P-ISSN: 2790-6795	Annals of Human and Social Sciences	Jan-March 2025,Vol. 6, No. 1
O-ISSN:2790-6809	http://doi.org/10.35484/ahss.2025(6-I)36	[415-428]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards

[1]Hassan Rasheed Siddiqui* and [2]Maria Muniza

1. Aviation law expert, Policy Critic,USA ,LLM University of Bedfordshire UK
2. Resident Editor, South Asia of KT Media Group, Islamabad, Pakistan

Corresponding Author Mariamuniza@gmail.com

ABSTRACT

This study aims to establish a comprehensive regulatory framework addressing privacy, security, and national concerns related to drones equipped with advanced facial recognition technology. As drones become more prevalent in surveillance, logistics, and law enforcement, existing regulations, such as those by the Federal Aviation Administration (FAA), fail to adequately address the privacy and security risks posed by these technologies. Despite the growth of digital privacy laws, aerial surveillance, particularly by drones, remains largely unregulated. This study analyzes current privacy laws, regulatory frameworks, and technological advancements in drone surveillance, focusing on privacy rights, national security, and the risks of cyberattacks. The research finds that current regulations are insufficient, particularly concerning unauthorized drone surveillance and national security risks, especially with foreign-made drones. The study highlights the need for stronger privacy protections, stricter manufacturing standards for foreign drones, and the use of blockchain technology to secure drone data and prevent cyberattacks. Recommendations include strengthening privacy laws for unauthorized drone use, tightening manufacturing standards, integrating blockchain for data security, and developing regulations based on the Fourth Amendment to protect citizens' privacy. Additionally, the study suggests an import ban on Chinese drones to address potential security vulnerabilities. The research calls for immediate regulatory action to safeguard privacy and national security in the face of growing drone capabilities.

Keywords: Drone Surveillance, Facial Recognition, Privacy Laws, FAA Regulations, Foreign-Made Drones

Introduction

The progress seen in drone systems is unprecedented, especially with the utilization of facial recognition and AI capabilities within these devices. But the expansion of drones, particularly those enabled with facial-recognition technology, raises serious issues of privacy, security and regulation. Even with the rising significance of drone technology, existing legal frameworks (i.e., The Federal Aviation Administration (FAA) are still ill-prepared to manage the potential threats they might impose(Nguyen, 2021).

This paper examines these regulatory holes and the ways in which privacy law, Cyber security, and Fourth Amendment-based laws can help to eradicate them altogether. Moreover, we also want to discuss the possibility to protect national security from foreign-made drones, especially from Chinese manufacturers.

While UAV technology and businesses are presently global, it is possible that regulatory frameworks and policy recommendations for these crafts may be significantly different between political jurisdictions. We argue that, in order to develop solutions for the challenges we've experienced with inefficient production, inconvenient border use, and damaging regulatory competition, new varieties of regulatory approaches and international harmonization must be in play. Harmonization may lead to reduction in

trade barriers and alignment of best practices from diverse jurisdictions (Meier, et al., 2022).

Drones are versatile and quick mobile platforms with various potential uses in smart cities, including environmental monitoring, civic security, product delivery, traffic and crowd control, and more. Because of their greater adaptability, they are able to operate in a variety of settings, including some that humans find challenging or even deadly. They can also fly quite close to their objectives, which allows for more targeted operations and more accurate assessments. These characteristics provide advantages when drones are used for smart city applications. In order for smart city residents to have their requirements met, delivery services must be more streamlined and quicker. As a preventative measure, one option is to use drone applications for delivery of packages. Because of its useful features, drones are already finding applications in smart cities, where they record accident scenes, aid first responders, and keep an eye on building sites (Huang, et al., 2021).

These days, you may choose from a wide range of powerful drone systems. On the other hand, thanks to advancements in battery technology, many systems that satisfy the payload, range, and environmental criteria are electrical systems that are lightweight. As an example, a new platform that employs drones for customer cargo delivery has been in the works by Amazon and Walmart. Amazon showcased a 30-minute-long octopus in 2018 that could transport up to 2.3 kg (five pounds) of packages—equal to 86% of Amazon's total deliveries. At the same time, the biggest shipping firm in China and Germany, DHL, has begun testing a fleet of drones that could transport an estimated 500 packages daily. Drones are rapidly becoming an integral part of consumer-focused service delivery (Microdrones 2021). The danger of aerial mishaps, however, increases as the number of drones in operation grows. As a result, traffic safety is reduced and civil aviation's security and infrastructure are jeopardized. Some of the most high-profile incidents with drones have occurred recently (Khan, et al., 2020).

This was the unprecedented time of the use of drones in the form of facial recognition and artificial intelligence (AI) technology which is worrisome and has shaken the ground of Privacy, Security and Regulation. Cameras should also come with a mechanism that allows citizens to opt out from being recorded when they are not engaged in a criminal activity."20 Current statutes do not provide such a protection to all American citizens. Additionally, foreign manufacture of drones, particularly in China, carries increased security risks because of their inferior manufacturing requirements and risk of espionage. The need for a regulatory regime is more than ever crucial not only to address regulatory gaps but also overcome emerging Cyber security threats.

Literature Review

Drone Management Systems

Under the context of this study, an unmanned aerial vehicle, or UAV, is any aircraft that flies without a human pilot, crew, or passengers on board. This class also includes drones. According to Hu and Lanzon (2018) and Sharma et al. (2020), a UAS consists of unmanned aerial vehicles (UAVs), a controller located on the ground, and a connectivity system. There are several methods in which Unmanned Aerial Vehicles (UAVs) may be operated, ranging from completely autonomous (completely devoid of human intervention) to semi-autonomous (with some human oversight) (Kim, et al., 2017).

Because electrical components such as sensors, microprocessors, batteries and navigation systems have become smaller, new types of drones have been developed. The wide variety of drones has been utilized by both civilian and military organizations. Drones are small micro-electromechanical devices like sensors or even robots — at sizes

that can range from large fixed-wing unmanned aerial vehicles (UAVs) to smart dust. The various unmanned aerial systems (UAS), including some on air and satellites and UASs at low and high altitudes are described in (Martinez-Alpiste, et al., 2021).

The FAA has mandated that all operators of small drones, defined as those weighing between 0.55 and 55 pounds, must register their drones. According to FAA rules, all drones must be monitored and controlled like aircraft. These restrictions are classified as follows: I. Operators of model aircraft; (ii) holders of 333 exemptions; (iii) operators serving the public; and (iv) operators serving the public have the option to operate under Part 107. It all depends on your flying style and identity when it comes to obtaining airspace and equipment permission. This method is easier to use and offers more leeway when piloting commercial drones. Beyond that, a "phased-in approach" has been used to include drones into a national airspace system, gradually expanding from low-density to high-density airspace and from rural to urban regions. And there are niche uses for drones in confined spaces, such weather monitoring (Kyriakakis, et al., 2021).

An ever-increasing drone population is causing problems in air traffic control and other areas of aviation, putting pilots and passengers in peril. As a result, routine flights need a special operational feature to ensure their safety and satisfaction. According to Sándor (2019), Sandor put forth UAS traffic management (UTM), which helps with flight completion and overall air traffic management. Using such a system may help maintain order in the traffic flow in the very low-level airspace regions and keep UAVs and conventional aircraft apart. The data that comes into this system allows it to function independently of the Air Traffic Management (ATM) (Jucevičius, et al., 2014).

Drone Surveillance and Privacy Concerns

Drones outfitted with facial recognition technology are being increasingly used in industries ranging from law enforcement to border security to urban planning, causing a good deal of controversy related to privacy. These drones can autonomously identify and track people, sometimes without consent, fuelling fears of mass surveillance and civil liberties violations. For instance, surveillance drones in cities like Los Angeles and New York City are being used to keep an eye on public spaces, raising concerns about the transparency of data collection and storage. A 2020 report by the Electronic Frontier Foundation (EFF) indicated that such technology has a disproportionate impact on marginalized communities and threatens to empower unchecked government overreach. Current practices could infringe on fourth amendment protections, as the legal backdrop has yet to designate aerial surveillance as an unconstitutional search (Nguyen, et al., 2020).

Regulatory Gaps and Legal Challenges

Despite these concerns, drone regulations remain piecemeal and outdated. The United States' Federal Aviation Administration (FAA) doesn't have much time to worry about privacy and cyber security, focusing instead on making sure only the safest aircraft can use the airspace. These landmark rulings, including Carpenter v. United States (2018), are not yet in effect, leaving a legal gap with respect to drone surveillance. These rulings extended the Fourth Amendment protections to digital data. Further complicating efforts to hold companies accountable worldwide are different standards — for example, the EU's strict GDPR regulations versus a less strict law in a country. The absence of progress on this front highlights the urgency of new laws governing the collection, storage, and use of data by drones (MohdDaud, et al., 2022).

National Security Risks of Foreign-Made Drones

Adding to these problems are national security risks linked to foreign-manufactured drones, especially those from Chinese companies like DJI. Bower (2021)

identified weaknesses including firmware backdoors and insecure data channels that could enable foreign powers to compromise sensitive data. In 2020, the U.S. Department of Defense prohibited the use of DJI drones amid concerns about data leaking to China, and Customs and Border Protection said there had been unauthorized transmissions of data. These peril is acute in crucial sectors like protection, the place drones monitor navy bases and energy grids. While legislation such as the American Security Drone Act seeks to reduce dependency on foreign technology, private-sector uptake of domestic substitutes has been slow (Mohamed et al., 2020).

While UAVs do have some utility, they also pose numerous challenges for society, including effects on human rights, sustainability, security, and social equity. Your data will be better because privacy and security have been extensively researched and there are systematic, high-level policies available. Concerning safety, UAVs do not usually have a pilot on board and their communication connection with the ground controller isn't always reliable. Consequently, there is an increasing likelihood of catastrophes like as crashes and collisions with commercial jets. The primary concern with commercial drone flying over public places, as stated by Rao et al., is the possibility for mishaps that might harm people, their health, and their property. There is an increased likelihood of accidents with micro or small UAVs since their hardware and software are of inferior quality. Moreover, UAV operators frequently fly them for extended durations that can lead to operator fatigue (Khan, et al., 2018).

Block chain as a Cyber security Solution

In order to tackle such challenges, Block chain technology has evolved as a viable candidate to secure the drone networks. Research, like this one done by Zhang et al. (2021) detailed Block chain frameworks that facilitate communication encryption, data tampering prevention, and drone usage tracking in real time. IBM, for example, has tested Block chain systems for managing urban drone traffic, and startups like DroneSec use decentralized ledgers to verify operators and identify malicious activity. But scalability and energy consumption issues continue to be a barrier. Stakeholders can increase data integrity and reduce cyber threats through the integration of Block chain, and improve public confidence in drone technologies. The combination of invasive surveillance, regulatory gaps, and foreign made drone threats calls for broad overhauls. Privacy is already governed by laws, but we can fill the legal gaps left in these efforts by enacting laws governing online privacy and we can use Block chain to strike a balance between innovation and ethical/security policy demands (Park, et al. 2018).

Material and Methods

In response to the research questions developed for this study, we took a holistic joined-up interdisciplinary approach, combining legal analysis, technology assessment and policy evaluation. This helped to do an extensive research about regulatory prospects of drone surveillance and issues of privacy and national security (Hassanalian, &Abdelkefi, 2017).

The methodology consisted of three key components:

Legal Analysis

In the first part of the methodology, we conducted a detailed legal analysis to determine the existing gaps in the legal frameworks that govern this area of drone surveillance. This included a close analysis of Federal Aviation Administration (FAA) rules governing drone operations in large-scale airspace but which fail to address key concerns identified with drone use for surveillance. Beyond the technical aspects of the laws, we delved into key judicial precedents—specifically, the Carpenter v. United States (2018)

case that is a cornerstone for better understanding how digital privacy law is evolving as a result of emerging surveillance technologies. Through their review of these legal frameworks and case law, the study aimed to identify the gaps in existing laws that do not adequately regulate drone surveillance, particularly in terms of facial recognition technology and the Fourth Amendment (Finn, & Wright, 2016).

Technology Assessment

The second pillar of the methodology consisted of an extensive technology assessment, specifically targeting the current abilities of drones equipped with facial recognition and AI-enhanced surveillance systems. The assessment mapped out the technological advances that render [drones] such potent surveillance tools. It also included a review of the vulnerabilities posed by foreign-made drones, particularly those produced by companies based in countries with weaker Cyber security laws, like China. The study examined these technological capabilities and their potential to be misused for unauthorized surveillance and the consequences of incorporating these technologies into public and private sectors (Hildmann, & Kovacs, 2019).

Policy Evaluation

The third part of the analysis consists of reviewing the current laws in the US and comparing the legal frameworks to the international legal landscape on privacy. Such a comparative policy evaluation sought to identify the optimal regulatory measures between the competing priorities of privacy, security and technology drive. The study conducted a comparative analysis to summarize the strengths and weaknesses of these regulatory approaches and aimed at deriving practical recommendations for a more inclusive regulatory framework that can be implemented worldwide. This doctrinal focus was designed to ensure that such policies would mitigate privacy and security risks if pursued, while supporting the responsible use of drone technology in service of national security goals. In this research, a three-way approach was adopted to cover the issues with drone surveillance and the next steps required to close existing regulatory gaps (Ghasri, &Maghrebi, 2021).

Results and Discussion

Privacy Protections and Legal Gaps

The study found glaring deficiencies between drone surveillance and the laws that govern it, particularly regarding privacy. The Federal Aviation Administration (FAA) has long established rules regarding how drones can be operated within the airspace, but it said little about its own issues in operating drones used for surveillance or monitoring. Environmental policy is also based on the necropant in the905 we9738/906 standing73153491902 drone901 in901 in537 ml. Current laws on privacy, especially those that concern digital privacy, are old and do not consider new technological advancements such as facial recognition and AI-based surveillance systems. It falls under this issue is that there is a lack of formal regulation in this area, leaving no clear legal structure to delineate what is and is not permissible in the use of drones for public area surveillance, resulting in earnest concern for[citizens] of violating their rights and lack of surveillance checking. There is thus an urgent need for updated and comprehensive privacy legislation that considers the intricacies of these emerging technologies (Barmpounakis, et al., 2016).

National Security Risks of Foreign-Made Drones

We detected serious national security risks with foreign-made drones, such as those manufactured in China. These counter-unmanned systems are commonly

manufactured under looser regulatory requirements and oversight that raises the odds that they design has a vulnerability that can be used for espionage or data theft. Drones manufactured in foreign countries securely transmit data back to those countries, thereby providing a security risk to the nation. These drones do not have stringent manufacturing standards, meaning sensitive information can be intercepted or manipulated, which is a major area for cyber espionage. Also, the risk that these probes will be used for purposes other than as advertized, including surveillance of critical points and acquiring sensitive intelligence, amplifies those threats. Therefore, it is vital to establish more stringent standards on the production and importation of these vehicles when it comes to foreign states that pose national security risks (Fedorko, et al., 2018).

Block chain as a Cyber security Solution

The Emergence of Block chain Technology to Mitigate Cyber security Threats in Drone Surveillance System Using Block chain allows drones to send and store data within a decentralized, tamper-proof network to protect sensitive data integrity and security. The transparent and secure nature of block chain could protect sensitive information collected by drones against unauthorized access, thus mitigating the risk of such attacks and data breaches. Knowing that information can secure the collected data and ensure legitimacy. It could also allow the drones and the people managing them to communicate securely, which would only boost the security of drone-based surveillance. Hence, the application of Block chain technology provides a potential response to the threats of drone information infiltration and unauthorized monitoring (Clarke, & Bennett Moses, 2014).

The Need for Fourth Amendment-Based Regulations

According to the legal analysis, the new regulation should contain Fourth Amendment protections to ensure the privacy rights of citizens. While the Fourth Amendment protects us from being unreasonably searched and seized, existing regulations fall short in addressing the privacy concerns associated with drone surveillance. In high-density urban environments, drones outfitted with facial recognition and AI systems represent a specific threat to this constitutional right, which ensures that individuals are not subject to worthy consequences without knowledge or consent. The study found that the existing regulations do not guarantee that drones are used in manner that does not infringe on citizens' privacy rights, particularly within public spaces where the risk of mass surveillance is significant. It is a matter of creating a new legal framework to govern their use, enshrining Fourth Amendment principles in surveillance law by regulating use of drones just as we have regulated the use of airplanes for surveillance. These types of regulations would help ensure drone surveillance tools are only being used with appropriate legal oversight in place, including requiring warrants under certain circumstances to protect individuals' privacy in the face of increasingly ubiquitous surveillance technologies (Comtet, & Johannessen, 2021).

Current regulations on UAVs

United States

In the United States, federal laws on unmanned aerial vehicles (UAVs) are still in their infancy. Unmanned Aerial Vehicles were formally designated as "aircraft" in a 2014 lawsuit (FAA v. Pirker) by federal courts. The FAA predicted that more than seven thousand companies will have access to drones within three years after announcing in 2015 that companies may apply for permission to operate unmanned aerial vehicles (UAVs). In 2015, commercial drones could only be flown during the day if they did not exceed certain weight and speed limits. These limits were 100 mph, 0.55 lbs (250 g), and 500 ft. Drone operators have to meet certain requirements, including being at least 17 years old, passing exams, and having a certificate. Notably, the regulations stipulated that

operators must have direct visual contact with drones and that they cannot be used for delivery purposes. Later that year, the FAA announced that drones weighing more than 0.55 kilograms on takeoff, containing all accessories, were needed to be registered. Deploying Small unmanned aircraft Over People: The FAA's Final Rule was Released in December 2020. This rule categorizes UAVs into four new groups according to weight and potential harm they can cause. Nighttime flight with frequent online training is also allowed (Dung, &Rohacs, 2018).

When thinking about safety, these new developments were paramount. With the introduction of remote identification, a major change happened: UAVs can now provide "recognition, location, and performance data that people on earth and other aircraft users can receive." Keeping unmanned aerial vehicles (UAVs) within sight range in the absence of Remote ID technology is another step toward making them safer. Take the United States as an example. Drones used for commercial purposes are required to stay below 0.55 lbs (including payload) and must surrender to human aircraft. On the other hand, drones operated for leisure purposes are exempt from this restriction and must never fly in close proximity to other aircraft. Addressing safety problems is the primary goal of most of these legislation. In addition, business operators must be certified, and recreational UAS users must register their vehicles and conduct safety exams (Hiebert, et al., 2020).

At the federal level, however, there are no privacy rules that deal specifically with the issues that UAVs bring to human privacy. This regulation does not address "privacy issues," as the FAA said in the Final regulation. Some state governments are addressing the issue of privacy, and there are additional rules and regulations that drone operators must follow. For instance, according to Chen and Huang (2021), certain states have made it a misdemeanor to use unmanned aerial vehicles (UAVs) to invade someone's privacy. One such state is Tennessee, which has a thriving music and concert industry. Another example is California, which in 2019 amended Assembly Bill No. 1129 to make it a misdemeanor to do so.

The E.U

Two EU bodies that are very involved in UAVs are the European Commission and the European Aviation Safety Agency. The first legislation to tackle the subject of regulating unmanned aerial vehicles (UAVs) was "control NO 216/2009 on Common Standards in the Department of Civil Aviation and Established a European Safety Aviation Agency" issued in 2008. Midway through the 2010s, however, was when the topic of regulation began to get more attention. Concerning unmanned aerial vehicle (UAV) safety, privacy, and data security, the European Commission released a statement in 2014 highlighting these issues. In addition to acknowledging the need to establish a risk-based framework for drone regulation, the 2015 European Union Aviation Strategy addressed concerns around confidentiality, information security, liability, insurance, and the environment.

The European Safety in Aviation Agency is another group that has addressed policies regarding unmanned aerial vehicles. For the purpose of "to improve the uniformity of drone operations across Europe" and "to boost the cost-effectiveness for drone managers, manufacturers and responsible authorities," the agency published an opinion paper in February 2019. There is no distinction between recreational and business-related drones in this new UAV regulation, with the exception of insurance requirements. Commercial drone operators, often called air carriers or aircraft operators, are required by law to have insurance (Bohloul, 2020).

There are three classifications for unmanned aerial vehicles (UAVs): open (low risk flights), specialized (mid risk), and certified (high risk, bigger size, or hazardous payload). The size, weight, and nature of the cargo determine the classification. Dangerous products,

like explosives, gasses, combustible liquids or solids, and so on, fall into certain categories. Subcategories further subdivide the general and particular categories into subsets defined by size and weight (Hu, &Lanzon, 2018).

In the regulation, there is a provision for safety. The restriction about flying ranges is the most notable. The open category prohibits UAVs from flying higher than 120 meters; the defined category allows them to fly higher; and the certified category requires specific permission. Training, in the form of certification or self-practicum, is required for all three categories of operators with the exception of those weighing less than 250 g. Also, for privacy reasons, UAVs that include sensors that might invade someone's privacy need to be registered. According to Aurambout et al. (2019), member states are also obligated to create registration systems for UAVs and maintain records of both UAV operators and manufacturers.

Again, there are no privacy-related regulations or papers outlining best practices for UAVs. European Union member states have instead been required to implement the General Data Protection Regulation (GDPR) as of 2015 [63]. While unmanned aerial vehicles (UAVs) aren't specifically addressed in the legislation, it does lay out a comprehensive framework for handling data subjects' rights and the transmission of personal information to third parties, as well as for protecting privacy throughout the digitization process. Regarding the General Data Protection Regulation (GDPR), it is up to the individual member states to devise policies and regulation frameworks that adhere to the GDPR but are suitable for their local situations. Unmanned Aerial Vehicle (UAV) privacy is also addressed in another EU legislation. Recognizing the significance of "public security or protection of privacy and personal data," Section VII of the European Union Regulation 2018/1139 addresses unmanned aircraft (Bailon-Ruiz, &Lacroix, 2020).

Germany

Germany must comply with the new regulations imposed by the European Aviation Safety Agency (EU 2019/947) as it is a member of the European Union. The federal government has also enacted certain additional country-specific regulations. Germany coined two words to describe unmanned aerial vehicles: flying models, which describe drones used for fun, and unmanned aviation systems, which describe drones used for business. In 2022, the government document pertaining to UAV laws suggests a gradual transition towards the EU2019/947, and the Luftverkehrsgesetz has been in place since April 2017. According to Ayamga et al. (2021), drone operators were authorized to operate their devices in the open category until December 2022 thanks to a national exemption.

Various safety-related rules exist in Germany. Stickers with the owner's name and address are required on any unmanned aerial vehicles (UAVs) having a weight over 0.25 kg in order to facilitate certification and identification processes. Proof of expertise is necessary for unmanned aerial vehicles (UAVs) with a weight exceeding 2 kg. Under the supervision of the Federal Supervisory Authority for Air Navigation Services (BAF), authorization to operate unmanned aerial vehicles (UAVs) at night or with a payload more than 5 kg is required. Germany stands up for recognizing the potential societal impacts of unmanned aerial vehicles (UAVs) on issues like airplane noise and environmental protection. A geospatial interactive drone map has also been produced in Germany to indicate where drones may be flown. Additionally, the nation plans to include extra safety features, such web apps, a route planner, and meteorological data for drone users, by the end of 2022. Concerning the operating of UAVs, the regulations address both safety and privacy concerns. Any unmanned aerial vehicle (UAV) capable of receiving, transmitting, or recording visual, auditory, or radio signals, or weighing more over 0.25 kg, is prohibited from flying above private residences (Ayamga, et al., 2021).

Japan

Drones and other unmanned aerial vehicles are overseen by Japan's Ministry of Land, Culture, Sports, and Tourism. Anyone flying unmanned aerial vehicles (UAVs) must have the proper authorization, under a 2015 change to the Aeronautical Act. It also forbade UAVs from operating in or near airports, airspace at or above 150 m, and heavily populated regions. Nighttime flights, flights beyond visual range, transporting dangerous items, and object dumping were all considered forbidden uses. Additional regulations were put in place in September 2019. These included bans on flying in a way that might cause crashes, flying under the influence of drugs or alcohol, and operating UAVs in a negligent or dangerous manner. In June 2022, a new regulation was put into effect that lowered the minimum weight restriction from 200 g to 100 g and mandated the registration of any drones weighing more than 100 g. It is possible to levy a punishment of 500,000 yen (about $4,500 USD) on anybody caught flying a UAV in an area that is off-limits or heavily inhabited. Operators of unmanned aerial vehicles (UAVs) face fines of up to 300,000 yen (about $2700 USD) or jail terms of up to one year if caught operating UAVs while under the influence of drugs or alcohol or failing to take any preflight procedures. Privacy concerns about unmanned aerial vehicles (UAVs) are often ignored, similar to the United States but different from Germany and the Netherlands. Rules and public communication governing UAV operation are set by the Civil Aviation Bureau, which is a branch of the Ministry of Land, Infrastructure, Transportation and Tourism. However, privacy is not addressed in any way (Albino, et al., 2015).

Conclusion

Drone technology, with its potential integration of facial recognition and AI-driven surveillance, has evolved at an unprecedented rate, creating a liability for privacy, security, and regulatory frameworks. These technologies facilitate the ability of drones to gather massive amounts of sensitive data and be essentially able to surveil in real time with unprecedented accuracy. This mode of communication is assumed by those that have an ever-increasing familiarity with drone technology. We research areas where current laws and regulations are ill-equipped to mitigate the novel risks of these emerging technologies. Existing regulations, including those in place by the Federal Aviation Administration (FAA), are mostly concerned with operational safety in airspace and lack the legal protections or guidelines for drones used in surveillance, especially ones that are enabled with advanced technologies including facial recognition and AI. Additionally, the privacy laws that were formed prior to this technology are out-of-date and incapable of protecting the rights of individuals. Although judicial decisions like Carpenter v. United States (2018) have helped create some borders in the landscape of digital privacy, they do not take account of the potential for drone surveillance to operate continuously and broadly.

Another key point our research highlights is what a security risk foreign-made drones, particularly the types made by Chinese companies, represent in terms of national security. The lax regulations attached to the imported drones represent a major weakness in national security. Some of these drones may have backdoor access or other vulnerabilities that make it easier for foreign governments or malicious actors to use the data collected through surveillance. The free flow and importation of these drones is a recipe for espionage, cyber attacks and abuse of sensitive data. These national security risks are compounded by the lack of clear standards and oversight as to the manufacturing, cybersecurity, and data management of foreign-produced drones. In view of these gaps, the research emphasizes allowing and achieving a comprehensive regulatory framework that not only addresses the issues pertaining to privacy, Cyber security and national security, but also makes sure not to throttle technological innovation in the drone industry. This framework would be completed by a modernization of privacy laws, stronger restrictions on foreign-made drones, and a clear and strong legal infrastructure

defending citizens from unauthorized surveillance and unauthorized data breaches. Until such reforms are implemented, the proliferation of drone use with advanced surveillance technologies may result in a mass breach of privacy and potentially be a grave security threat to the nation.

Recommendations

The results of this study have implications for several much-needed reforms in regulatory frameworks governing drone surveillance, which we outline here. These recommendations are designed to protect privacy, strengthen national security, and ensure the responsible use of drone technology while reducing its potential negative consequences.

Strengthen Privacy Laws

The first recommendation is to update and strengthen existing privacy laws so they can account for drone surveillance. New technologies such as facial recognition or AI are being integrated into drones while existing privacy laws have been unable to keep up. The rules should develop a comprehensive legislation addressing rules on which neighborhoods these are trained on. These general basic privacy laws need to control how drones can collect personal data, provide information on the usage of drones and restrain the purposes of surveillance in private space using drones. Such updates are vital to safeguarding individuals' privacy rights in an age of ever greater reach of surveillance technologies.

Establish Stricter Manufacturing Standards

To address national security concerns, the federal government must impose stringent manufacturing requirements on drones, particularly those made internationally (such as in China). Drone manufacturers, and the commercial and governmental entities that use the technology, should establish Cyber standards that will ensure that rich data from drones are not compromised, and that sensitive information collected in the fly zone is encrypted correctly. Developing strict manufacturing standards would allow the U.S. to guarantee that all drones, domestically produced or imported, operating on American soil, meet high security standards. Reducing the risks associated with the use of foreign-made drones, which could potentially be hacked and used for espionage or other malicious purposes.

Implement Block chain for Data Security

Integrate Block chain technology into the drone system to secure the data collected by the drone. Blockchain can offer a decentralized, transparent, and tamper-proof way of storing and transmitting data, which will ensure the sensitivity of information collected by the drone is safe from unauthorized access and refusal to alter. Implementing smart contracts in Block chain prevents cyber attacks and data breaches, ensuring the integrity and privacy of data collected through drone surveillance. As a result, it can address and help reduce concerns about misuse or illegal use of drones by ensuring that drone usage is completely transparent and auditable witch Block chain.

Develop Fourth Amendment-Based Regulations

The proliferation of drones has raised serious issues of potential intrusion on individuals' privacy and Fourth Amendment protections.407 As technology advances, so too must regulations that define the permissible use of drones that potentially captures a person's private, yet publicly, livable space. These types of regulations should mandate that law enforcement agencies and other government entities acquire appropriate

warrants to use drones to surveil private spaces or for lengthy periods of time. Moreover, specifying in what situations drones may be used for surveillance would help prevent any potential infringement on constitutional protection from unwarranted searches and seizures. These regulations would create a legal structure for drones that balances individuals' privacy with allowing law enforcement to use drones to pursue their legitimate goals.

Enforce Import Bans on Risky Drone Manufacturers

Lastly, with the national security risks associated with foreign-made drones, specifically those made by companies located in countries with dubious security practices, the U.S. government should be open to instituting import bans on such drones. The U.S. should not sell drones manufactured by companies that have well-documented links to foreign governments that are active in cyber espionage or other forms of surveillance. This would greatly minimize the risk of data breaches, espionage, and unauthorized surveillance activities. Targeted enforcement of the import ban will help the United States protect its national security in the form of forward-looking drone innovation while ensuring that drones used by entities inside its borders won't read sensitive data or pose a threat to its citizens. Until then, however, we have seen how surveillance drones raise a whole host of regulatory gaps and security concerns, and these recommendations together put us on a better path to making these important devices safer for the public. It is possible to balance the advantages of drone technology with the need to protect privacy, national security and civil liberties through stronger privacy legislations, stiffer manufacturing standards, implementation of Block chain technology and Fourth Amendment-based regulations as well as the implementation of import bans on risky drone manufacturers.

References

Albino, V., Berardi, U., &Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology, 22*, 3–21. https://doi.org/10.1080/10630732.2015.1017103

Aurambout, J.-P., Gkoumas, K., &Ciuffo, B. (2019). Last mile delivery by drones: An estimation of viable market potential and access to citizens across European cities. *European Transport Research Review, 11*, 30. https://doi.org/10.1186/s12544-019-0389-x

Ayamga, M., Akaba, S., &Nyaaba, A. A. (2021). Multifaceted applicability of drones: A review. *Technological Forecasting and Social Change, 167*, 120677. https://doi.org/10.1016/j.techfore.2021.120677

Bailon-Ruiz, R., &Lacroix, S. (2020). Wildfire remote sensing with UAVs: A review from the autonomy point of view. In *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*, Athens, Greece, September 1–4; pp. 412–420. https://doi.org/10.1109/ICUAS49001.2020.9203073

Barmpounakis, E. N., Vlahogianni, E. I., &Golias, J. C. (2016). Unmanned aerial aircraft systems for transportation engineering: Current practice and future challenges. *International Journal of Transportation Science and Technology, 5*, 111–122. https://doi.org/10.1016/j.ijtst.2016.05.004

Bohloul, S. M. (2020). Smart cities: A survey on new developments, trends, and opportunities. *Journal of Industrial Integration and Management, 5*, 311–326. https://doi.org/10.1142/S242486222050012X

Chen, Y.-C., & Huang, C. (2021). Smart data-driven policy on unmanned aircraft systems (UAS): Analysis of drone users in U.S. cities. *Smart Cities, 4*, 78–92. https://doi.org/10.3390/smartcities4010005

Clarke, R., & Bennett Moses, L. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Review, 30*, 263–285. https://doi.org/10.1016/j.clsr.2014.03.007

Comtet, H. E., &Johannessen, K.-A. (2021). The moderating role of pro-innovative leadership and gender as an enabler for future drone transports in healthcare systems. *International Journal of Environmental Research and Public Health, 18*, 2637. https://doi.org/10.3390/ijerph18052637

Dung, N. D., &Rohacs, J. (2018). The drone-following models in smart cities. In *2018 IEEE 59th Annual International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, Riga, Latvia, November 12–13; Piscataway: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/RTUCON.2018.8659418

Fedorko, G., Žofčinová, V., &Molnár, V. (2018). Legal aspects concerning use of drones in the conditions of the Slovak Republic within the sphere of intra-logistics. *PeriodicaPolytechnica Transportation Engineering, 46*, 179–184. https://doi.org/10.3311/PPte.10353

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Security Review, 32*, 577–586. https://doi.org/10.1016/j.clsr.2016.04.008

Ghasri, M., &Maghrebi, M. (2021). Factors affecting unmanned aerial vehicles' safety: A post-occurrence exploratory data analysis of drones' accidents and incidents in Australia. *Safety Science, 139*, 105273. https://doi.org/10.1016/j.ssci.2021.105273

Hassanalian, M., &Abdelkefi, A. (2017). Classifications, applications, and design challenges of drones: A review. *Progress in Aerospace Sciences, 91*, 99–131. https://doi.org/10.1016/j.paerosci.2017.04.003

Hiebert, B., Nouvet, E., Jeyabalan, V., &Donelle, L. (2020). The application of drones in healthcare and health-related services in North America: A scoping review. *Drones, 4*, 30. https://doi.org/10.3390/drones4020030

Hildmann, H., & Kovacs, E. (2019). Review: Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety. *Drones, 3*, 59. https://doi.org/10.3390/drones3040059

Hu, J., &Lanzon, A. (2018). An innovative tri-rotor drone and associated distributed aerial drone swarm control. *Robotics and Autonomous Systems, 103*, 162–174. https://doi.org/10.1016/j.robot.2017.12.019

Huang, C., Chen, Y.-C., & Harris, J. (2021). Regulatory compliance and socio-demographic analyses of civil unmanned aircraft systems users. *Technology in Society, 65*, 101578. https://doi.org/10.1016/j.techsoc.2021.101578

Jansen, P. (2015). *An ethical evaluation of the use of surveillance-capable unmanned aerial systems in civil contexts*. University of Twente. Available online: https://essay.utwente.nl/69031/1/Jansen_MA_Behavioural%2C_Management_and_Social_Sciences.pdf. Accessed on 5 May 2022.

Jucevičius, R., Patašienė, I., &Patašius, M. (2014). Digital dimension of smart city: Critical analysis. *Procedia-Social and Behavioral Sciences, 156*, 146–150. https://doi.org/10.1016/j.sbspro.2014.11.147

Khan, M. A., Alvi, B. A., Safi, E. A., & Khan, I. U. (2018). Drones for good in smart cities: A review. In *International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC)*, Vaniyambadi, India, January 28–29.

Khan, N. A., Jhanjhi, N. Z., Brohi, S. N., Usmani, R. S. A., &Nayyar, A. (2020). Smart traffic monitoring system using unmanned aerial vehicles (UAVs). *Computer Communications, 157*, 434–443. https://doi.org/10.1016/j.comcom.2020.04.019

Kim, S. J., Lim, G. J., Cho, J., &Côté, M. J. (2017). Drone-aided healthcare services for patients with chronic diseases in rural areas. *Journal of Intelligent & Robotic Systems, 88*, 163–180. https://doi.org/10.1007/s10846-017-0600-0

Kyriakakis, N. A., Marinaki, M., Matsatsinis, N., &Marinakis, Y. (2021). Moving peak drone search problem: An online multi-swarm intelligence approach for UAV search operations. *Swarm and Evolutionary Computation, 66*, 100956. https://doi.org/10.1016/j.swevo.2021.100956

Martinez-Alpiste, I., Golcarenarenji, G., Wang, Q., &Alcaraz-Calero, J. M. (2021). Search and rescue operation using UAVs: A case study. *Expert Systems with Applications, 178*, 114937. https://doi.org/10.1016/j.eswa.2021.114937

Meier, K., Hann, R., Skaloud, J., &Garreau, A. (2022). Wind estimation with multirotor UAVs. *Atmosphere, 13*, 551. https://doi.org/10.3390/atmos13040551

Mohamed, N., Al-Jaroodi, J., Jawhar, I., Idries, A., & Mohammed, F. (2020). Unmanned aerial vehicles applications in future smart cities. *Technological Forecasting and Social Change, 153*, 119293. https://doi.org/10.1016/j.techfore.2020.119293

MohdDaud, S. M. S., Yusof, M. Y., Heo, C. C., Khoo, L. S., Singh, M. K. C., Mahmood, M. S., &Nawawi, H. (2022). Applications of drone in disaster management: A scoping review. *Science & Justice, 62*, 30–42. https://doi.org/10.1016/j.scijus.2021.10.006

Nguyen, D. D., Rohács, J., Rohács, D., &Boros, A. (2020). Intelligent total transportation management system for future smart cities. *Applied Sciences, 10*, 8933. https://doi.org/10.3390/app10308933

Nguyen, D.-D. (2021). Cloud-based drone management system in smart cities. In R. Krishnamurthi, A. Nayyar, & A. E. Hassanien (Eds.), *Development and future of Internet of Drones (IoD): Insights, trends and road ahead* (pp. 211–230). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-59979-2_14

Park, S.-Y., Shin, C. S., Jeong, D., & Lee, H. (2018). DroneNetX: Network reconstruction through connectivity probing and relay deployment by multiple UAVs in ad hoc networks. *IEEE Transactions on Vehicular Technology, 67*, 11192–11207. https://doi.org/10.1109/TVT.2018.2837647