

Proliferation of unmanned aerial systems (drones) and policy challenges on the horizon: A Policy Memorandum to John P. Holdren

Allyn K. Milojevich

Oak Ridge National Laboratory, Global Security Directorate

Corresponding author: milojevichak@ornl.gov

Keywords: Unmanned Aerial Systems, drones, policy gap analysis

Executive Summary: In February 2015, the White House released a memorandum outlining policy guidelines and development for unmanned aerial systems (UAS). I call on the White House Office of Science and Technology Policy to pursue its memorandum and issue an Executive Order developing an Interagency Working Group (IAWG) to design a comprehensive framework for drone policy. UAS-related public policy is especially complicated for two reasons: 1) drone technology is advancing far more rapidly than associated legislation and regulation, and 2) the issues span across regulatory agencies and levels of enforcement. An IAWG would ensure that a comprehensive policy and regulatory system is developed, with clear roles for agencies without replication or contradiction. This memo outlines the gaps in domestic UAS policy and suggests questions that must be addressed.

I. Introduction

The past twenty years have seen a massive expansion of unmanned aerial systems (UAS) technology (also known as drones or unmanned aerial vehicles). This includes a large variety of drones, from sixty-six foot wingspan military surveillance drones capable of flying over 1,000 miles, to one-foot wide video drones with nine minutes of flight time available on Amazon.com. While the FAA has developed rules for drone flights, it has not addressed a wide array of potential public policy concerns, including privacy laws, search and seizure, airspace monitoring, lawful use, and the potential for domestic terrorism. As with most rapidly evolving technologies, the list of policy questions and challenges is immense. A non-exhaustive list includes:

- What are citizens' expectations of privacy with regard to drones and surveillance?
- Who owns the airspace and how is it monitored?
- What is the relationship between drone use and law enforcement?
- How are no-fly zones determined and how are they enforced? How do we identify

violators? Can we track the history of where drones have been flown?

- How can we track drones and assure the safety and security of our national airspace?
- Should the U.S., as a nation that values privacy, track drone use of its citizens? Drone tracking could violate the privacy rights of both the drone users, as well as compromise any information the drone may have collected.
- What happens when non-state actors acquire this technology and encourage its use among their followers?

Current federal regulation is through the Federal Aviation Administration (FAA), as it is the primary agency promoting safe flight of civil aircraft in air commerce. The rules developed thus far develop three classes of UAS use – public entities, civil operations, and hobby or recreational use (Federal Aviation Administration 2015b). The number of recreational UAS users is increasing rapidly, and while they are required to follow guidelines (Federal Aviation Administration 2015a) including flight restricted zones (Federal Aviation Administration

2010), enforcement of these guidelines is exceedingly difficult. Many of the enforcement issues stem from a lack of technology – there are few mechanisms for detecting drones when they enter restricted airspace (especially temporary flight restricted zones which change rapidly) and few technologies to safely land drones without crashing them (especially problematic around large crowds at, for example, football stadiums). Once a drone is landed or captured, determining ownership of the UAS, especially if it is a small recreational drone, is difficult, making prosecution challenging. Research is being done at attempt to address these concerns, but the rapid expansion of of UAS technology is greatly outpacing mitigation technology.

Federal policy largely does not address privacy and information gathering concerns, leading states to pass their own rules and regulations. As of August 2015, 26 states have passed some type of drone-related legislation (NCSL 2015), largely focusing on protection of privacy from potential surveillance, including requiring warrants for information collection (Rothfuss 2014, Zoldi 2013). This patchwork of rules and regulations creates unnecessary confusion for operators and law enforcement.

The courts have provided little to no legal precedent directly related to drones, although it is clear that they will soon have to address their legal ramifications. Having in place a strong regulatory and enforcement framework will ease the inevitable legal process. The precedent that does exist is largely drawn from surveillance-related cases and expectations of privacy (Olmstead v. United States 1928, Katz v. United States 1967, Dow Chemical Company v. United States 1986, Florida v. Riley 1989, United States v. Knotts 1983, United States v. Jones 2012, United States v. Causby 1946).

II. Regulatory and Policy Considerations

The FAA has been tasked with developing additional regulations by October 2015, including licensing and routes to further open the national airspace to drones. To most effectively improve the regulatory framework, it should clearly identify the organizing regulator (such as the FAA itself) and the roles other agencies play in supporting UAS regulation (including the Department of Defense, the

Department of Homeland Security, the Department of Energy, and others). This is where an IAWG plays a vital role – supporting discussions and negotiations among agencies so as to develop a well-defined and comprehensive UAS policy that can be implemented nationwide. Much of the work that an IAWG would best excel at is defining rules and regulations, as well as the legislation to support them, at the national level. This would include much of the work outlined in the rest of this memo. There would be a strong role for state and local governments as well, including implementation of the rules at the state level, defining drone use for state and local law enforcement, and licensing, all activities already performed at the state level for other programs.

Guidelines for enforcement will be vital to articulate, as the current regulatory framework provides little guidance in this area. As drones increase in popularity, their misuse will likely increase as well. Law enforcement, especially at the state and local level, will need clear and well-defined guidelines. Drone policy will require the adaptation of technologies and strategies to monitor and enforce rules, especially those related to flight restricted zones and drone identification. The remainder of this memo will outline some of the drone-related policy gaps for consideration by the IAWG.

Privacy Interests

Scholars suggest that current law does not adequately protect an individual's privacy from the users of drones (Zoldi 2013). For example, there is no clear rule on whether a drone can be flown over privately owned property and at what levels. Flying a drone 50 feet over a person's backyard could not only lay open the possibility of surveillance of individuals against their will, but it could also survey properties for burglaries. When purchasing property, do you own the airspace above your property and, if so, to what height? How are violations of privacy monitored and mitigated? One could imagine a scenario where surveillance technology becomes increasingly accurate as the amount of airspace one "owns" above their property increases.

It will also be necessary to determine whether evidence gathered by drones can be used in prosecution. What happens if a drone inadvertently

observes criminal activity? Can this evidence be used to obtain a warrant? If law enforcement has a warrant, can a UAS be used to gather evidence without alerting the named individuals? These are some of the questions that must be answered to protect individual safety and security. Clearly outlining legal, protected uses of drones by law enforcement will assuage future privacy concerns and guide legal precedent.

Drone Identification

The drone market is rapidly growing, especially for hobby use. Recreational use of drones does not require aircraft registration, although operators are subject to a number of FAA rules regarding use. This creates a paradox – how does the FAA enforce rules if registration is not required? If a small hobbyist drone is flown over a nuclear power plant, how can the owner/operator be identified? The current lack of drone identification mechanisms needs to be addressed in order to provide a reasonable level of accountability.

A “license plate” registration system for drone operators could address the problem, but there is a compliance issue. How do you assure that every person who purchases a drone is a responsible owner who obtains a license for their drone? A better option would be to develop internal devices tied to the purchaser. These could be passive devices, such as QR codes or transponders, only becoming monitored when the drone has committed a violation, such as violating a flight restricted zone. In this way, privacy is maintained for the majority of operators who commit no violations, but still identifies operators out of compliance. The internal devices would need to be cheaply mass produced and withstand a wide range of weather conditions. A greater challenge will be developing and employing detectors to scan for unauthorized drones. Not only would these devices have to scan permanent flight restriction zones (such as airports and power plants), they would need to be deployed quickly over temporary flight restriction zones (such as stadiums). A mechanism to track the history of drone flights will also assist in interdiction of flight restriction zone violators.

Another potential option for tracking drones is to expand air traffic control to include operation closer

to ground level. If incorporating drones into air traffic control is to be considered, a complete reorganization of air traffic control may be necessary as current technology is largely out-of-date. Tracking drones that are flying in the national airspace will help assure the safety and security of all air traffic.

Restricted Airspace

Several drone manufacturers have voluntarily incorporated restricted flight zones into their GPS systems, though not all manufacturers are supportive of these voluntary measures. Not only does it add to design costs, temporary restricted flight zones change regularly, requiring a mechanism for updating GPS codes. If a drone operator in violation is identified, assigning penalties, perhaps based on the severity of the violation, will be an important aspect of UAS policy.

Weaponization of Drones

Several states have preemptively prohibited the use of UAS in hunting. While it is likely wise to prohibit recreational drone operators from placing weapons on drones, the question of law enforcement weaponization is more unclear. As police forces become more heavily armed across the country, placing weapons of some sort on drones becomes a logical extension of a militarized police force. The question becomes especially difficult when considering a response to potential terrorist activity, which requires rapid identification, interdiction, and mitigation.

Safety Concerns

As the skies become more crowded and companies like Amazon consider delivering packages with drones, safety concerns become paramount. We need to establish a system for mitigating crashes between drones, as well as for collateral damage. Even small drones colliding midair and crashing on a vehicle have the potential to cause significant damage. What if an Amazon drone drops a package and damages a home? Assigning fault is an important aspect to UAS policy development (and another reason drone identification is vital). Internal mechanisms for detecting and avoiding other UAS will lessen collision probabilities and increase safety

as well. Addressing collateral damage will be an important part of future regulation. Perhaps one could propose an insurance market, much like automobile insurance, that would protect a drone operator from damages in the case of an accident. Again, we see compliance and drone identification become paramount issues.

Infrastructure Monitoring

Drones can be used to inspect critical infrastructure, detecting potential safety and security hazards before the vulnerability is exploited. Chemical facilities and industrial parks, for example, can span thousands of acres. Drones could be used to monitor facility exterior walls to enhance security, especially if fitted with motion detectors to identify intruders or other potentially hazardous activity for security personnel to investigate. Remote monitoring of storage fields of highly flammable chemicals or oil rigs, for example, could be accomplished by drones with detection equipment to identify spills and leaks before they become explosive.

UAS can also be used to support infrastructure inspections, especially when inspections are time consuming (such as along thousands of miles of railways and pipelines in the U.S.) or dangerous (as in the case of high voltage power lines). When using drones to inspect infrastructure, inspections may be performed more frequently, increasing safety and security. To effectively leverage this technology, it will be necessary to adapt inspection licenses and outline, specifically, how drones can be used (visual inspections, environmental monitoring, etc.).

Potential Domestic Terrorism

While it is highly unlikely that a terrorist or terrorist organization will obtain the technology or the technical expertise to operate a Predator drone over U.S. soil, a significant amount of damage can be done with a small commercial drone. Attaching explosives to a drone and violating a no fly zone over an event could quickly cause panic and significant damage. Panic might be enhanced by the use of chemical, biological, or radiological material, affecting event security for years to follow. How could the FBI or DHS respond if terrorist websites published drone technology blueprints and instructions? Is there a way to protect the homeland against this vague and ill-defined threat?

III. Conclusion

Unmanned aerial vehicles are an exciting technological development, but one that requires a robust regulatory and enforcement framework in the very near future. Congress is continuing to show interest in privacy concerns and the Department of Defense as well as the Department of Homeland Security have provided testimonies on security issues regarding infrastructure, espionage, and threats. Identification of drone operators who violate rules and regulations will be vital to the continued growth of the industry and the realization of the anticipated social benefits of the technology. I propose that the White House issue an Executive Order forming an Interagency Working Group to quickly develop rules, regulations, and enforcement guidelines to ensure this rapidly advancing technology grows in a safe and secure manner.

References

- Dow Chemical Company v. United States. 1986. 476 U.S. 227. Available from https://www.faa.gov/uas/model_aircraft/.
- Federal Aviation Administration. 2010. TFR Authorit Ready Reference. edited by U.S. Department of Transportation. Federal Aviation Administration. 25 August. *Unmanned Aircraft Systems* 2015b [cited 2015 25 August]. Available from <https://www.faa.gov/uas/>.
- Federal Aviation Administration. 2015. *Model Aircraft Operations* 2015a [cited 20 August 2015].
- Florida v. Riley. 1989. 488 U.S. 445.

-
- Katz v. United States. 1967. 389 U.S. 347. Drone Surveillance." *Journal of Law, Economics, and Policy* no. 10 (2):441-462.
- NCSL. 2015. *Current Unmanned Aircraft State Law Landscape*. National Conference of State Legislatures 2015 [cited 24 August 2015]. Available from <http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx>.
- Olmstead v. United States. 1928. 277 U.S. 438.
- Rothfuss, Ian F. 2014. "An Economic Perspective on the Privacy Implications of Domestic United States v. Causby. 1946. 328 U.S. 256.
- United States v. Jones. 2012. 132 U.S. 945.
- United States v. Knotts. 1983. 460 U.S. 276.
- Zoldi, Dawn M.K. 2013. "Drones at Home: Domestic Drone Legislation – A Survey, Analysis and Framework." *National Security and Armed Conflict Law Review* no. 4:48-81.

Author Biography

Allyn K. Milojevich serves as a Postdoctoral Researcher in the Global Security Directorate at Oak Ridge National Laboratory. Her research revolves around the use and development of robust legal and regulatory frameworks to support security in both the domestic and international realm. She obtained her Ph.D. in political science in 2014 from the University of Tennessee with a focus on public policy. She also holds M.S. and B.S. degrees in chemistry from Virginia Tech and Washington and Lee University, where she focused on analytical spectroscopy.