-af76-19f2df55c465>> accessed: 16 June 2020

Swanson B, 'Understanding the Fundamental Rights of the Data Subject and establishing your Data Privacy Program with SOAR' (Swimlane, 20 Aug 2020) <[https://swimlane.com/blog/establishing-your-data-privacy-program-with-soar?gclid=Cj0KCQjwidSWBhDdARIsAloTVb1Z5Mm1QXFSIMIDz0tLAsWE0wv8mjioomM6f4ojDGinksigEECRZYaAqOTEALw\\_wcB](https://swimlane.com/blog/establishing-your-data-privacy-program-with-soar?gclid=Cj0KCQjwidSWBhDdARIsAloTVb1Z5Mm1QXFSIMIDz0tLAsWE0wv8mjioomM6f4ojDGinksigEECRZYaAqOTEALw_wcB)> accessed 12 July 2022

Taylor A, 'Data protection: threat to GDPR's status as 'gold standard' (International Bar Association, 25 August 2020) <<https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED53221>> December 2022. 25 August 2020

Taurino D, 'Drones4Safety: Regulatory Gap/Barriers Analysis' (Drones4Safety: Version 1.0 14 September 2020) <<https://drones4safety.eu/wp-content/uploads/2021/01/D2.2-Regulatory-Gap-Barriers-Analysis.pdf>> accessed 2 June 2022

The GDPR Data Subject Rights' (OneTrust, 24 May, 2021) <[https://www.onetrust.com/blog/the-gdpr-data-subject-rights/#:~:text=Right%20to%20object%20\(GDPR%20Article,automated%20decision%20making%20or%20profiling](https://www.onetrust.com/blog/the-gdpr-data-subject-rights/#:~:text=Right%20to%20object%20(GDPR%20Article,automated%20decision%20making%20or%20profiling)> accessed 12 July 2022

Thomasen K, 'Personal drones, AI and our Privacy' (Policy, Options & Politiques, February 20, 2018) <<https://policyoptions.irpp.org/magazines/february-2018/personal-drones-ai-and-our-privacy/>> accessed 30 March 2020

Thompson R M, 'Domestic Drones and Privacy: A Primer' (Congressional Research Service 30 March 2015) <<https://sgp.fas.org/crs/misc/R43965.pdf>> accessed 11 March 2021

Van Gyseghem J, 'Model Law on Data Protection Support for Harmonization of ICT Policies in Sub-Sahara Africa (HIPSSA)', (International Telecommunications Union (ITU), 06 June 2012) <[https://www.itu.int/ITU-D/projects/ITU\\_EC\\_ACP/hipssa/docs/HIPSSA\\_implementation\\_strategy\\_EN\\_090608.pdf](https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/HIPSSA_implementation_strategy_EN_090608.pdf)> accessed 28 January 2022

Verhaegen B, 'ICAO Legal Seminar' (PowerPoint Presentation, Banjul, The Gambia, 24-25 February 2020) <<https://www.icao.int/Meetings/GambiaSeminar2020/Documents/2.3%20Benoit%20Verhaegen%20%20International%20Framework%20for%20Air%20Navigation%20Safety.pdf>> accessed 18 August 2022

---

Warren N J, 'Private Drone Use causing many to Worry, Chubb Survey Finds' (8 September 2014) <[www.prenewswire.com-releases](http://www.prenewswire.com-releases)> accessed 28 April 2021

Whitfield B, 'How It Works: ADS-B' (Flying Magazine, 8 February 2017) <<https://www.flyingmag.com/how-it-works-ads-b/>> accessed 7 January

Zaaruka B, Tjeriko C and Shilongo H, ' Paper #1: Overview of Digital Transformation in Namibia' (Bank of Namibia Annual Symposium, 4 November 2021, Windhoek) <<https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/c7/c7dc8056-584a-4558-a5a3-2d20c7f73279.pdf>> accessed 1 Jan 2022

## **Thesis**

Dima F, 'Drone Technology and Human Rights' (Bachelors Thesis, University of Twente 2017)

Donnelly D-L, 'Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law' (PhD Thesis, University of Kwazulu-Natal School of Law 2020)

Gersher S, 'Eyes in the Sky: The Domestic Deployment of Drone Technology & Aerial Surveillance in Canada'(Master's Thesis, Carleton University 2014)

Ingham L A, 'Considerations for the Roadmap of Unmanned Aerial Vehicles (UAV) in the South African Airspace' (PhD Dissertation, Stellenbosch University 2008)

Karun C,'The horizontal application of the South African Bill of Rights (LLM. Thesis, University of Natal 1998)

Lukács A, 'Protection of Employees Right to Privacy and right to Data Protection on Social Network Sites – with special regard to France and Hungary' (DPhil Thesis, University Paris Panthéon Sorbonne and University of Szeged 2020)

Majama K, 'Data Protection in Zimbabwe under the African Continental Free Trade Area: Prospects and Challenges' (Master Thesis, Africa University 2021)

Makulilo A B, 'Protection of Personal Data in Sub-Saharan Africa' (PhD Thesis, University of Bremen 2012)

Maneschijn A, 'A Framework and criteria for the operability of Unmanned Aircraft Systems' (DPhil thesis, Stellenbosch University 2010)

Milan A. Plücken, 'The regulatory approach of ICAO, the United States and Canada to Civil Unmanned Aircraft Systems, in particular to Certification and Licensing' (Master's Thesis, University Montreal, 2015)

Mwamlangala D F, 'Privacy and Security; In the Cloud: Tanzania and South Africa In Comparative Perspective' (Phd Thesis, Open University of Tanzania 2020)

Nas M JM, 'Classifying Unmanned Aircraft Systems: Developing a Legal Framework for the Purposes of Airworthiness Certification' (Master's Thesis, Murdoch University 2015)

---

Okoye J N, 'Privacy by Design' (Master's Thesis, Norwegian University of Science and Technology 2017)

Pathirana D, 'Towards better Regulation of Unmanned Aerial Vehicles in National Airspace: A Comparative Analysis of selected National Regulations' (Master of Laws Thesis, Institute of Air and Space Law and McGill University Montreal 2019)

Rodgers M W E, 'Integration of Unmanned Aircraft Systems into Civil Aviation: A Study of the U.S, South Africa And Kenya' (Phd Thesis, University of South Africa 2020)

Roos A, 'The Law of Data Protection: A Comparative Theoretical Study' (LLD Thesis, University of South Africa 2003)

Townsend B A, 'Privacy and Data Protection in E-health in Africa'(PhD Dissertation, University of Cape Town 2017)

Verboven J, 'No Fly Drone Drones versus the right to privacy (LLM Thesis, University of Tillburg 2016)

Yiannakis O A, 'Does the Current Drone Legislation in South Africa and the United Kingdom Adequately Assist Insurers and Their Underwriters to Assess and Address the Liability Risks Associated Therewith? A Comparative Study' (Masters Thesis, University of Johannesburg 2019)

## Newspaper Articles

Bernhard A, 'The Flying Car is here and it could change the World' BBC (12 November 2020) <<https://www.bbc.com/future/article/20201111-the-flying-car-is-here-vtols-jetpacks-and-air-taxis>> accessed 31 October 2022

Erastus N, 'Online shoppers' protection delayed' *The Namibian Newspaper* (Windhoek, 2 August 2021) <<https://www.namibian.com.na/208505/archive-read/Online-shoppers-protection-delayed>> accessed 1 January 2021

Khyanyile N, 'Fun with a Warning' News24 (RSA, 11 November 2019) <<https://www.news24.com/SouthAfrica/News/fun-with-a-warning-20190204-2>> accessed 4 January 2022.

National Planning Commission, Namibia, 'Launch of Namibia's Fifth National Development Plan (NDP5)' *Tralac* (RSA, 02 Jun 2017) <<https://www.tralac.org/news/article/11698-launch-of-namibia-s-fifth-national-development-plan-ndp5.html#:~:text=By%202030%2C%20Namibia's%20population%20is,disadvantaged%20persons%20into%20mainstream%20economy>> accessed 1 Jan 2022.

Routh R, 'NCIS appeal judgment: Supreme Court dismisses Intelligence appeal' *New Era* (Windhoek, 15 April 2019) < <https://neweralive.na/posts/ncis-appeal-judgmentsupreme-court-dismisses-intelligence-appeal>> 10 March 2022  
The Future of Drones Depends on Regulation, Not Just Technology *The Economist* (Online Jun. 8 2017) < <https://perma.cc/W6NR-CGEN>> accessed 22 February 2022

## Other

Abdilla A, 'EASA Drone Regulations: Overview and Implementation' (Powerpoint presentation Civil Aviation Directorate December 2019)

---

<[https://www.transport.gov.mt/Drones\\_Presentation\\_website.pdf-f4647](https://www.transport.gov.mt/Drones_Presentation_website.pdf-f4647)>  
accessed 12 June 2022

Burger CR and Jones T, 'Adapting existing training standards for unmanned aircraft: finding ways to train staff for unmanned aircraft operations' (International Aerospace Symposium of South Africa (IASSA), Centurion, South Africa, 26-28 September 2011 <<https://researchspace.csir.co.za/dspace/handle/10204/5723> >

Chetty P, 'Presentation on Regional Assessment of Data Protection Law and Policy In SADC' (PPTs) (Workshop on the SADC Harmonized Legal Framework for Cyber Security Gaborone Botswana 27th February-3rd March 2012) <[https://extranet.sadc.int/files/1813/3232/7429/media\\_statement\\_cyber\\_security\\_version\\_2.pdf](https://extranet.sadc.int/files/1813/3232/7429/media_statement_cyber_security_version_2.pdf)> accessed 28 January 2022

Da Silva S, 'ICAO UAS - Update from the UASSG (NPF/SIP/2010-WP/14)' (Workshop Presentation: International Civil Aviation Organization Eastern and Southern African Office Workshop on the Development of national performance framework for Air Navigation Systems Nairobi, 6-10 December 2010) <[https://www.icao.int/ESAF/Documents/meetings/2010/wdnpf\\_ans/docs/wp\\_02.pdf](https://www.icao.int/ESAF/Documents/meetings/2010/wdnpf_ans/docs/wp_02.pdf)>accessed 17 August 2022

Meglana K, 'Personal data: The Emergence of a New Asset Class'(Statement at World Economic Forum, 17 Jan 2011) <[https://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf)> accessed 2 Jan 2019

Privacy International "The Right to Privacy in Namibia" (2015 Universal Periodic Review 24<sup>th</sup> Session- Namibia)

SCAA, 'Remotely Piloted Aircraft Systems Part (Part 101) Regulations Workshops' Available at <<http://www.caa.co.za/Documents/RPAS/Part%20101%20-%20RPAS%20Workshops.pdf>> accessed 11 August 2020

Snail S and Ka Mtuze S and Stroom-Nzama L, 'GDPR – oriented privacy laws in South Africa and Mauritius' (PowerPoint Presentation, WEBINAR, 22 APRIL 2021) <<https://www.privacylaws.com/media/3449/southafrica.pdf>> accessed 28 November 2022

## International and Regional Instruments

### Chicago Convention

1944 Convention on International Civil Aviation (adopted 7 December 1944, entered into force 4 April 1947) 15 [UNTS 295]

### 1945 ICJ Statute

United Nations, Statute of the International Court of Justice, adopted on 18 April 1945 and entered into force on 24 October 1945 (1179, 59 Stat 1055, TS No 993).

### UDHR

1948 Universal Declaration of Human Rights (adopted 10 December 1948 [UNGA Res 217 A(III)])

### Convention 108

---

1981 Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data (adopted 28 January 1981, entered into force 1 October 1985) [CETS 108]

### **UNCLOS**

1982 United Nations Convention on the Law of the Sea adopted on Dec. 10, 1982, Montego Bay, Jamaica, 3rd UN Conference on the Law of the Sea [1833 U.N.T.S. 397,21 ILN 1261 (1982] Doc 7300

### **CRC**

1986 United Nations Convention on the Rights of the Child adopted 7 March 1990 [E/CN.4/RES/1990/74]

1990 Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly [Resolution 45/95 of 14 December 1990]

### **ICCPR**

1996 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) Treaty Serie Vol. 999 [UNTS 171]

### **Kyoto Protocol**

1997 United Nations (UN) Protocol to the United Nations Framework Convention on Climate Change (adopted 11 December 1997, entered into force 16 February 2005) (Doc FCCC/CP/1997/7/Add.1)

### **Convention 108+**

2001 & 2018 Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Supervisory Authorities and Transborder Data Flows, updated in 2018),[CETS 181+]

2001 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

2004 Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for Air Carriers and Aircraft Operators (OJ L 138, 30.4.2004, p. 1–6). Available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0785&from=EN>> accessed 31 July 2022

### **EU Charter**

2007 Charter of Fundamental Rights of the European Union adopted on 12 December 2007 (signed 12 December 2007, took effect 1

- 
- December 2009) [2012/C 326/02] (Lisbon Treaty). [2012/C 326/02]
- 2013      **SADC Model Law**  
SADC Model Law on Data Protection, e-transactions and Cybercrime
- 2009      **Malabo Convention**  
African Union Convention on Cyber Security and Personal Data Protection adopted June 27, 2014 (not operational)
- 2015      Commission Implementing Regulation (EU) 2015/1018 of 29 June 2015 laying down a list classifying occurrence in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 of the European Parliament and of the Council (OJ L 163, 30.6.2015, p. 1–17) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-20151018>> accessed 17 July 2022
- 2016      **GDPR**  
EU General Data Protection Regulation 2016/679 of 27 April 2016 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the processing of Personal Data and on the free movement of data, and repealing Directive 95/46/EC [2016] OJ L119/1
- 2018      **Basic Regulation**  
Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (PE/2/2018/REV/1 OJ L 212, 22.8.2018, p. 1–122) Available at <<http://data.europa.eu/eli/reg/2018/1139/oj>> accessed 31 July 2022
- 2019      **IR**  
Commission Implementing Regulation (EU) 2019/947 of 24 May 2019: on the Rules and Procedures for the Operation of Unmanned Aircraft entered into force on 1 July 2019 and became applicable on 31st December 2020 (C/2019/3824 OJ L 152, 11.6.2019, p. 45–71) Available at <<https://eur-lex.europa.eu/legal->

---

content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN >  
accessed 28 April 2022

#### **DR**

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems entered into force & became applicable on 1 July 2019. (C/2019/1821 OJ L 152, 11.6.2019, p. 1–40) Available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>> accessed 1 Jan 2022

#### **AMC and GM**

Acceptable Means of Compliance (AMC) and General Guidance Material (GM) to Regulation (EU) 2019/947: [Issue 1, Amendment 2 | AMC & GM to the Annex to Regulation (EU) 2019/947]. Available at < <https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2022002r>> accessed 10 July 2022

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (PE/45/2019/REV/1 OJ L 169, 25.6.2019, p. 1–44) Available at < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019R1020>> accessed 31 July 2022

#### **2020**

Commission Implementing Regulation (EU) 2020/639 of 12 May amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight (C/2020/2937 OJ L 150, 13.5.2020, p. 1–31) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2020639>> accessed 3 July 2022

Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards postponing dates of application of certain measures in the context of the COVID-19 pandemic. (C/2020/3599 OJ L 176, 5.6.2020, p. 13–14) Available at < [http://data.europa.eu/eli/reg\\_impl/2020/746/oj](http://data.europa.eu/eli/reg_impl/2020/746/oj)> accessed 31 July 2022

#### **ICAO Model UAS Regulations**

#### **2021**

ICAO, Model UAS Regulations titled Parts 101, 102 and 149. <<https://www.icao.int/safety/UA/UAID/Pages/Model-UAS-Regulations.aspx>> accessed September 2020



---

Commission Implementing Regulation (EU) 2021/665 of 22 April 2021 amending Implementing Regulation (EU) 2017/373 as regards requirements for providers of air traffic management/air navigation services and other air traffic management network functions in the U-space airspace designated in controlled airspace C/2021/2672 (OJ L 139, 23.4.2021, p. 184–186) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2021665-0>> accessed 31 July 2022

Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (C/2021/2671 OJ L 139, 23.4.2021, p. 161–183) Available at <<https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2021664>> accessed 26 June 2022

## **Domestic Legislation**

### **The Republic of South Africa**

Air Services Licensing Act 115 of 1990

Air Services Licensing Act 115 of 1990.

Childrens Act 38 of 2005

Civil Aviation Act 13 of 2009

Constitution of the Republic of South Africa

Consumer Protection Act 68 of 2000

Department of Transport RSA, 'The White Paper National Policy on Civil Aviation' 2017 (GG 40847 of 19 May 2017)

Domestic Air Services Regulations, 1991

#### **SACARs**

Eighth Amendment to the 2001 Civil Aviation Regulations: Part 101 Remotely Piloted Aircraft Systems [As amended by GNR 40376 of 28 October 2016, GNR 432 of 19 May 2017 (w.e.f. 21 June 2017) and GNR.1503 of 15 November 2021].

Electronic Communications and Transactions Act 25 of 2005

Financial Intelligence Act 2 of 2000

Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

National Credit Act 32 of 2005

National Health Act 61 of 2003

---

**PAIA**

Promotion of Access to Information Act 2 of 2000

**POPIA**

Protection of Personal Information Act 4 of 2013

**SACATS**

RSA Civil Aviation Technical Standards SA-CATS 101: 101.01.07 (d). Available at<caa.mylexis.co.za)

Standards Act 8 of 2008

**The Republic of Namibia**

Civil Aviation Act 6 of 2016

Constitution of the Republic of Namibia

Namibia Data Protection Bill [Version workshopped 24-26 February 2020

Proclamation No. 13 Amendment of State of Emergency COVID-19 Regulations: Namibian Constitution Available at<<https://www.lac.org.na/laws/2020/7180.pdf>> accessed 12 February 2022

**NAMCARs**

Part 101: 'Drones and other Remotely Piloted Aircraft' [Government Gazette No 7157 on 27 March 2020]

**List of Cases****Foreign Judgments**

Germany v Council, C-399/12, ECLI:EU:C:2014:2258

Rynes v Úrad pro ochranu osobních údajů (Case C-212/13) EU:C:2014:2428 [2014] All ER (D) 124 (May)

František Ryneš v Úřad pro ochranu osobních údajů (CJEU, Case C-212/13)

Tietosuojavaltuutettu v Jehovan todistajat (CJEU, Case C-25/17)

Bodil Lindqvist Case C-101/01 ECLI:EU:C:2003:596

Facebook Ireland Limited, Facebook Inc; Facebook Belgium BVBA v. the Belgian Data Protection Authority ("Belgian DPA") C-645/19

Appeal relating to the Jurisdiction of the ICAO Council under Article 84 of the Convention on International Civil Aviation (Bahrain, Egypt, Saudi Arabia and United Arab Emirates v. Qatar), Judgment, I.C.J. Reports 2020, p. 81

---

## **The Republic of South Africa**

Black Sash Trust v Minister of Social Development and Others (CCT48/17)  
[2018] ZACC 36; 2018 (12) BCLR 1472 (CC)

De Reuck v Director of Public Prosecutions, 2004 (1) SA 406 (CC) Directorate: Serious  
Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2001 (1) SA 545 (CC) 557D-G  
Du Plessis And Others v De Klerk and Another 1996 (3) SA 850

In re: Certification of the Constitution of the Republic of South Africa, 1996 (10)  
BCLR 1253 (CC)

Khumalo and Others v Holomisa 2002 (5) SA 401 (CC). 2002 (8) BCLR 771

Komapo v Minister of Basic Education and others (1416/2015) [2018] ZALMPPHC 18 (23 April  
2018

Manamela & Another (Director-General of Justice Intervening 2000 (3) SA 1 (CC), 2000 (5)  
BCLR 491 (CC)

Mistry v Interim Medical and Dental Council of South Africa 1998 [4] SA 1127  
Johncom Media Investments Limited v M and Others CCT 08/08) [2009] ZACC 5; 2009 (4) SA  
7 (CC).  
NM v Smith (Freedom of Expression Institute as Amicus Curiae) 2007 (5) SA 250 (CC)

Tshabalala-Msimang v Makhanya 2008) (6) SA 102 (W)  
Johncom Media Investments Limited v M and Others (CCT 08/08) [2009] ZACC 5 2009 (4) SA  
7 (CC)

Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others 14867/20)  
[2020] ZAGPJHC 186

## **The Republic of Namibia**

Director-General of Namibian Central Intelligence Service and Another v Haufiku and Others  
[2019] NASC 7

S v Lameck NAHCMD 25 (19 February 2019)

**[END]**