ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi
Alliance School of Law

International Journal
of Law and Social Sciences (IJLS)
Volume 10, Issue 1, 2024
Print ISSN: 2454-8553, Online ISSN: 2583-8644

DRONES AND PRIVACY: THE INDIAN STORY

Abhishek Dua[1]

DOI: https://doi.org/10.60143/ijls.v10.i1.2024.125

Abstract

In the 21st century, the industry of drones, also known as Unmanned Aerial Vehicles (UAVs) or Remote Piloted Aircraft Systems (RPAS), has witnessed an exponential growth, more so in civilian applications, such as surveillance and parcel delivery. From its traditional use in military operations for over a century, drones have readily been introduced in various industries ranging from agriculture, media, mining, insurance to mention a few, due to its revolutionary benefits and affordability. However, the use of drone technology has its pitfalls too. Its intricate software and hardware have the ability to use a variety of sensors to gather information/data from unique vantage points-for long periods and on a continuous basis. The prospect of having every move, every action, being monitored and possibly recorded, raises grave privacy concerns. This paper is aimed to offer a brief introduction to the concept of drones, associated privacy risks/concerns, the extant regulatory regime and finally concludes with suggestions and countermeasures to mitigate the risk.

Keywords: Drones, Privacy, Regulatory Framework, Technology, Unmanned Ariel Vehicles

Introduction

What was a dream yesterday, is reality today; and that is how technology has evolved and made path breaking advancements and changed human lives in numerous ways– be it the way wars are being fought or businesses are being conducted or the way humans are resorting to recreation. Of the many technological advancements, drones are one such progeny of technology, that embody and reflect all that technology that has changed, both in letter and spirit.

From being an application, predominantly used by the military for years, drones or unmanned aerial vehicles (UAV's) have gradually moved into public sphere by offering multipurpose civilian and commercial uses. The key reasons for this advancement may be attributed to the converging technological advances such as diminishing hardware, sophisticated software functionalities, and advanced sensors[2].

From aerial mapping to monitoring critical infrastructure areas such as ports and power plants from surveying, mining and construction, to agriculture, to media and entertainment, from insurance, to security, surveillance and enforcement, the domains using drone technology, continue to rapidly grow[3].

The drone space exceeded frontiers of imagination in 2013, when Amazon announced that it would seek to experiment with drones to make deliveries, and finally made its first drone delivery in 2016[4]. Ever since, there has been no looking back and an explosion in the usage of drones and drone-based services in the retail and commercial space has taken place.

---

1. Ph.D. Research Scholar, Alliance University and Advocate, High Court, Lucknow Bench, Lucknow.
2. Bart Elias, Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy Perspectives and the Regulatory Landscape, (CRS Report No. R44352) (Washington, DC: Congressional Research Service, 2016).
3. Anantha Padbhanabhan,(2019) Civilian Drones: Privacy Challenges and Potential Resolution, Centre for Policy Research, Working Paper, *Civilian Drones: Privacy Challenges and Potential Resolution* - CPR (cprindia.org), (last visited Jul. 6, 2024).
4. BBC News, www.bbc.com/news/technology-38320067 (last visited November 18, 2023).

A recent report by Goldman Sachs puts the global spending on drones over the next five years at approximately US$100 bn; a significant share in the commercial/civil sector is set to be focused on the construction industry[5]. Another recent report shows that the global commercial drone market revenue forecast will reach 129.33 billion dollars by 2025[6]. The scenario back home in India is no different. According to news reports, currently there are 150-200 start-ups in India that are part of the drone ecosystem, with drone taxis likely to be launched soon[7]. While drones have been around for a while, it is only in the wake of the Covid-19 pandemic that their use in various sectors was keenly explored. In April-May 2020, drones were made use of to sanitize localities, make announcements and for continuous monitoring of areas to ensure that lock downs were being properly enforced. It has been appropriately averred that "Essentially, drones moved from being a 'good-to-have' to a 'must-have' technology[8].

According to BIS Research, the drone market in India is expected to reach $1.21 billion (Rs 8,911 crore) in CY2021. It is likely to touch $1.81 billion (Rs 13,330 crore) by FY 2026 growing at a compound annual growth rate (CAGR) of 14.61 percent, as per news reports[9]. As the global and the domestic market for drones sees an upward trend and predictions show exponential growth in the years to come, debates on the legal, regulatory, and even moral issues around the use of drones have begun to take centre stage. This research is aimed to briefly introduce the concept of drones, discuss the privacy challenges posed with the deployment of drones in civilian space in India, analyse the privacy, legal and regulatory landscape and concludes with suggestions.

Drone: The Concept

Drone means an aircraft that can operate autonomously or can be operated remotely without a pilot on board[10]. In other words, it is an aircraft or an object that can be operated from far, on multiple surfaces, including air, without a human being on board to control it. In simpler terms, a drone is a flying robot which can be distantly controlled or can fly independently by the use of software-controlled flight plans in its embedded systems, that work together with onboard sensors and a global positioning system (GPS). Interestingly, drones are not a novel concept and their origin can be traced back to as early as 1896, when the first pilotless steam-powered aircraft registered a powered flight lasting over a minute[11]. From being a military exponent in the erstwhile, drones have progressed to be utilized for an expansive range of civilian uses in the present day. From being used in search and rescue operations, to surveillance, traffic monitoring, weather forecasting, fire-fighting, agriculture, photography, as well as delivery services, the application of drones in the current day and age is expanding by the day. Unlike the traditional drones or unmanned aircrafts of the past, those had considerable size and weight, therefore limited use and maneuverability, a typical modern day drone is different. It is built of light composite material, as a consequence of which it weighs much less, therefore has increased mobility. To add to the foregoing, it is equipped with different state of the art technologies such as infrared cameras, GPS and laser, that enable multifarious uses, all being controlled by remote ground control systems (GSC), also referred to as a ground cockpit. No wonder, the present day drones have the capability of flying at both, high and low altitudes, with data capturing capabilities of smart computing devices. To stitch a golden thread to the numerous utility char-

5. DroneDJ,www.dronedj.com/2019/01/28/drones-reporting-for-work-goldman-sachs (last visited Jul. 20, 2024).
6. Yassine Mekdad,Ahmet Aris, Leonardo Babun,AbdeslamEl Fergougui, Mauro Conti, Riccardo Lazzeretti,A. Selcuk Uluagac, Science Direct, *A survey on security and privacy issues of UAVs*, 224, ELSEVIER,1 (2023).
7. Naini Thaker, Drone Rules 2021: What It Means For India's Drone Technology Sector, , https://www.forbesindia.com/article/take-one-big-story-of-the-day/drone-rules-2021-what-it-means-for-indias-drone-technology-sector/70363/1(last visited Jul. 22, 2024).
8. *Id.*
9. *Id.*
10. The Drone Rules, 2021, Rule 2(h).
11. Vishvanathan, Parthan, A Game of Drones: *The Legality of the Use of Unmanned Aerial Vehicles in Targeted Strikes and Targeted Killings*, 2 (1) AALCO Journal of International Law 165 (2013), SSRN: https://ssrn.com/abstract=2385448 (last visited Jul. 22, 2024).

acteristics of a drone, the present day drone is significantly economical to operate and easily accessible to a wide range of population.[12]

Right to Privacy in India

The Right to Privacy may be defined as the right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned", a bare perusal of which would indicate that the right to privacy is a general term, encompassing a bundle of rights, viz the right to be let alone, the right to be free from unwarranted publicity etc.

As the right to privacy is widely considered to be one of the basic inalienable human right, it has been explicitly encapsulated under Article 12, the Universal Declaration of Human Rights as:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks"[13].

However, like most western nations, that have a robust framework of laws relating to privacy, the Constitution of India did not patently grant the right to privacy as a fundamental right; It did not even mention of it or specifically protect it. Nonetheless, the apex court did infer and protect the right in light of the other existing fundamental rights, viz freedom of speech and expression under Art 19(1)(a) and right to life and personal liberty under Art 21 of the Constitution of India, subject to reasonable restrictions.

Interestingly, recently the Supreme Court of India in its judgement[14], conferred upon the Right to Privacy, the status of a fundamental right, emanating from Article 21 of the Constitution of India, subject to certain reasonable restrictions. Considering the technological developments/ advancements and the attached perils, the apex court clarified that a claim of protection of privacy would be available not only against the state but also against non-state actors, as the danger of infringement of privacy could originate, from both. The Court further averred, that in this technological day and age, the right to privacy would not only be limited to the traditional right to privacy, but would also extend and cover under its ambit, privacy of digital information or informational privacy, that being an inalienable part of the right. To elucidate, this would imply that an individual would have the right to exercise control over his/her data and the ability to control his/her existence on the internet and any unauthorized use of such information would be an infringement of his/her fundamental right to privacy. However, the judgment, did not describe the specific contours of the right to informational privacy, neither did it lay down specific mechanisms through which this right was to be protected.

Drones and Privacy

Consider this: One evening, a 27-year-old woman returns home from the gym, takes off her clothes and goes dipping in the seclusion of her backyard pool. Little does she know, that she isn't alone. There is a small drone hovering 10-15 meters above her head, capturing her and her movements. In another case, a woman gets the shock of her life, when she steps out of the shower, of her fifth floor apartment, to find a drone staring at her through the window.[15] A casual perusal of such incidents, send a shrill down the spine and we are forced to ask our self, do we truly have any privacy?

As drones are being increasingly deployed for diverse purposes such as surveillance and monitoring, weather forecasting, fire-fighting, agriculture, photography, delivery services as well as recreational purposes, it is but obvious, considering their inherent characteristics of maneuverability, inbuilt state of the art technologies such as infrared cameras, GPS and laser, that in the course of their use, data/information is not only collected but is also retained, which may be critical to an

12. Holden, Paul, *Flying Robots and Privacy in Canada*, (2016) 14.1 CJLT 65., SSRN: https://ssrn.com/abstract=2571490 or http://dx.doi.org/10.2139/ssrn.2571490 (last visited Jul. 22, 2024).
13. UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), https://www.refworld.org/docid/3ae6b3712c.html Article 12, Universal Declaration of Human Rights, 1948 (last visited Jul. 22, 2024).
14. Justice K.S.Puttaswamy (Retired). vs Union of India & Ors, (2017) 10 SCC 1
15. Des Butler, *Drones and Invasions of Privacy: An International Comparison of Legal Responses*, 42(3), UNSW Law School, 1039, 2019.

individual's privacy. For instance, a woman is sunbathing topless in her backyard is photographed by a drone, commissioned by a real estate firm to advertise for a property[16].

Interestingly, the utility of drones has been best seized by surveillance/vigilance agencies and drones are being used for the purpose of mass surveillance, as their super high resolution gigapixel cameras and fake towers, enable to track people and vehicles from altitudes as high as 20,000 feet, as well as break Wi-Fi codes and intercept text messages and cell phone conversations, without the knowledge of the user or the communication service provider. These technology equipped drones can also enter test networks and collect data which is not encrypted and even set up fake access points. In lieu, such surveillance activities, whether warranted or unwarranted, effect privacy of an individual, both, directly and indirectly[17]. The use of drone by law enforcement agencies during the anti-citizenship amendment act protests and the recent farmer's protest, raised privacy violations concerns. What makes the situation alarming is the fact that the use of drones is not only restricted to the state. Even the private companies use drones, and in their use, generate vast amounts of data, to make a fortune from the collection, by using and selling such personal data, thereby compromising privacy.

Data aggregation with other personal information like bank account details, biometrics, telephone numbers, etc. acquired from other resources, can also lead to privacy infringement, which is beyond mere collection of individual data. The consequence of collection of such data and its integration with other data, which otherwise is unobservant, leads to Big Data, which may raise various latent problems relating to violation of privacy rights and consumer power. In addition, the use of drones for recreational purposes has increased over time and is promoted by the sale of drones in shops and departmental stores, where a drone with all facilities like camera, laser etc. can be purchased for a reasonable amount of 1999/-[18].

To add to the economy, such drones can be used without specialist knowledge or training and therefore the risk of damage to property or person, including violation of privacy increases manifold. Any abuse or inappropriate use of data/information collected by drones, which is retained and/or is aggregated, leads to unique privacy challenges, irrespective of the fact, whether the drones were being used by government agencies, commercial entities, or by private individuals for recreational purposes. The privacy and liberty of an individual stands on slippery ground and stands to be infringed[19].

Drones and Privacy: Regulatory Framework in India

For the first time, the Director General for Civil Aviation (DGCA), in the month of August 2018, issued rules to regulate the operation of drones in India. However, the rules overlooked amongst others, the issue of privacy.

Thereafter in January 2019, the Ministry of Civil Aviation released the 'Drone Ecosystem Policy Roadmap, 2019' (Drone Policy) which suggested for the protection of personal data/privacy generated through drone operations. In lieu, it suggested that the Original Equipment Manufacturers (OEM's) as well as the Digital Sky Service Provider (DSP's) (service providers registered on a Digital Sky platform hosted by the DGCA for various activities related to the management of unmanned aircraft system activities) can be required to include such principles of privacy and protection of personal data, by design and by default, right from the very outset. In addition, the policy recommended for establishing mechanisms for review of data, collected by use of drones and for feedback, along with establishing mechanisms for the purposes of receiving requests from the data principles to access, anonymize, and/or erasure of the data. The policy further stressed upon the need for imparting basic knowledge of the prevalent privacy/data protection regulations to the remote pilots as minimum training requirements.

16. *Id.*
17. Nishith Desai Associates, *Unravelling The Future Game of Drones. Can they be legitimized?* (2018), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Unravelling_The_Future_Game_of_Drones.pdf (last visited Aug. 2, 2024).
18. Best Drones in India Worth Buying (Legally), 2022.
19. Ann Cavoukian, Report: "Privacy and Drones: Unmanned Aerial Vehicles", IPCO, Canada (2012).

Accordingly, the Unmanned Aircraft System Rules, 2021 (UAS Rules, 2021)[20], were notified in March, 2021. However apart from other issues/lacunas, the rules inadequately tackled the issue of privacy by inserting a single provision which callously cast the entire onus of protecting the privacy of an individual as well as property on the drone operator, without elaborating on any procedural safeguards to tackle privacy breaches. It may be necessary to point out here, that the rules remain silent on the responsibility/liability of the corporate(s)/company(s) those store data, including personal data obtained by the use of drones. In pursuance, the rules attracted much criticism, thereby compelling the Ministry of Civil Aviation to replace the said rules.

In pursuance, the Ministry of Civil Aviation in August, 2021, notified Drone Rules, 2021[21], a perusal of which reveals that although there was a major policy shift towards liberalization, when compared with the erstwhile rules, the rules were but silent on the subject of privacy, with not a mention or reference, unlike the preceding rules, which at least entrusted the responsibility of ensuring privacy of persons as well as property on the drone operator, under Rule 27(h). Appallingly, there have been no attempts made to address this pressing issue of privacy infringement by operation of drones, ever since.

In a void like this, where a dedicated privacy framework for new technologies like drones, unmanned aerial systems etc., is absent, issues of privacy breaches have been regulated in a piecemeal manner under the provisions of the (Indian) Information Technology Act, 2000(IT Act, 2000) and the relevant provisions of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (SDPI Rules, 2011) issued under the Information Technology Act, 2000.

The following provisions under the IT Act, 2000 and the SDPI Rules, 2011 seek to regulate issues of privacy in relation to new technologies like drones:

The (Indian) Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Section 43-A of the (Indian) Information Technology Act, 2000, provides that a body corporate that is in possession of, or deals and handles any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances[22].

In conjunction, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, contain provisions to deal with protection of 'Sensitive Personal Data or Information of a Person', which includes personal information relating to: -

- Passwords;
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The rules provide for reasonable security practices and procedures, which a body corporate or an individual, who on its behalf collects, receives, possess, stores, deals or handles personal information/data, is required to adopt and comply, failing which and in case of breach of the obligations, pay damages to the person so affected.

Interestingly, Section 66-E of the of the (Indian) Information Technology Act, 2000 penalizes any person who violates the privacy of a person, by intentionally capturing, publishing and transmitting images of the

20. Notification date 12, March 2021.

21. Notification date 25, August, 2021.

22. Vijay Pal Dalmia, *India: Data Protection Laws in India - Everything You Must Know*, www.mondaq.com. (last visited Aug 9, 2024).

private area(s) of the person without the persons consent, with imprisonment up to three years or with fine not exceeding Rs. 10 lakh.

Under Section 72-A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of a lawful contract has been made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000 (approx. US$ 8,000)[23].

On the flip side, Section 69 of the Information Technology Act, 2000 is an exception to the foregoing rule of maintenance of privacy and secrecy of information, which provides that, when the Government is satisfied and considers it necessary in the interest of:

- the sovereignty or integrity of India,
- defence of India,
- security of the State,
- friendly relations with foreign States or
- public order or
- for preventing incitement to the commission of any cognizable offence relating to above or
- for investigation of any offence,

it may direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. A perusal of the instant provision reveals that it empowers the government/state with a free hand to intercept, monitor or decrypt any information including information of personal nature in any computer resource for reasons mentioned herein above, with no privacy obligations.

Tackling The Drone Privacy Concern

That said, the Indian Institute of Science (IISc) has formulated a method which could be a potential solution to the issue of violation of privacy, by the use of drones in the commercial sphere. According to the method, each host airspace should develop their own drone privacy policy, for which the institute has developed Privaros[24], a method that permits host airspaces to have their own set of privacy rules, which all drones entering the airspace must follow. Once a host airspace develops its own drone privacy policy, it is to be shared with the aviation authority and the drone operator, post which the privacy policy is uploaded to the drone flying into the airspace.

There are plans to integrate Privaros into the Digital Sky Network, however, until now, Privaros hasn't been officially adopted by the Indian government, as Privaros system is still being tested[25].

Interestingly, another approach to counter violations of privacy by the use of drones, which finds adoption by several counties including Australia and Canada, is the Privacy by Design (PbD) approach. The approach follows the idea of embedding privacy into the design specifications of information technologies, accountable business practices, and networked infrastructures, as a default setting, right from the outset. This would focus on setting out minimum standards for information management practices and for providing remedies for privacy breaches[26].

It is worth mentioning that the Drone Policy, 2019 suggested a similar approach of including data protection/privacy by design and default, to protect privacy. However, until now it has been kept in abeyance and it needs to be seen if and when the stakeholders adopt it to tackle the menace of violations of privacy by the use of drones.

Conclusion

It is abundantly clear that the extant drone rules do not even pay lip service to privacy concerns arising from to the use of drones in civilian space, neither has the government adopted any methods like, to integrate Privaros into the Digital Sky Network or adopt PbD (Privacy by Design) to tackle privacy violation concerns.

However, with the Digital Personal Data Protection Act, 2023 being notified, dated 11th August, 2023, gives

23. *Id.*
24. *Id.*
25. Indian Institute of Science tackles drone privacy concerns - DroneDJ.
26. Ann Cavoukian, Report: "Privacy and Drones: Unmanned Aerial Vehicles", IPCO, Canada (2012).

some reprieve, as it mandates compliance of its provisions by Data Fiduciaries, including but not limited to, processing of digital personal data only after the data principal has given affirmative consent for such processing, use of such data only for legitimate purposes, ensuring accuracy and completeness of such data, protection of such personal data in its possession or control, erasure of personal data as soon as its purpose has been accomplished.

However, as the Digital Personal Data Protection Rules are yet to be notified, the relevant provisions of the Information Technology Act, 2000, including Section 43-A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 shall remain in force for the time being.

References

1. Anantha Padbhanabhan, (2019) Civilian Drones: Privacy Challenges and Potential Resolution, Centre for Policy Research, Working Paper, Civilian Drones: Privacy Challenges and Potential Resolution - Cpr (cprindia.org), (last visited Jul. 6, 2024).
2. Ann Cavoukian, Report: "Privacy and Drones: Unmanned Aerial Vehicles", IPCO, Canada (2012).
3. Ann Cavoukian, Report: "Privacy and Drones: Unmanned Aerial Vehicles", Ipco, Canada (2012).
4. Bart Elias, Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy Perspectives and the Regulatory Landscape, (CRS Report No. R 44352) (Washington, DC: Congressional Research Service, 2016).
5. BBC News, www.bbc.com/news/technology-38320067 (last visited November 18, 2023).
6. Best Drones in India Worth Buying (Legally), 2022.
7. Des Butler, Drones and Invasions of Privacy: An International Comparison of Legal Responses, 42(3), UNSW Law School, 1039, 2019.
8. DroneDJ,www.dronedj.com/2019/01/28/drones-reporting-for-work-goldman-sachs (last visited Jul. 20, 2024).
9. Holden, Paul, Flying Robots and Privacy in Canada, (2016) 14.1 CJLT 65., SSRN: https://ssrn.com/abstract=2571490 or http://dx.doi.org/10.2139/ssrn.2571490 (last visited Jul. 22, 2024).
10. Indian Institute of Science tackles drone privacy concerns - DroneDJ.
11. Justice K.S.Puttaswamy (Retired). vs Union of India & Ors, (2017) 10 SCC 1
12. Naini Thaker, Drone Rules 2021: What It Means For India's Drone Technology Sector, https://www.forbesindia.com/article/take-one-big-story-of-the-day/drone-rules-2021-what-it-means-for-indias-drone-technology-sector/70363/1(last visited Jul. 22, 2024).
13. Nishith Desai Associates, Unravelling the Future Game of Drones. Can they be legitimized?(2018), https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Unravelling_The_Future_Game_of_Drones.pdf (last visited Aug. 2, 2024).
14. The Drone Rules, 2021, Rule 2(h).
15. UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), https://www.refworld.org/docid/3ae6b3712c.html Article 12, Universal Declaration of Human Rights, 1948 (last visited Jul. 22, 2024).
16. Vijay Pal Dalmia, India: Data Protection Laws in India - Everything You Must Know, www.mondaq.com. (last visited Aug 9, 2024).
17. Vishvanathan, Parthan, A Game of Drones: The Legality of the Use of Unmanned Aerial Vehicles in Targeted Strikes and Targeted Killings, 2 (1) Aalco Journal of International Law 165 (2013), SSRN: https://ssrn.com/abstract=2385448 (last visited Jul. 22, 2024).
18. Yassine Mekdad, Ahmet Aris, Leonardo Babun, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, A. Selcuk Uluagac, Science Direct, A survey on security and privacy issues of UAVs, 224, ELSEVIER,1 (2023).