International Journal of Aviation, Aeronautics, and Aerospace

Volume 9 | Issue 1 Article 7

2022

Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky

K Kirthan Shenoy
Gujarat National Law University, kirthanphd202020@gnlu.ac.in
Divya Tyagi
Gujarat National Law University, dtyagi@gnlu.ac.in

Use of Unmanned Aircraft Systems and Regulatory Landscape: Unravelling the Future Challenges in the High Sky

Cover Page Footnote

Conflict of Interest: No conflicts with any of the authors exist. Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

The unmanned aircraft system (UAS) is emerging as an important and fast-developing segment in aviation (Pasztor, 2018). The UAS, with its operational flexibility and diverse application, is set to command a significant share of aviation revenue (FAA, 2021c). The UAS is presently being used to inspect critical infrastructures such as surveying railways (Bojarczak & Lesiak, 2021), roadway, bridges (Feroz & Dabous, 2021), power lines (Bögel et al., 2020), or in emergencies like forest fires, volcanic activity, and flash floods when access and mobility are minimum (Tilburg, 2017). A large segment of UAS users are journalists (Goldberg, 2015), aviation enthusiasts gathering content or flying UAS for their recreational purpose. The UAS is also heavily deployed by the military (Farrow, 2016) and civil law enforcement authorities (Carr, 2021) for national security mandates. The new generation UAS with enhanced payload capacity is being used in pandemic to carry medicines and essential supplies (WEF Report, 2021). Overall, in the past decade, technology has simplified the use of UAS with significant improvement in the ability to fly more distance, onboard sensors and recording capability, increased payload capacity, and autonomous flight mode.

The UAS has come a long way from being a small parcel of the aviation segment to present time international sky dominance. The term drone or UAS has found multiple interpretations. Unmanned aircraft can traverse air space in autonomous mode or with ground control systems. The aviation regulatory organization around the globe refers to the same as drone, remotely-piloted aircraft systems, unmanned aerial vehicle (ICAO Cir 328 Unmanned Aircraft Systems (UAS; ICAO, 2011). The Convention on International Civil Aviation (Chicago Convention) (ICAO, 1944) finds no mention of the terms as mentioned earlier used in the context of UAS. The Chicago Convention under Article 8 only specifies pilotless aircraft (ICAO, 1944). The article states that the operation of pilotless aircraft needs special authorization within the contracting state's territory and permission to fly over other territories, including fulfilling the aspects of being insured.

The UAS regulatory landscape has not evolved at the same rate as the technology and falls short of addressing some issues regarding UAS operations (Current Unmanned Aircraft State Law Landscape, 2021). The first of such problems is surveillance by law enforcement authorities. Also, UAS can fly in lower airspace which raises privacy and data protection issues that need introspection. The data collection and information exchange amongst various parties also need to be addressed. The Drone cargo deliveries (Lee et al., 2019) and beyond visual range operations are in the initial stages, requiring further clarity on payload safety, product liability, and safe aerial operations.

The regulatory aspect of the use of drones has seen a lot of debate and discussion in recent times. The advent of the Covid-19 pandemic led to a significant rise in the use of UAS by state authorities and private operators (Drone Industry

Barometer 2021, 2021). The countries worldwide saw temporary ordinances and legislations floated to cope with and permit the use of UAS in varied scenarios (OECD/ITF, 2020). The UAS systems, as discussed above, have various usage. However, the same has brought forth specific issues and challenges, namely persistent surveillance, privacy, data protection, data sharing, safety, and security of individuals and other objects in navigable airspace and on the ground. The following issues need introspection to understand the challenges UAS brings forth in times to come.

Purpose

The study focused on emerging challenges from the use of Unmanned Aircraft Systems and analyzes relevant stakeholders' responses and regulatory policies.

Method

The framework used in the study is a conceptual analysis of statutes, policies relating to Unmanned Aircraft Systems. The study has also referred to case laws and incidents to understand the issues of privacy, safety, data protection in aviation law. This study primarily focuses on challenges in the operation of unmanned aircraft systems and efforts undertaken to create a secured ecosystem.

Challenges Arising From Use of Unmanned Aircraft System

Privacy

The right to privacy during UAS operations has emerged as an important issue. The UAS's ability to operate in lower air space with excellent vertical and horizontal mobility makes it suitable for various operations (Rule, 2015). UAS systems have an array of gadgets and sensors to record images, sound, data (Farris, 2018). This enhanced capability with onboard aerial sensors gives rise to situational conflict with the freedom of movement of UAS and the right to privacy of individuals on the ground. The issue also brings into question what amounts to a reasonable expectation of privacy and whether such expectation is reasonable in the eyes of society at large (Scharaf, 2019). The right to operate UAS also needs to pass the test of allowing individual peaceful enjoyment of property without falling within realms of trespass (Mathew, 2015). The conflict also arises as operators of UAS also have freedom of mobility and record relevant data in furtherance of liberty.

In the United States, the Constitution's Fourth Amendment (US Constitution - Fourth Amendment, 1791) construes essential aspects concerning privacy. The element of Aircraft surveillance was first discussed in the case of Dow Chemicals (Dow Chemical Co. V. United States, 476 U.S. 227 (1986). The Environmental Protection Agency chartered a plane and took photographs of the chemical facility without the permission of Dow chemicals. The Dow chemicals approached the federal District Court against the following action, which held that

the photography and search violated the 4th amendment of the constitution. The 6th Circuit court reversed the following decision stating that images of Dow Chemical's open facilities taken from navigable airspace did not violate the 4th amendment. The Supreme Court also affirmed the decision of the 6th Circuit, stating that the open fields visible from lawfully flying aircraft in navigable airspace will not amount to a search. Hence, it will not be a violation of the 4th amendment. The court, however, also observed that the advancement of technology and specific flying patterns to record images with advanced equipment might lead to violation of privacy in some instances.

In the Ciraolo case (California V. Ciraolo, 476 U.S. 207 (1986)), the law enforcement officials received information about illegal marijuana cultivation in the backyard of a home. The officers could not get a clear line of sight into the backyard due to fencing and enclosures. The officer used aircraft flying at 1000 feet to confirm the cultivation of marijuana and, with the photographs taken from that flight, were able to obtain a search warrant. The issue before the court was whether there was a breach of the 4th amendment while obtaining the information for the warrant, leading to seizure. The court opined that there must be a reasonable expectation of privacy and that such reasonable expectation must also be reasonable and accepted by society in general. In the present case, law enforcement officials did not breach through the fence. Still, they improvised and received the confirmation of marijuana cultivation by flying over the navigable airspace with a recording device. As such, there was no expectation of not flying such a path. Similarly, in Riley's case (Florida V. Riley, 488 U.S. 445 (1989)), the court upheld the law enforcement authorities' observations from a helicopter that verified the existence of illegal marijuana cultivation. In the following case, one of the judges pointed out that the question of violation of privacy must not be based on FAA flight height regulation but also on whether search flights are recurrent or rarity, only being conducted for achieving a particular cause must be considered.

The Kyllo case (Kyllo V. United States, 533 U.S. 27 (2001)) also brings out an essential aspect of the type of payload and data, which may affect the context of privacy. In the following case, law enforcement officials used thermal imaging devices to understand the temperature variation to assume the possible growth of illegal marijuana within the house. The use of thermal imaging devices to scan the home without a judicial warrant violated the 4th amendment. In the present case, the court observed that the image procured with the equipment was breaching the internal privacy within the four walls of the home, which was the essential cornerstone of privacy. With technology evolving, privacy will be further at-risk times to come. Thus, it is necessary not to substantially use such technology without judicial overview or sanction.

In the Jones case (United States V. Jones, 565 U.S. 400 (2012)), the use of external payloads or devices was analyzed. In the following case, the law

enforcement officers suspected that the accused was involved in the narcotics trade. The law enforcement official in that belief affixed a GPS monitoring and tracking device on the vehicle to track the movements of the Individual under investigation. The Supreme Court held the action violated the rights protected under the Fourth Amendment, stating that it was warrantless execution of authority and search to substantiate the charge of narcotics trade based on location tracking. The judges also took notice of the emergence of aspects of persistence surveillance with technology fusion in law enforcement methodology.

The Policymakers and the Courts are continuously battling technology advancement, payload structure, and data obtained by aerial Platforms (FAA, 2016). The core issue lies in the diffusion of instruments and their ability to extract data. The definition of navigable airspace and the ability to fly within limits set by federal aviation guidelines are also crucial in decision making. The unmanned aircraft system is unique with its flexible vertical and horizontal take-off/landing ability. The unmanned aircraft system predominately dominates the lower strata of navigable airspace. The aspect of payload configuration has significant advances with the ability to record images, video, audio, thermal data points. The continuous improvements lead to longer endurance wherein the individuals can be tracked and kept under Persistent Surveillance.

Persistent Surveillance

Persistent surveillance is a subset of privacy issues but has grave repercussions on the rights of individuals in the context of the use of UAS by the state (Stanley, 2014). The law enforcement agencies within the countries are constantly upgrading their surveillance mechanisms. The surveillance manner employed varies from situation to situation. The privacy of individuals is non-negotiable and can be transgressed only as an exception. The concept of persistence surveillance was initially introduced for military operations (Seymour, 2013). The idea was not to identify the individual in question but to track individuals' forward and backward movement from a particular place in each time segment. The significantly advanced systems are now foraying into the civilian/commercial domain. The aerial surveillance from unmanned aircraft systems with long endurance will significantly impact the rights of individuals (Deller, 2021). The idea of reasonable expectation of privacy and social acceptance will largely govern the use of unmanned aircraft systems.

The law enforcement authorities authorized to use UAS constantly collect data with or without a warrant. The prolonged ability of UAS to stay on station and record individuals on the ground gives immense power in the hands of law enforcement to hold massive data and analyze the target area without a warrant (Brien, 2013). The probable cause or event to access the data might be vague or uncertain, leaving scope for grave violation of freedom and privacy of individuals. Continuous data collection and its storage make it highly susceptible to misuse. The

law enforcement authorities may not always access the live feed of the target area. They may come back later to review the data feed, giving access to multiple individuals' private and personal data. With every advancement of technology, the intrusion will get amplified, and the question that emerges is whether it is reasonable to travel without getting tracked every moment.

The present thresholds test of what is justified use of aerial surveillance is suitable for fixed-wing and rotary aircraft, which are significantly different in an operational capacity. The same was highlighted when the French privacy authority National Commission for Information Technology and Civil Liberties (CNIL) recently banned using UAS by police to enforce the lockdown rules stating it exceeded the surveillance mandate (Noack, 2021).

Data Protection

The other issue to discuss in the UAS operation is data protection. There are policy discussions across Europe, North America, and Asia on data protection. In France, the National Commission for Information Technology and Civil Liberties (CNIL) issued its opinion on the 'Global Security bill' where it proposed the regulation by the legislature of airborne cameras and monitor its implementation with an independent assessment during the transition period (CNIL, 2021). The European Union has issued the 'Data Protection Impact Assessment Template' (DPIA, 2019) as policy guidance for UAS operators. In Canada, UAS operators must abide by the Personal Information Protection and Electronic Documents Act (PIPEDA) (Personal Information Protection and Electronic Documents Act (S.C. 2000, C. 5), 2000). The UAS operator must take consent to collect, use or disclose the personal information gathered and follow PIPEDA's ten fair information principles (Office of the Privacy Commissioner of Canada, 2019). The UAS, with its diverse use in civilian and law enforcement, needs detailed protocol regarding data recording, data transfer, data sharing, and data deletion. This new generation UAS has enhanced accuracy in collecting personal data like body images, biometric data, sound, locations visited. The versatility and vast operator pool make data collection beyond the UAS operation mandate a significant risk. In privacy and data protection issues, the risk arising from UAS operation varies from the specific payload, type of operator, and area of UAS operation. In addition to that, the UAS operation takes place in airspace far away from individual subjects on the ground without their knowledge.

The issue of data protection is parallel to privacy. Law enforcement authorities are already employing technology to scan the number plates of the vehicles to track movement patterns of vehicles (Blitz, 2013). The data sharing and transfers with multiple entities also call for ethical data management. If the state authorities do not specify the mandatory deletion of data after a specific time, the data is indefinitely stored with organizations to be accessed and used as per the prevailing situation. If the unmanned aircraft system collects data, then access,

deletion, and transfer protocol for such data will require clear protocols to eliminate misuse and affix accountability.

Safety and Security Concerns

The use of UAS also brings forth the question of the safety of other aircraft and individuals on the ground. The number of incidents of UAS incursion in classified airspace near airports has increased significantly (Cybersecurity and Infrastructure Security Agency, 2020). The UAS collision with any aircraft with passengers and cargo will have severe repercussions. Further, the recreational use of drones where compliance requirements are minimal can cause nuisance and damage due to inadvertent incidents (Konert & Kasprzyk, 2021). The identification of UAS and protocol to deny take-off permission remotely are presently limited. The requirement of license and training is also limited to UAS, which are classified heavy by weight or denoted with high-risk classification. The aspect of insurance and third-party liability needs further introspection to understand the damages which might arise out of UAS operation (Mathews, 2015). The procedure to ascertain the liability and identification of the operator combined with the incident investigation process still needs significant improvements.

Aviation security protocols are of the highest standards to maintain a sterile and incident-free environment, including recovery of UAS under emergency conditions (ASTM F2849-10(2019), 2019). The UAS operations are unique as the launch and recovery of most UAS are beyond the designated area presently controlled by regulators. The UAS technology can also be modified and used by non-state actors and extremists to cause security threats to harm sensitive installations (Pledger, 2021). The UAS systems are at the mercy of the intentions of the operator. Further, the UAS is dependent on a combination of onboard systems, which might be vulnerable as the same are unencrypted. The following may lead to hacking, jamming, interception leading to partial or complete loss of control.

Recent Trends from UAS Ecosystem

Privacy by Design Methodology

Privacy by design is a methodology where the drone manufacturer accounts for privacy and data protection in the design and implementation stages of the manufacturing process of the unmanned aircraft system (Cavoukian, 2012). The process involves including a robust design and registration process with an understanding of privacy policies in addition to inputs of UAS controllers and bystanders to have a compliant operation of UAS (Yao et al., 2017). Privaros is one such framework that has been developed recently for delivery drones or guest drones to be compliant with the privacy mandate of host airspace (Beck et al., 2020). Privaros framework has been designed to allow hosts to specify regulations not allowing audio/video content transmission or restricting the storage of data when guest drones are within a defined host area, which may be an apartment,

school, or complex. This allows smooth transition of drones and creates a privacy-friendly environment. An application like the Privaros framework helps the user/operators be more compliant with the regulation enacted in the domain of privacy and data protection.

Remote Identification Policy

Remote ID will act like a virtual number plate helping the operation of UAS. The rules will allow easy identification of type, size, category, authorization, and other essential parameters of the unmanned aircraft system. The initial step towards making a secure unmanned aircraft system operation is to implement mandatory remote identification (FAA, 2019b). The Remote ID types consist of a Broadcast variant which beams radio signals from operating UAS to all the receivers, and a networked centered variant where all users are connected via the internet to network Remote ID service provider (ASTM F3411-19, 2019). FAA has mandated either a standard Remote ID which is inbuilt in UAS, or a broadcast Remote ID module to be mounted on UAS (FAA, 2021d). The FAA has not mandated a network Remote ID variant. The manufacturers of UAS and Remote ID broadcast modules have to fulfill FAA accepted means of compliance (FAA, 2021a) and submit the declaration of compliance (FAA, 2021b). The European Union has issued ASD guideline 'prEN 4709-002 - Direct Remote Identification' caters to the digital identification requirements (ASD-STAN Direct Remote ID, 2021). It has also amended requirements from Regulation (EU) 2020/1058 to include networked centered Remote ID variant. The FAA can now assess the feasibility of introducing the network Remote ID variant in certain clusters to study the operational efficacy of the system.

Law Enforcement Usage - Transparency and Accountability

The use of unmanned aircraft systems by law enforcement authorities in the context of individuals must be governed to a certain extent by the issuance of a judicial warrant. The courts initially in case of Ciraolo (California V. Ciraolo, 476 U.S. 207 (1986), 1986), Riley (Florida V. Riley, 488 U.S. 445 (1989), 1989), and Dow Chemical (Dow Chemical Co. V. United States, 476 U.S. 227 (1986), 1986) held that warrantless surveillance did not violate the fourth amendment.

The Kyllo case (Kyllo V. United States, 533 U.S. 27 (2001)), examined the use of a thermal scanner, and the court held that warrantless use of a scanner violated the Fourth Amendment. Further in the Carpenter case (Carpenter V. United States, 585 U.S._, 138 S. Ct. 2206 (2018)), where the federal government obtained cell phone records and locations to track Mr. Carpenters' movement through cell site locator information. The court held that obtaining access to cell records in excess of 100 days without a warrant violated the Fourth Amendment.

The case against the Baltimore Police Department (Leaders of a Beautiful Struggle V. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021)) examined the department's use of aerial surveillance for prolonged tracking of individuals.

The U.S. Court of Appeals for the Fourth Circuit held that persistence surveillance and Aerial Investigation Research (AIR) data carried out by the Baltimore police department violated the fourth amendment. Further, in Maxon's case (Long Lake Township V. Todd Maxon and Heather Maxon, No. 349230 (Mich. Ct. App. Mar. 18, 2021), 2021), the Michigan officials contended that Maxon's were in violation of existing local zoning ordinances by keeping excess junk on the property. The Michigan officials substantiated this by photos of property obtained through drone surveillance. The Michigan court held that person has a reasonable expectation of privacy, and officials must seek a warrant for surveillance through drones. The courts are now examining the manner of UAS use, and in coming times the law enforcement authorities must be transparent on the use of unmanned aircraft systems used for surveillance and take the community into confidence.

Data Access, Retention, and Deletion Policy

The authorities or drone users collecting data must have a clear policy on accessing and retaining the data collected by unmanned aircraft systems (McNeal, 2015). Data deletion and cross-border transfer data protocols are emerging concerns. The policy must align with local data protection guidelines applicable to the aggregator of the data.

Risk Assessment and Audits

The drone ecosystem needs a custom risk assessment and audit system to continuously assess and evolve the operational efficiency and align with regulatory requirements. The Standard Practice for Compliance Audits to ASTM Standards on Unmanned Aircraft Systems is one such guideline that sets minimum requirements for all the parties involved in the UAS ecosystem to follow the manner of the audit as set forth by Committee F38 on Unmanned Aircraft Systems (ASTM F3365-19, 2019). FAA has also issued Unmanned Aircraft Systems Safety Risk Management Policy which grants authorization, waivers, and exemption to applicants in accordance with Safety Risk Management (SRM) Policy Requirements (FAA ORDER 8040.6; FAA, 2019a). The JARUS guidelines on Specific Operations Risk Assessment (SORA) issued by Joint Authorities for Rulemaking of Unmanned Systems (JARUS) is an informative document that requires six different Specific Assurance and Integrity Levels to be met where operator and competent authority are part of the qualitative process (JARUS, 2019). The drone service providers, commercial operators, and law enforcement authorities must have such detailed assessments and audits as per the above standards, which can be shared with the public to increase acceptance of UAS usage in the public domain.

The drone manufacturers are looking at possible solutions to mitigate the challenges arising from UAS operations. The operators are now looking to provide options to shield personal identification information collected during UAS operations by pixelation (Yu et al., 2018) and face anonymization of images

collected (Lee et al., 2020). UAS policies for surveillance operations by law enforcement also vary based on state legislation within the United States of America (Smith, 2015). Law enforcement use, manner of operation, exemption from disclosure of data collected during UAS operation needs to be balanced for beneficial use of UAS for policing the community (Bentley, 2019). The following aspect of national security with privacy will be tested shortly in legislative and judicial forums. In the context of safety, the manufacturers are actively installing the geofencing systems (Torens et al., 2020) to stop UAS from traversing through restricted areas. Geofencing system helps in giving timely alerts and information to an operator of possible imminent breach of a restricted area or proximity to sensitive installation (Balachandran et al., 2018).

The regulators are also trying to classify UAS based on risk category, thereby moderating compliance requirements based on the nature of UAS operation. The recent liberalization of operation over the people rule by the Federal Aviation Administration shows the flexibility from the regulator to help the UAS ecosystem (Federal Register, 2021). The aspect of registration, licensing, and compulsory marking on individual UAS is also being regulated with the compliance deadline set for the new Remoted ID rule for manufacturers set as September 16, 2022, and for UAS operators September 16, 2023 (FAA, 2021e). The stakeholders recognize the Omni role capabilities of UAS in terms of data collection. The issues about data sharing, cross border data transfer are also the center of discussion across the globe, with the European union releasing ‘Rules and procedures for the operation of unmanned aircraft (Regulation (EU) 2019/947, 2019) mandating the protection of personal data. The security paradigm has also received a fillip with sensitive installations coming under threat due to attacks mounted using modified rouge UAS as a weapon platform (Congressional Research Service, 2020). The Counter drone technology (Gettinger, 2019) and intercept protocols are being strengthened to deal with emerging threat scenarios (Guelfi et al., 2020). The civil aviation regulators are planning for a designated new vertiport (NASA/NUAIR, 2021) for effective airspace management and to desist aerial conflict with crewed flights. A vertiport will allow seamless air mobility, especially in urban centers (NUAIR, 2021).

Conclusions

The growth and expansion of the UAS industry will continue to happen rapidly. In consensus with stakeholders, the authorities must develop a balanced approach to manage UAS operations in civilian airspace. Due to daily technological advancements, there must be constant interaction with UAS manufacturers and service providers to understand the ever-changing technology landscape. The issue of privacy and data protection must be given due importance as the same appears to emerge as a constant friction point given the payload-carrying ability of UAS.

Further, the protocol related to operations and use of UAS by law enforcement must be established to avoid violation of the liberty of individuals. There must be clear protocols for BVLOS operation and high-risk flying categories. The Counter Drone regulation must specify what amounts to optimum use of force and the situation when lethal force can be used to knock out rogue UAS. The aspect of operator liability, insurance, and third-party liability also needs introspection to consider varied operating scenarios where the UAS operation may encounter adverse incidents which may or may not be reported. The cargo bearing and long-haul trial of UAS operations will bring a new set of challenges, and its operation will be required to be integrated into the present ecosystem. The UAS industry will move ahead, but the challenges need to be addressed in the interests of all stakeholders.

References

ASD-STAN Direct Remote ID. (2021). *ASD-STAN*. https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_ Introduction_to_the_European_ digital_RID_UAS_Standard.pdf

ASTM F2849-10(2019). (2019). *Standard practice for handling of unmanned aircraft systems at divert airfields*. https://www.astm.org/f2849-10r19.html

ASTM F3365-19. (2019). *Standard practice for compliance audits to ASTM standards on unmanned aircraft systems*. https://www.astm.org/f3365-19.html

ASTM F3411-19. (2019). *Standard specification for remote ID and tracking*. https://www.astm.org/f3411-19.html

Balachandran, S., Narkawicz, A., Munoz, C., & Consiglio, M. (2018, September 5). *A geofence violation prevention mechanism for small UAS*. NASA Technical Reports Server. https://ntrs.nasa.gov/citations/20190000716

Beck, R. R., Vijeev, A., & Ganapathy, V. (2020). *Privaros: A framework for privacy-compliant delivery drones*. CSA – IISc Bangalore. https://www.csa.iisc.ac.in/~vg/papers/ccs2020/ccs2020.pdf

Bentley, J. M. (2019). Policing the police: Balancing the right to privacy against the beneficial use of drone technology. *Hastings Law Journal*, *70*(1), 249-296. https://www.hastingslawjournal.org/policing-the-police-balancing-the-right-to-privacy-against-the-beneficial-use-of-drone-technology-2/

Blitz, M. J. (2013). The fourth amendment future of public surveillance: Remote recording and other searches in public space. *American University Law Review*, *63*(1), 21-86. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1899&context=aulr

Bögel, G., Cousin, L., Iversen, N., Ebeid, E. S. M., & Hennig, A. (2020). *Drones for inspection of overhead power lines with recharge function, 2020 23rd Euromicro Conference on Digital System Design (DSD)*. https://ieeexplore.ieee.org/document/9217835

Bojarczak, P., & Lesiak, P. (2021). UAVs in rail damage image diagnostics supported by deep-learning networks. *Open Engineering*. https://doi.org/10.1515/eng-2021-0033

Brien, J. (2013). Warrantless government drone surveillance: A challenge to the fourth amendment. *The John Marshall Journal of Information Technology and Privacy Law*, *30*(1), 55. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1732&context=jitpl

California v. Ciraolo, 476 U.S. 207 (1986). (1986). https://www.loc.gov/item/usrep476207/

Carpenter v. United States, 585 U.S._, 138 S. Ct. 2206 (2018). (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Carr, N. K. (2021). Programmed to protect and serve: The dawn of drones and robots in law enforcement. *Journal of Air Law and Commerce, 86*(2), 183-2018. https://scholar.smu.edu/jalc/vol86/iss2/2/

Cavoukian, A. (2012, August 1). *Privacy and drones: Unmanned aerial vehicles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/pbd-drones.pdf

CNIL. (2021, February 3). *La CNIL rend son avis sur la proposition de loi « sécurité globale » | CNIL*. CNIL |. https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-la-proposition-de-loi-securite-globale

Congressional Research Service. (2020, September 3). *Protecting against rogue drones*. https://sgp.fas.org/crs/homesec/IF11550.pdf

Current Unmanned Aircraft State Law Landscape. (2021, August 3). *National Conference of State Legislatures.* https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

Cybersecurity and Infrastructure Security Agency. (2020, November). *The threat of unmanned aircraft systems (UAS)*. https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf

Deller, R. A. (2021). Why get a warrant when you can fly over the wall? The constitutionality of aerial surveillance without a warrant. *New Mexico Law Review*, *51*(1), 234. https://digitalrepository.unm.edu/nmlr/vol51/iss1/8/

Dow Chemical Co. v. United States, 476 U.S. 227 (1986). (1986). https://tile.loc.gov/storage-services/service/ll/usrep/usrep476/usrep476227/usrep476227.pdf

DPIA. (2019). *DroneRules.eu*. https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf

Drone Industry Barometer 2021. (2021, September 13). *Drone industry insights*. https://droneii.com/project/drone-industry-barometer

Farris, K. J. (2018). Flying inside America's drone dome and landing in aerial trespass limbo. *Valparaiso University Law Review*, *53*(1), 247. https://scholar.valpo.edu/vulr/vol53/iss1/8/

Farrow, A. (2016). Drone warfare as a military instrument of counterterrorism strategy. *Air University*. https://www.airuniversity.af.edu/Portals/10/_Spanish/Journals/Volume-28_Issue-4/2016_4_02_farrow_s_eng.pdf

Federal Aviation Administration. (2016, March 16). *FAA aerospace forecast fiscal year 2016-2036*. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/fy2016-36_faa_aerospace_forecast.pdf

Federal Aviation Administration. (2019a, October 4). *FAA order 8040.6*. https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.6.pdf

Federal Aviation Administration. (2019b, December 31). *FAA remote ID, toolkit*. https://www.faa.gov/uas/media/Remote_ID_Toolkit.pdf

Federal Aviation Administration. (2021a, January 14). FAA *advisory circular 89-1*. https://www.regulations.gov/document/FAA-2019-1100-53267

Federal Aviation Administration. (2021b, January 14). *FAA advisory circular 89-2*. https://www.regulations.gov/document/FAA-2019-1100-53268

Federal Aviation Administration. (2021c, December 16). *FAA aerospace forecast fiscal years 2021–2041*. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/unmanned_aircraft_systems.pdf

Federal Aviation Administration. (2021d, October 13). *FAA remote ID for industry and standards bodies*. https://www.faa.gov/uas/getting started/remote_id/ industry/

Federal Aviation Administration. (2021e, October 13). *Remote identification for drone pilots*. https://www.faa.gov/uas/getting_started/remote_id/drone_pilots/

Federal Register. (2021, March 10). *Operation* of small unmanned aircraft systems over people; delay; withdrawal; correction. https://www.federalregister.gov/documents/2021/03/10/2021-04881/operation-of-small-unmanned-aircraft-systems-over-people-delay-withdrawal-correction

Feroz, S., & Dabous, S. A. (2021). UAV-based remote sensing applications for bridge condition assessment. *Remote Sensing*, *13*(9). https://doi.org/10.3390/rs13091809

Florida v. Riley, 488 U.S. 445 (1989). (1989). https://www.loc.gov/item/usrep488445/

Gettinger, D. (2019). Counter drone systems. *Center for the Study of the Drone*. https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

Goldberg, D. (2015). Dronalism: Journalism, remotely piloted aircraft, law and regulation. *FIU Law Review*, *10*(2), 405. https://ecollections.law.fiu.edu/lawreview/vol10/iss2/8/

Guelfi, E. A., Jayamaha, B., & Robison, T. (2020). The imperative for the US military to develop a counter-UAS strategy. *NDU Press*. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_4-12_Guelfi-Jayamaha-Robison.pdf?ver=2020-03-31-113800-930

International Civil Aviation Organization. (1944). *Convention on international civil aviation - Doc 7300*. https://www.icao.int/publications/pages/doc7300.aspx

International Civil Aviation Organization. (2011). *ICAO cir 328 unmanned aircraft systems (UAS)*. ICAO. https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf

JARUS. (2019, January 30). *JARUS guidelines on specific operations risk assessment (SORA*). http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v2.0.pdf

Konert, A., & Kasperzyk, P. (2021, October 27). UAS safety operation – Legal issues on reporting UAS incidents. *Journal of Intelligent & Robotic Systems*. https://doi.org/10.1007/s10846-021-01448-5

Kyllo v. United States, 533 U.S. 27 (2001). (2001). https://www.loc.gov/item/usrep533027/

Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021). (2021). https://www.ca4.uscourts.gov/opinions/201495A.P.pdf

Lee, H., Kim, M. U., Kim, Y., Lyu, H., & Yang, H. J. (2020, May 29). Privacy-protection drone patrol system based on face anonymization. *arXiv*. https://arxiv.org/abs/2005.14390

Lee, S. Y., Bates, P. R., & Kille, T. (Eds.). (2019). *Unmanned aerial vehicles in civilian logistics and supply chain management*. IGI Global.

Long Lake Township V. Todd Maxon and Heather Maxon, No. 349230 (Mich. Ct. App. Mar. 18, 2021). (2021). https://law.justia.com/cases/michigan/court-of-appeals-published/2021/349230.html

Mathew, B. (2015). Potential tort liability for personal use of drone aircraft. *St. Mary Law Journal*, *46*, 573. https://libraryguides.missouri.edu/ld.php?_id=37958458

McNeal, G. S. (2015). Government-operated drones and data retention. *Washington and Lee Law Review*, *72*(3), 1139. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4460&context=wlulr

NASA/NUAIR. (2021, May 27). High-density automated vertiport concept of operations. *NASA Technical Reports Server*. https://ntrs.nasa.gov//20210016168

Noack, R. (2021, January 14). In victory for privacy activists, France is banned from using drones to enforce coronavirus rules. *The Washington Post*. https://www.washingtonpost.com/world/in-victory-for-privacy-activists-france-is-banned-from-using-drones-to-enforce-covid-rules/2021/01/14/b384eb40-5658-11eb-acc5-92d2819a1ccb_story.html

NUAIR. (2021, March 24). *NUAIR lays automation groundwork for high-density vertiports*. NUAIR. https://nuair.org/2021/03/24/nuair-lays-automation-groundwork-for-high-density-vertiports/

OECD/ITF. (2020, June 19). Drones in the era of coronavirus. *International Transport Forum.* https://globalmaritimehub.com/wp-content/uploads/2020/07/drones-covid-19.pdf

Office of the Privacy Commissioner of Canada. (2019). *PIPEDA fair information principles*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-

canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Pasztor, A. (2018, March 18). FAA projects fourfold increase in commercial drones by 2022. *The Wall Street Journal*. https://www.wsj.com/articles/faa-projects-fourfold-increase-in-commercial-drones-by-2022-1521407110

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). (2000). Laws.justice.gc.ca. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Pledger, T. G. (2021). The role of drones in future terrorist attacks. *Association of the United States Army*. https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf

Regulation (EU) 2019/947. (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN

Rule, T. A. (2015). Airspace in an age of drones. *Boston University Law Review*, *95*, 155. https://www.bu.edu/bulawreview/files/2015/02/RULE.pdf

Scharaf, R. (2019). Drone invasion: Unmanned aerial vehicles and the right to privacy. *Indiana Law Journal*, *94*(3), 1065-1107. https://www.repository.law.indiana.edu/ilj/vol94/iss3/6/

Seymour, M. (2013). *Eye spy: Art, visibility and global war.* Sydney eScholarship repository. https://ses.library.usyd.edu.au/handle/2123/9667?show=full

Smith, M. L. (2015). Regulating law enforcement's use of drones. *Harvard Journal on Legislation*, *52*(2), 424-453. https://harvardjol.com/wp-content/uploads/sites/17/2015/10/HLL207_crop1.pdf

Tilburg, C. V. (2017). First report of using portable unmanned aircraft systems (drones) for search and rescue. *Wilderness & Environmental Medicine*, *28*(2), 116-118. https://www.wemjournal.org/article/S1080-6032(17)30004-2/fulltext#articleInformation

Torens, C., Nikodem, F., Dauer, J. C., Schirmer, S., & Dittrich, J. S. (2020, May 16). *Geofencing requirements for onboard safe operation monitoring*. ELIB-DLR. https://elib.dlr.de/135054/1/Torens2020_Article_GeofencingRequirementsForOnboa.pdf

United States v. Jones, 565 U.S. 400 (2012). (2012). https://www.loc.gov/item/usrep565400/

US Constitution - Fourth Amendment 1791 | Resources | Constitution Annotated | Congress.gov | Library of Congress. (n.d.). Constitution Annotated. https://constitution.congress.gov/constitution/amendment-4/

WEF Report. (2021, April 5). *Medicine from the sky: Opportunities and lessons from drones in Africa*. https://www.weforum.org/reports/medicine-from-the-sky-opportunities-and-lessons-from-drones-in-africa

Yao, Y., Wang, Y., Xia, H., & Huang, Y. (2017, May). *Privacy mechanisms for drones: Perceptions of drone controllers and bystanders* [CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems]. https://dl.acm.org/doi/10.1145/3025453.3025907

Yu, H., Lim, J., Kim, K., & Lee, S. (2018). *Pinto: Enabling video privacy for commodity IoT cameras*. https://dl.acm.org/doi/10.1145/3243734.324383