Vol.16No.2(2025):44-59
DOI:https://doi.org/10.61841/turcomat.v16i2.15268

EYES IN THE SKY: STRENGTHENING PUBLIC AWARENESS AND LAW ENFORCEMENT RESPONSE TO DRONE-DRIVEN INFRINGEMENTS ON PRIVACY RIGHTS IN THE UNITED STATES

Ata ul Moeed Hashmi
Aviation /Corporate Lawyer, Educator,
LLM, University Of Bedfordshire UK

ABSTRACT

The rapid proliferation of drones in the United States has created urgent challenges concerning individual privacy, institutional readiness, and legal enforcement. While drones serve diverse functions, their use in surveilling private spaces without consent has exposed significant regulatory gaps in both federal and local legal frameworks. This research investigates these gaps by analyzing a real-life case from Silicon Valley, where a civilian encountered a drone hovering above their private residence and was unable to obtain meaningful assistance from law enforcement.Drawing on recent scholarship, including Siddiqui and Muniza's "Regulatory Gaps in Drone Surveillance" [Annals of Human and Social Sciences, 2025] and "The Drone's Gaze: Religious Perspectives on Privacy and Human Dignity" [Al-Qamar, 2024], this paper reveals how current laws fail to protect against aerial intrusions, especially in residential zones. The findings are further contextualized within broader institutional weaknesses, as previously identified in "Public Funds, Private Gains" [JARSSH, 2022] and "Hybrid Warfare and the Global Threat of Data Surveillance" [PSSR, 2025].Moreover, the paper critiques recent legislative efforts, such as the U.S. Countering CCP Drones Act (H.R.2864), through the lens of Siddiqui and Muniza's (2025) analysis published in the Social Sciences & Humanity Research Review, and assesses their ineffectiveness against AI-powered foreign-manufactured surveillance drones. Philosophical and constitutional dimensions are explored through works like "Liberalism in South Asia" [CIBGP, 2008], and "Constitutional Vulnerability in the Age of Digital Surveillance" [CRLSJ, 2025]

The research proposes a three-pronged regulatory framework:

1. Modernization of legal statutes to close regulatory and constitutional loopholes;
2. Institutional upskilling through integrated AI-based geofencing and centralized FAA-DHS-local reporting platforms;
3. Public empowerment via education, civic engagement, and participatory complaint channels.

The paper concludes that safeguarding privacy and national security in the drone era requires an interdisciplinary approach—bridging law, technology, ethics, and public participation. Only through such coordinated efforts can drone innovation be directed toward public benefit without compromising civil liberties.

Introduction

Lately, using drones and other devices made in foreign countries that use artificial intelligence has greatly impacted national security and the civil liberties of Americans. Due to technologies that are often developed in China and Russia, there are tough challenges for cybersecurity, data privacy, and control by authorities. More use of unmanned aerial vehicles (UAVs) has led officials to question how data is handled and whether it belongs to the government or private sector.

The U.S. Department of Commerce is discussing new rules because of concerns about espionage that could result from too many Chinese and Russian drones. The worry is that drones made outside the U.S. may be programmed or accessed remotely to collect important American data and so could threaten the country's security (Siddiqui & Muniza, 2024). Such problems are made worse by advancements in AI that can easily record someone's face, track their routines, and save their location records on the internet with possible links to overseas servers. So, lawmakers have suggested introducing rules that would lessen the country's dependence on insecure technology in important areas.

Still, some challenges have emerged regarding key points in this legislation. Experts in the field say that prohibiting drones could lead to financial problems, mainly for sectors that depend on them a lot. For precision agriculture, inspecting structures, and emergency situations, drones are now vital tools for up-to-date data and boosting operations. Taking away cheap foreign choices can reduce how much we can develop new things, restrict access to them, and mostly hurt smaller businesses and public service agencies .

Specialists and researchers have pointed out that the clash between national security and revenue on one hand and the way the economy relies on trade highlights important issues in the regulation structure today. Hassan Rasheed Siddiqui points out that the U.S. has not created enough up-to-date laws for UAVs, mostly when used together with AI. He points out that because the rules for aviation and surveillance are old, there are opportunities through which foreign-built systems can be used without much supervision. Experts insist it is essential to revise the frameworks to address the relationship among cybersecurity engineering, having control over technology, and privacy protection.

This research uses similar ideas to look at how drone surveillance impacts the U.S., addressing three linked issues: weak rules and regulations for UAV use, little awareness by the public about their rights, and inadequate preparation among law enforcement agencies. Analysis of a specific case and review of policies hope to introduce solutions that support data privacy, encourage ethical development, and enhance efforts to manage changes caused by drones.

Purpose of the study

Market Vacuum Created by the Ban on Chinese and Russian Drones

The ban on Chinese and Russian drones in the U.S. has left a huge space for other drone manufacturers to take over. Some Chinese businesses, key among them DJI, have seized the drone industry because their drones are relatively inexpensive, advanced, and go well beyond the military

sphere. Even now, domestic manufacturers have yet to make and sell enough products to replace those sold by the companies previously in the U.S. market (Siddiqui & Muniza, 2024). This shortage affects the regular operations of agriculture, firefighting, and urban planning, as those areas have counted on UAVs a lot. Lacking prompt and cheap alternatives, crucial services could get delayed, become less productive, and cost more money.

Impact of Price Competition and Availability of Alternatives

Chinese drones are leading in the U.S. market because they charge less than similar products made at home. As a result of the bans, Americans have to pick between solutions that are more costly locally or ones provided by unknown brands, most of which are not as well prepared for logistics and technological needs as the brands that are banned. Because of this, the jobs and incomes of people are disrupted and the costs for both local governments and small companies rise. As an example, emergency organizations with limited funds often find it hard to keep up their levels of surveillance and operations. Besides, the scarcity of less costly products may stop some organizations from competing and delay the development of new drone technology in these sectors.

Technical Vulnerabilities of AI-Enabled Surveillance Systems in Foreign-Manufactured Drones

Most foreign-produced drones connected to AI are sold with software that is hard to read and the way data is sent is not discussed. Among their abilities, these drones can gather biometric info, take video shots, and record locations. Without realizing it, the operator could send all collected data to foreign remote servers (Siddiqui, 2025). Facial recognition, behavior analysis, and predictive tracking are some of the extra services that AI adds to surveillance by drones. They alert that such drones could be used for normal activities as well as for spying or obtaining personal information in large quantities. The risk is further increased since drone technology has changed faster than the country's current security and law standards.

Feasibility of Implementing Security Measures While Ensuring Industry Stability

It is very important to use real-time data encryption, geofencing, or put in place laws that require data processing within a country's borders to protect national interests. Nonetheless, making these security regulations effective while ensuring the industry's stability is still a hard issue to solve. Most operators that rely on small or medium drones struggle to use cybersecurity systems or switch to domestically manufactured models. Also, strict enforcement of new standards may stop people from introducing new ideas or acting in the market. Policy makers need to keep technological security from becoming an obstacle for businesses that do not have great resources or for new developments in arenas that matter.

Policy Alternatives to Address Cybersecurity Risks and Economic Concerns

It is necessary to bring several policymaking strategies together to face these various issues. One option could involve making a national policy that certifies drones by checking where they were made, the security of their software, and how they handle important information. Subsidies, R&D support, and joining forces with private organizations are more ways the government might increase the domestic production of secure drones. There is also the option of encouraging more

international work with allies to create a collection of reliable UAV and software companies for use by partner armies. They would limit the chances of cybersecurity threats while guaranteeing the supply of drones needed for the economy's continued growth.

Contextualization through Case Studies

In order to offer solid reasoning, this paper relies on examples such as the use of drones by the Ahmedabad Municipal Corporation in India and cyberattacks that used pager-walkie talkie systems in Lebanon. The earlier example shows that if drones used by cities are not well managed, important information and data could be made available. In this situation, clear examples of how easily old, unsecured devices can be monitored and changed similarly reflect the weaknesses found in today's drones. Such cases show how surveillance technologies change the country's geopolitical and infrastructure scene, making it important to have a thorough approach to how drones are regulated.

By analyzing case studies and real-world incidents, including the Ahmedabad Municipal Corporation's surveillance infrastructure and the pager-walkie talkie attacks in Lebanon, this paper provides a comprehensive perspective on the intersection of national security, cybersecurity risks, and economic consequences.

Literature review

Since drones were introduced, they have greatly affected modern surveillance, creating new benefits as well as serious risks. Before, these aircraft were just used in the military, but today other fields like agriculture, police, infrastructure checks, and media are also using them. However, the large-scale use of mobile apps has provoked talks about privacy, the rules that apply to them, and human rights. There is growing interest among specialists to understand the moral and legal issues connected to drones, mainly those used for surveillance. Most people now realize that a proper legal and institutional system is needed to take care of these issues.

An important point in the research is how there are regulations missing for drones. In the United States, the FAA is the main agency that oversees UAV operations and mostly pays attention to safety and managing airspace. Although they call for the registration of drones, define how high drones can fly, and identify areas where drones should not fly, they do not take care of privacy issues. Siddiqui (2025) believes that FAA's regulations do not include rules for drones with modern AI surveillance technology. He states that although the FAA is good at controlling air traffic, it still lacks measures to handle the issue of people using drones to gather and use private data, watch over others, and harass them.

Localized rules against voyeurism, trespass, and data collection have been put in place by states to cover this gap. For example, California made it a law that people cannot use drones to capture pictures or recordings without the owner's permission on private property (Cal. Civ. Code §1708.8). Similar rules are put in place in Texas and Florida. At the same time, it is not always possible to enforce such laws since many law enforcement agencies are not aware and do not have the required equipment. They point out that, though there are laws, police departments usually do not have SOPs for dealing with drone-related concerns. Such inconsistency gives unequal protection to people in different areas and depending on the level of training officers receive.

A new issue mentioned in many studies is the boost in drones equipped with AI and made abroad, which makes it easier to monitor people. Because these drones have facial recognition, tracking people's actions, and geolocation, many are worried about them being used for espionage and storing lots of personal data. It is mentioned that creating critical technologies in those two countries could allow them to be used for both peaceful and military purposes. They may be used for business objectives yet be secretly adjusted to spy on people. It is very hard to notice, monitor, or rule over these drones because their data transfer process is not clear.

Drone surveillance adds another difficult point to consider when reading the Fourth Amendment. The amendment has often been used to prevent government officials from performing unlawful searches or taking away people's possessions. At the same time, drones used by individuals make it impossible to tell when someone is watching for public or private reasons. In 2025, Siddiqui argues that today's court judgments do not properly handle situations caused by modern technologies. Even though GPS tracking and thermal imaging are now part of the law, there is no clear ruling yet on what drone surveillance by non-governmental groups might mean. In this situation, the victims of privacy misuses struggle to do much about the wrongdoing.

Along with legal gaps, it is common to notice that law enforcement agencies are unprepared in the available literature. When people report drones, the local police departments usually find it hard to handle the matter. Besides, departments are not equipped with drone detection systems, lists of registered drones, or pathways for joint communication with the FAA or Homeland Security. Siddiqui (2025) proposes that local and suburban areas establish new drone violation response squads and work out agreements with other agencies for sharing important information and coordinating operations.

The documents point out that being aware of and involved in society is important for combating illegal drone tracking. They suggest that, in most cases, people do not understand what their federal and state laws on privacy and drone use mean for them. When the general public does not understand drones, rogue operators can fly with no fear. Many people are not using the DroneZone platform and B4UFLY mobile app because the information about them is not being shared widely. They suggest that setting up educational campaigns, public service announcements, and workshops in the community will help people recognize drone violations and inform the authorities when they see them. It is also possible for people to react promptly and legally using inexpensive technological equipment.

It is being suggested by researchers that geofencing and AI-powered tools should be used to stop and handle kids' access to adult content. With these technologies, digital borders can be made for schools, hospitals, and government properties to block drones from such areas. They hope that making these capabilities rules for all U.S. commercial drones will make flights safer. They also suggest that drones get approved through certification that ensures their data protection, visible signals, and strict surveillance rules are met.

The wider uses of drone surveillance are presented by examining cases from different countries around the world. In India, the Ahmedabad Municipal Corporation has resorted to drone

surveillance for checking crowds and illness in the community. Although good for public health, these programs cause some people to worry about their data and who is responsible for it. Just like in Lebanon, unregulated drones' vulnerabilities may allow them to be used for surveillance. Such cases prove that this matter is worldwide and calls for all nations to use the same standards and best approaches.

All in all, what the literature clearly shows is that there are many complex issues existing at the juncture of law, technology, governance, and civil liberties. The abuse of drone surveillance technology creates big problems within the present laws, enforcement, and knowledge among the public. According to legal scholars, there should be updates to federal laws so that people have the same Fourth Amendment rights against drones operating by private businesses as by the government, and so that all UAV data and software are handled transparently. Those in charge should concentrate on providing law enforcement training, using integrated reporting, and making sure compliance is maintained through geofencing and AI surveillance. Lastly, it is important to educate and support the community to make sure various groups are able to resist and hold others responsible. Because drone technology is advancing, the policies overseeing it should also change. Unless lawmakers, organizations, and citizens act quickly and together, the growth of innovation could eventually lead to a loss of privacy and people's trust.

Case Study: Drone Surveillance Incident in Silicon Valley

In an uneasy situation from Silicon Valley, the author's brother noticed that a drone kept flying just above his house several times. This series of events left the resident uneasy and scared because he feared that the drone would watch or listen to him without his permission. In order to be safe and get answers, the resident took photos and noted the times of the incidents and contacted the local police. On the other hand, after everything, it turned out that the police did not give us any assistance. They clearly expressed that they were not familiar with drone rules and were not sure if what the reporting person did was against the law. No formal investigation was carried out by the officers, and they did not answer questions related to the law or pass the matter to the right aviation or cybersecurity officials.

This situation proves that official bodies are catching up slowly with the quick adaptation of drones by society. The problem is even greater considering that there are well-known FAA rules that specify how drones should be used for both commercial and recreational purposes. These rules are flying under 400 feet, keeping contact with your drone all the time, and obtaining permission before flying over someone's property. Furthermore, privacy laws exist in several states, for example California Civil Code §1708.8, which prevent anyone from invading privacy electronically, including drones. Due to weak and incomplete training, local officers find it hard to detect any relationship between drone mishaps and these laws . Because of this case, we also wonder if citizens can get justice: usually, those facing possible surveillance threats do not understand the law or have access to support from authorities. Siddiqui (2025) claims that an event like this highlights that the law and rules to manage technology are not as advanced as the developments in technology.

The fact is that this situation is not the only one of its kind. The situation shows that overall, law enforcement in the country is not ready, as many agencies do not have clear procedures for handling complaints about drones. Most police officers do not get training related to privacy and trespass rules for drones, and they do not have necessary tech tools to monitor or stop them. Even though the FAA supplies tools such as DroneZone and the B4UFLY app for the public, many people are unaware of them. Without everyone working together and explaining how to protect themselves through education, it is likely that cases like the Silicon Valley incident will occur more often as autonomous AI drones are developed. By this case, we learn that personal privacy can be threatened, causing us to highlight the importance of improving police education, agency coordination, and public discussions over drone regulations and digital surveillance threats.

Legal Gaps and Regulatory Ambiguities

Present guidelines for drone flying in the United States have some major problems and are not very clear, mostly when it comes to privacy. Handling airspace safety is the Federal Aviation Administration's main concern, and to achieve this, it has made rules on heights for different types of aircraft, registration for drones, and controlling the movement of multiple types of aircraft in the same airways. At the same time, the regulations focus more on safe operations than on protecting peoples' privacy. A sizable part of the FAA's policies does not address formally the use of drones to watch over private property. While taking care of air space is important, it has resulted in a gap in privacy law that now concerns more and more people living in residential areas.

Since the federal law isn't enough, multiple states have taken steps to prevent drones from being used to snoop or harass people. California's Civil Code makes it possible to sue anyone who drone images or records in private using aerial drones without your agreement. In the same way, Texas and Florida both prohibit flying UAVs for surveillance unless you have proper permission from the relevant authorities. The inconsistent application of these laws is mainly caused by absence of expertise, not enough public awareness, and technical issues in different locations. Police departments, who are dealing with many other cases, usually lack the proper resources to deal with drone surveillance issues that involve both technology and legal laws.

Legal experts say that the law regulating drones was created a long time ago and should be updated to meet today's AI-related advancements. As stated by Siddiqui (2025), the technology progress of drones surpasses the U.S. government's ability to regulate them, since many of these devices are now fitted with sophisticated facial, thermal, and real-time location instruments. Such AI-driven functions make it much riskier for privacy to be violated, because drones can now easily gather, store, and review private data with little assistance from people. They state that the growing number of AI-drvone from foreign countries aggravates the problem. As these drones are used by countries whose interests differ from the U.S. ideals, they are a great worry because they could be used for spying and sneaking data. Since these drones are remote and have closed systems, their surveillance might work without the user being aware, which makes it very difficult to identify or find out about any misuse of data.

Making the matter more complicated is how the Fourth Amendment is read, which is designed to safeguard against unfair searches and seizures. Generally, this protection from the

constitution helps only in situations involving government bodies, not individuals or companies. Thus, people who use drones to monitor others without permission commonly benefit from the legal uncertainty in this matter. So far, the Supreme Court has not made a direct ruling regarding the use of drones for surveillance by private people. Because the issue is uncertain in court, people have few options to address privacy invasions by non-government drones, which makes it even more important to pass laws in both state and national authorities (Siddiqui, 2025).

Overall, the way drones are managed by laws in the United States is not enough for the problems that today's UAVs bring. Because of AI, foreign technology, and airborne surveillance, immediate changes to privacy laws are needed to meet the new challenges between public safety, people's freedom, and the nation's security.

The Role of Law Enforcement Agencies

Citizens usually tell their local police first when they see any suspicious activity involving a drone. Even though police often respond first, the majority of departments aren't geared to properly deal with such complaints. The reason is real and linked to the gap that seems more serious because drone technology keeps evolving and is becoming more widely used. Most police and sheriff officers have not learned about the rules from the Federal Aviation Administration that deal with drone altitudes, areas where drones are not allowed, and the rules for registration. Seldom are people informed about state laws that oversee aerial surveillance, private viewing of others electronically, and drone trespassing (Siddiqui, 2025). That's why when dealing with drone crimes, the police sometimes either have no idea how to handle it or incorrectly describe the incident using other laws.

There is a major problem with properly enforcing laws since there are not any standardized operating procedures (SOPs) for dealing with drone incidents. Due to the new nature of drone crimes, many laws around them are unclear for officers. Sometimes, people are not sure in different places whether a drone flying over their backyard means trespassing, spying, or causing a nuisance, and which proof is required to bring legal action. Besides, hardly any departments have systems to discover, trail, or shut down unauthorized drones. Even if the police go to the scene after a complaint, it is often tough for them to track and arrest the person responsible for the drone. High-risk zones, which include areas by airports, important infrastructure, or government buildings, make this an especially serious problem since drones could threaten the nation's safety.

It is also difficult because local law enforcement, the FAA, and groups like the DHS do not communicate well. Federal authorities can investigate drones that go to restricted areas or perform suspicious actions, but sharing and exchanging information or teaming up for an investigation is not generally possible. Having a single drone to monitor all airspace results in delays, confusion about law enforcement, and the opportunity to spot similar acts of unlawful activity is missed. Siddiqui (2025) believes that if local police, aviation authorities, cybersecurity units, and emergency response teams all work as one, they can handle this fragmentation. Thanks to such a model, people could exchange information live, handle emergencies using joint teams, and use counter-drone systems rapidly where they are needed.

Police departments also need changes in organization and should invest in training their staff. Collaboration between the government and businesses provides great opportunities to create new training systems. If law enforcement collaborates with drone makers, AI professionals, and cyber consultants, it will be able to manage UAV activity, analyze the dangers, and take action within the law. The programs should have sections on civil liberties so that enforcement agencies do not overstep their constitutional powers. In addition, they support the installation of radar, sensor equipment, and geofencing systems in areas under surveillance so that police can spot unapproved drones more easily.

In the end, empowering law enforcement to manage drone issues means changing their culture and procedures to acknowledge that drones are essential in future security matters. As long as there isn't this change, people dealing with unlawful drone surveillance will still feel frustrated, confused, and unsafe.

Public Awareness and Civic Empowerment

In a world where drone technology is growing, being knowledgeable and strong citizens can be one of the best ways to fight unlawful surveillance. Since drones are appearing more often in neighborhoods, public parks, workplaces, and sensitive offices, regular people are now playing a bigger role in safeguarding privacy. Only very few people are familiar with the laws that govern drone operations or ways to protect their rights if needed. Being unaware of such things means that communities are not protected against such acts by law enforcement. So, sharing information is critical, as it helps enforce accountability when police or the government are not quick to help.

Before anything else, people should understand the privacy laws at both the state and federal levels. The Fourth Amendment and several federal laws give basic privacy protection, but many cases of drones violating privacy are carried out by regular people and mostly remain unresolved. There are laws in California, Texas, and Florida that stop people from flying drones to picture or record those on private property without permission. However, if the public does not realize what these rights are, people often do not fight against violations. Therefore, people need to be made aware of what is considered legal use of drones, when someone's privacy is breached, and the legal solutions available to them.

It is also crucial for the general public to realize the limitations that drones have because of rules set by regulatory organizations such as the FAA. For aeromodelers, it is important to stay below 400 feet of altitude, avoid certain areas like near airports, government places, or important facilities, and also be allowed to fly at night with proper lighting . When individuals know these boundaries, they can tell if using a drone goes against the law or not. For example, spotting a drone right next to your bedroom or children's school is a possible threat that should not be ignored.

Giving the public useful ways to record and notify drone violations is also part of empowering them. Everyone should get guidance on handling images or films of suspicious drones, keeping records of their movements, and spotting particulars, for example the model or the lights. Such evidence may be very important when investigating a case. Using the DroneZone portal or the B4UFLY app makes it easy for anyone to find rules in their area and report law

violations. Nevertheless, these resources are not used as much as possible because they are not promoted effectively. Informing the public about their benefits by putting information on social platforms, websites, and event programs can attract many people.

It is sometimes possible to use technology to fight these problems, but this should only be done thoughtfully and while following the law. For example, signal jammers are currently illegal in the U.S. since they mess with wireless signaling. Still, other equipment such as motion detectors, radar, and drone spotters is allowed, so they may be added to your safety setups. They call for safe use of such technologies, mainly in urban housing, places of worship, and communities next to borders, since those areas are often targeted by unauthorized surveillance.

Resilience is built in the community through endeavors like public service messages, classes at schools, and workshops held in neighborhood places. These initiatives make people aware and also encourage vigilance and teamwork among everyone. People from the community should be aware of what they can do to encourage others and act if they see something suspicious done by a drone. Moreover, local authorities and nonprofit groups ought to offer help to these initiatives by giving out pamphlets, conducting webinars, and educating watch groups on drone safety. To sum up, strengthening civic involvement against unauthorized drone watching helps fix openings in the law and renews people's trust. They mention that, when everyone is informed and open about the subject at the community level, this results in people standing collectively against abusive use and can really reduce it in underserved and high-risk areas where usual enforcement may not work well enough.

Conclusion

With more and more drones being used in business, for pleasure, and by the authorities, there is a growing necessity to deal with the legal, institutional, and social issues it divulges. Because so many drones are outfitted with advanced AI, the air has become a new area where privacy is threatened. The experience of a man in Silicon Valley, who was constantly watched from the sky without being able to take any legal action, well demonstrates what Americans across the country go through. Despite the person's efforts to report drone activities inside his rights, local officials did not know what to do—blindly showing their unpreparedness in the matter.

It is not unusual because of problems at many levels: old federal laws that do not match new drone technology, different rules in each state, unclear guidelines for law enforcement, and many people having no idea about drone rights and what to do. Each problem by itself is serious, but all of them combine to weaken society and leave people unprotected. In addition, with an increasing number of foreign-made drones enhanced by AI, collecting private data is much simpler. This becomes especially important as countries worry more about their data security.

These risks can only be handled with a wide and coordinated approach. It is necessary for the federal government to draft legislation that offers standard privacy protections that control drone surveillance used by any actor. Such laws should state that data should be handled in certain ways; pilots must keep away from some private spaces; and all drone activity should be clearly visible in the air as it happens. At the same time, law enforcement needs to gain training in how

the Federal Aviation Administration, individual states, and ethics affect aerial privacy for proper and constitutional guidelines. Just as importantly, people should be taught in public campaigns how to notice, record, and report illegal use of drones.

Once the legislative structure, institutions, and people are prepared, the United States will have the ability to keep its main values of privacy, safety, and personal liberty safe from new technology threats. If introduced ahead of time, these efforts will protect the airspace from turning into a field where privacy diminishes and authority rises.

Recommendations

For Law Enforcement Agencies:

The presence of law enforcement is important in controlling the risks caused by illegal surveillance using drones. It is important to add training that includes FAA and state safety and privacy rules throughout all the company's departments. Such sessions should focus on rules over drone height, using drones over private property, guidelines for surveillance, and procedures for collecting evidence by flying a drone. If they do not know these basics, officers are not ready to manage citizen complaints or enforce the law.

The creation of a "Drone Violation Response Unit" in urban and suburban police forces would guarantee fast and professional attention to any drone incidents. Units ought to be equipped with systems that identify drones, work with digital evidence, and connect in real time to make monitoring and dealing with threats more exact. Some of their important duties are gathering evidence, stopping flights in prohibited areas, and cooperating with various government agencies in cases of high risks.

Law enforcement should also set up an online portal that connects all local groups to the FAA, Department of Homeland Security (DHS), and groups focused on cybersecurity. It would make possible the immediate logging of incidents, the ability to spot patterns, and coordination by different organizations. It would also let anyone have direct contact with the authorities through relevant images or proof, which would relax the workload on 911 teams and lead to quicker investigations.

For Policymakers:

Because the current law is unclear, strong federal rules need to be made to provide privacy protection from drone spying. They ought to set guidelines for using drones, ensure accountability of operators, and give punishments for people who take pictures or video without consent. It is just as important to include private companies under the legislation, so that surveillance does not undermine the safety of civilians.

Besides, lawmakers should agree to fund and authorize the widespread use of drone technology in all sensitive areas, including residential areas, schools, and government offices. Thanks to these sensors and analyzers, along with AI radar, people and officials know about unauthorized drones right away and so respond to them more rapidly.

For better enforcement, using AI and geofencing should be made compulsory for any commercial drone in operation within the United States. Some drones equipped with geofencing technology will automatically be restricted from entering restricted places like schools, hospitals, and country landmarks. With a digital boundary in place, organizations can prevent violations and relieve the duties of officials while lowing the risks of intentional or accidental errors.

For the Public:

The involvement and careful attention of the public help a lot in tackling unlawful drone use. It is important to motivate people to try out application such as B4UFLY or DroneZone to know about nearby rules and airspace zones for drones. On these platforms, the public can also report about suspicious drones, which assists in collecting data that is useful for law enforcement and aviation authorities.

Anti-surveillance tools that require little investment, such as motion-triggered alarms, radar detectors, and low-range drone jammers, are other self-defenses allowed for homeowners. Such devices are able to notice unwelcome UAVs and support the filing of complaints for legal action. Sometimes, devices are able to detect what type a drone is and how it flies in the air, which is important for tracking the operators.

Finally, people should speak up and urge leaders to set up better privacy laws locally and nationally. Getting involved in town meetings, giving opinions in public consultations, and joining in on campaigns or petitions can encourage elected officials to pay attention. Residents of areas that are considered underrepresented or at greater risk should advocate for civic safety since drone misuse may be a bigger threat to them.

References

1. Blancato, F. G. (2024). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet, 16(1), 12–32.
2. Busby, C. (2024). Evidence for the use by Israel of a neutron uranium warhead in Palestine and Lebanon. ResearchGate. https://www.researchgate.net/publication/376445659
3. Chakraborty, S. (2024). Moral simpliciter of ethical giving. https://doi.org/10.1007/978-3-319-23514-1_1309-1
4. Chowdhary, M., & Diasso, S. (2024). Taxing big tech: Policy options for developing countries. State of Big Tech. https://projects.itforchange.net/state-of-big-tech/taxing-bigtech-policy-options-for-developing-countries/
5. Egan, J., & Rosenbach, E. (2024). Biosecurity in the age of artificial intelligence: What's the risk? Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/biosecurity-age-ai-whats-risk
6. Graham, A. (2024). Is China beating America to AI supremacy? The National Interest. https://www.belfercenter.org/publication/china-beating-us-ai-supremacy
7. Grochmalski, P. (2024). American–Chinese war for strategic dominance in the field of artificial intelligence and the new AI geopolitics. Bellona Quarterly. https://kwartalnikbellona.com/article/143837/en

8. Hassan Rasheed Siddiqui, and Ms. Maria Muniza. (2024). "The Drone's Gaze: Religious Perspective on Privacy and Human Dignity in the Age of Surveillance." Al-Qamar.
9. Hassan Rasheed Siddiqui, Maria Muniza. (2025). Analyzing the Shortfalls of the U.S. Countering CCP Drones Act in Light of China's National Intelligence Law. Social Sciences & Humanity Research Review. Style)
10. Hoffman, S., & Podgurski, A. (2024). Artificial intelligence and discrimination in healthcare. Yale Law School Open Scholarship Repository. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/5964/
11. Kambouris, M. E. (2024). Hybrid warfare 2.2. Advanced Sciences and Technologies for Security Applications. https://rieas.gr/images/KAMBOURISM.pdf
12. Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the public policy process? The case of generative AI. Policy and Society, 2024, puae012.
13. Roumate, F. (2024). Artificial intelligence and the new world order: New weapons, new wars and a new balance of power. Springer.
14. Rowell, J. (2024). The cold war never ended. Providence Magazine. https://providencemag.com/2023/05/the-cold-war-never-ended/
15. Sharma, S. (2024). Biotechnology and the return of biological warfare. Observer Research Foundation. https://carnegieendowment.org/research/2024/02/biotechnology-and-the-return-of-biological-warfare
16. Siddiqui, H. R., & Muniza, M. (2025). Hybrid Warfare and the Global Threat of Data Surveillance: The Case for International Standards and Regulation. Pakistan Social Sciences Review.
17. Siddiqui, H. R., & Muniza, M. (2025). Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards. Annals of Human and Social Sciences.
18. Varoufakis, Y. (2024). Technofeudalism: What killed capitalism. Melville House.
19. Yüksekdağ, Y. (2024). Commodification, datafication and smart cities: An ethical exploration. Journal of Urban Affairs, 1–17.
20. Zhang, J. (2025). Navigating in the clouds: The triumphs and drawbacks of the Cloud Act. Seton Hall University Student Scholarship. https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2267&context=student_scholarship
21. Zhang, M. Y. (2024). Cold war 2.0: Artificial intelligence in the new war between China, Russia and America. Australian Journal of International Affairs, 78, 520–526.
22. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2868
23. **How to cite:** Siddiqui, H. R. ., & Leghari, A. . (2007). FAITH, FREEDOM, AND THE FUTURE: RECLAIMING INCLUSIVE DEMOCRATIC VALUES IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 13(1), 107–116. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2868
24. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2870
25. **How to cite:** Siddiqui, H. R. ., & Leghari, A. . (2008). LIBERALISM IN SOUTH ASIA, A CASE STUDY OF CIVIC LEADERSHIP AND INTERFAITH HARMONY. The Journal of Contemporary Issues in Business and Government, 14(2), 90–97. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2870
26. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2871

27. **How to cite:** Siddiqui, H. R. ., & Muniza, M. . (2009). SOWING ILLUSIONS, REAPING DISARRAY: MEDIA INFLUENCE, URBAN MIGRATION, AND THE DISMANTLING OF SOCIETAL NORMS IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 15(2), 126–139. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2871
28. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2872
29. **How to cite:** Siddiqui, H. R. . (2011). IN THE COURT OF KNOWLEDGE, JUDGING THE JUDGES OF LEARNING. The Journal of Contemporary Issues in Business and Government, 17(1), 83–91. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2872
30. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2873
31. **How to cite:** Siddiqui, H. R. . (2013). THE PERSONAL LENS IN ACADEMIC EVALUATION: A CRITIQUE OF EDUCATOR BIAS. The Journal of Contemporary Issues in Business and Government, 19(1), 93–101. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2873
32. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2876
33. **How to cite:** Siddiqui, H. R. . (2024). UNLICENSED MEDICAL PRACTICE AND INSTITUTIONAL SILENCE: A CASE STUDY ON PMDC'S INEFFECTIVE RESPONSE AND THE IMPLICATIONS FOR PUBLIC HEALTH AND NATIONAL INTEGRITY. The Journal of Contemporary Issues in Business and Government, 30(1), 503–508. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2876
34. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2877
35. **How to cite:** Siddiqui, H. R. . (2010). DELAYED JUSTICE AND DUAL STANDARDS: THE ENFORCEMENT OF ARBITRAL AWARDS IN PAKISTAN. The Journal of Contemporary Issues in Business and Government, 16(2), 88–99. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2877
36. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2881
37. **How to cite:** Hussain, N. . (2025). EVALUATING THE NATIONAL SECURITY AND ECONOMIC CONSEQUENCES OF U.S. RESTRICTIONS ON FOREIGN DRONES. The Journal of Contemporary Issues in Business and Government, 31(2), 1–14. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2881
38. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2882
39. **How to cite:** Siddiqui, M. . (2024). BRIDGING THE GAP: EFFECTIVE PARENT COMMUNICATION AND ENGAGEMENT IN DIVERSE EDUCATIONAL SETTINGS. The Journal of Contemporary Issues in Business and Government, 30(2), 192–200. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2882
40. **Publication Link:** https://cibgp.com/index.php/1323-6903/article/view/2883
41. **How to cite:** Kharal, S. . (2025). STRATEGIC BLINDNESS: HOW BANNING TECHNOLOGY WITHOUT ALTERNATIVES INVITES ECONOMIC RECESSION AND SOVEREIGNTY RISKS. The Journal of Contemporary Issues in Business and Government, 31(2), 15–22. Retrieved from https://cibgp.com/index.php/1323-6903/article/view/2883
42. **Publication Link:** https://jarmhs.com/index.php/mhs/article/view/564
43. **How to cite:** Siddiqui, H. R. (2016). ESTABLISHING AIR AMBULANCE SERVICES IN PAKISTAN: A REGULATORY AND INVESTMENT FRAMEWORK FOR EMERGENCY

MEDICAL AVIATION. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 2(5), 17-30. https://doi.org/10.61841/z1tjva12
44. **Publication link:** https://jarmhs.com/index.php/mhs/article/view/565
45. **How to cite:** Siddiqui, H. R. (2023). STRUCTURAL INJUSTICES IN THE RECOGNITION OF FOREIGN MEDICAL DEGREES BY THE PAKISTAN MEDICAL COUNCIL: A CALL FOR POLICY REFORM. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 9(1), 58-66. https://doi.org/10.61841/vmqgts53
46. **Publication Link:** https://jarmhs.com/index.php/mhs/article/view/568
47. **How to cite:** Aziz, E.-U.-., & Memon, S. . (2025). FROM 2016 TO 2025: PAKISTAN'S LIFELINE STILL GROUNDED – A RENEWED CALL FOR AIR AMBULANCE REFORM. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 11(5), 6-16. https://doi.org/10.61841/5qjkfa18
48. **Publication Link:** https://nnpub.org/index.php/SSH/article/view/2829
49. **How to cite:** Siddiqui, H. R. (2022). PUBLIC FUNDS, PRIVATE GAINS: INVESTIGATING CORRUPTION IN NADRA'S MEGA CENTER LEASE DEALS. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 8(12), 17-28. https://doi.org/10.61841/2s3kmv78
50. **Publication Link:** https://nnpub.org/index.php/SSH/article/view/2873
51. **How to cite:** Siddiqui, M. (2023). THE ETHICS OF NURTURE: A PHD MIND AND AN EDUCATOR'S COMPASSION—29 YEARS SHAPING GENERATIONS AT HISD. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 9(11), 27-39. https://doi.org/10.61841/xvf2d770
52. **Publication Link:** https://nnpub.org/index.php/SSH/article/view/2874
53. **How to cite:** Ara, T. (2023). FROM MARKET TURBULENCE TO TRIUMPH: USHERING IN AMERICA'S ECONOMIC GOLDEN AGE. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 9(11), 40-50. https://doi.org/10.61841/as72e067
54. **Publication Link:** https://nnpub.org/index.php/EL/article/view/2828
55. **How to cite:** Siddiqui, H. R. . (2019). WHO JUDGES THE JUDGES? ADDRESSING INTEGRITY AND SECURITY GAPS IN THE SINDH JUDICIAL RECRUITMENT SYSTEM. International Journal of Advance Research in Education & Literature (ISSN 2208-2441), 5(8), 5-15. https://doi.org/10.61841/txq2w096
56. **Publication Link:** https://nnpub.org/index.php/EL/article/view/2855
57. **How to cite:** Siddiqui, M. (2025). LEARNING TO BELONG: AFGHAN NEWCOMER CHILDREN AND THE SOCIAL FABRIC OF AMERICAN SCHOOLS. International Journal of Advance Research in Education & Literature (ISSN 2208-2441), 11(3). https://doi.org/10.61841/h3p2a632
58. **Publication Link:** https://www.turcomat.org/index.php/turkbilmat/article/view/15240
59. **How to cite:** Rasheed Siddiqui, H. . (2018). DELAYED JUSTICE AND INCOMPLETE REFORMS:THE ENDURING CHALLENGE OF ARBITRAL AWARD ENFORCEMENT IN PAKISTAN. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 9(3), 1460–1483. https://doi.org/10.61841/turcomat.v9i3.15240
60. **Publication Link:** https://turcomat.org/index.php/turkbilmat/article/view/15241
61. **How to cite:** Ara, T. . (2025). TARIFFS, MARKET DYNAMICS, AND PROTECTING U.S. CONSUMERS: A CASE FOR STRATEGIC IMPORT POLICY. Turkish Journal of Computer

and Mathematics Education (TURCOMAT), 16(1), 109–122. https://doi.org/10.61841/turcomat.v16i1.15241