AU/ACSC/2011 SPRING A

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Focusing the Eyes Over America: Regulating and Training for the Ethical Domestic Use of Remote Piloted Aircraft (RPA)

By

Major Lindsey Bullard

Advisor: Colonel Fred Stone

Maxwell AFB, AL

February 2011

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED

Disclaimer

Contents

Page

Acknowledgements

I wish to thank my instructors Professor Gary Lester and Colonel Fred Stone for their detailed critiques of my paper and consistent support as I navigated the sometimes rough waters of this project. I thank my classmates of RE1 and RE2 for their fresh perspectives and angles of approach to this topic. I thank my contacts at NASA and NOAA. Though they asked not to be cited by name I really benefited from their views and gained a greater understanding of their work through our conversations. I thank my colleagues and coworkers who have supported me and provided me challenging viewpoints and counterpoints of debate. Most of all I thank my family, Jürgen, Jahn, RReagan, and J.D. for their unwavering patience and support as this paper was written and re-written.

Abstract

With the increasing usage of Remote Piloted Aircraft (RPA) domestically by a wide range of government agencies, there is an increased potential for violation of the civil liberties of U.S. persons. A review of the current regulations governing the employment of RPA domestically reveals shortfalls that need to be addressed to better provide an acceptable balance between mission accomplishment and protection of U.S. persons' civil liberties. Three courses of action to address these shortfalls were evaluated: prohibiting all RPA usage domestically, implementing additional regulations, and not taking any action to change current regulations. The implementation of additional regulations to govern the domestic RPA usage was determined to be the best course of action. Recommendations were made regarding the possible implementation of overarching guidance governing the ethical usage of RPA domestically. This guidance would address the permissible collection, retention and dissemination of information on U.S. persons, modeled after the existing Intelligence Oversight Program regulations. The need for judicial clarification regarding when warrants will be required by law enforcement, as well as what laws may need to be implement to govern private use of RPA, was also identified.

Chapter 1 - Introduction

Remote Piloted Aircraft (RPA), also known as Unmanned Aerial Vehicles (UAVs), are being utilized over U.S. soil to an increasing extent. These systems' thermal sensors, streaming video, and medium to high altitude, long endurance capabilities have made them an attractive asset for use by government organizations ranging from the military to law enforcement to the scientific community. As the legitimate domestic missions involving RPA increase, so do the concerns regarding possible abuses of their capabilities to violate civil rights.

U.S. military RPA have been utilized in support of the Department of Homeland Security and law enforcement, doing drug interdiction and identifying illegal border crossings.[1] During Hurricane Katrina, there was an attempt to use them to identify survivors using their thermal sensors, but airspace issues could not be resolved in time, something that has since been addressed and is not expected to pose a problem during future natural disasters.[2] Law enforcement agencies such as Customs and Border Protection and the Miami-Dade Police Department, have purchased their own RPA with the intent to use them to identify and capture criminals and combat terrorism.[3] They also plan to use them as support assets after natural disasters to survey damage and identify survivors. The scientific communities at NASA and the National Oceanic and Atmospheric Administration (NOAA) have developed roadmaps to utilize RPA to meet their mission objectives in areas to include research on climate, weather,

[1] U.S. Office of the Secretary of Defense, *Unmanned Aircraft Systems (UAS) Roadmap, 2005-2030* (Washington D.C.: U.S. Department of Defense, August 2005), I-3.
[2] Staff Sgt. Amy Robinson, "FAA authorizes Predators to seek survivors," Air Force Print News Today, 27 July 2006, http://www.af.mil/news/story.asp?storyID=123024467 (accessed 30 August 2009).
[3] UAS Overview - http://www.cbp.gov/xp/cgov/border_security/air_marine/uas_program/uasoverview.xml; Tim Elfrink, "Miami-Dade police buy drones," Miami NewTimes, 09 December 2010, http://www.miaminewtimes.com/2010-12-09/news/miami-dade-police-buy-drones/ (accessed 7 January 2011).

ecosystems, commerce and transportation.[4] NASA has also worked in conjunction with the U.S. Forest Service during the California wildfires to identify areas of hidden embers that could result in flare ups, as well as provide post-burn damage assessments.[5]

The domestic uses of RPA stand to benefit society, but the need to review and relate the current privacy laws and statues to RPA usage has been identified and is even being addressed in some academic[6] and legal forums.[7] There are no standardized regulations across all government agencies in place regarding the collection and dissemination of RPA collected information. Due to this gap, the question needs to be asked, "What is the best way to regulate domestic RPA use while balancing mission accomplishment with the protection of civil liberties of U.S. persons?" "U.S. persons" is defined in DODD5240.1-R as U.S. citizens, permanent resident aliens, unincorporated associations substantially composed of U.S. citizens or permanent resident aliens, and corporations incorporated in the United States, except for corporations directed and controlled by a foreign government or governments.[8] Given the capabilities of RPA, ranging from video to thermal imaging to extended flight times, it is critical that all individuals using the systems are given detailed training on regulations that will prevent accidental, incidental, or intentional compromise. When there are multiple agencies working together, such as with the military supporting law enforcement, and NASA supporting the U.S. Forest Service, there is the

[4] NASA Flight Research Projects - http://www.nasa.gov/centers/dryden/research/index.html; Sara Summers, "TAAC 2007 Conference NOAA UAS Applications" (Presentation, TAAC, Albuquerque, NM, 6 December 2007). ; NOAA, "NOAA UAS Town Hall - AUVSI Conference" (Presentation, AUVSI Conference, Washington, D.C., 8 December 2007). Accessible at http://uas.noaa.gov/library/presentations/index.html

[5]NASA, "NASA Aircraft Flies California Post-burn Imaging Mission," NASA News Release, 24 November 2009, http://www.nasa.gov/centers/dryden/news/NewsReleases/2009/09-71.html (accessed 16 January 2011).

[6] Geoffrey Christopher Rapp, "Unmanned Aerial Exposure: Civil Liability Concerns Arising From Domestic Law Enforcement Employment of Unmanned Aerial Systems," *North Dakota Law Rev*iew Vol 85: No 3 (2009): 623-648. Available at: http://web.law.und.edu/LawReview/issues/web_assets/pdf/85-3/85NDLR623.pdf

[7] http://www.sherdog.net/forums/f54/uav-surveillance-advancing-rapidly-1036505/ - In 2001, the United States Supreme Court decided that performing FLIR surveillance of private property without a search warrant by law enforcement violates the Fourth Amendment's protection from unreasonable searches and seizures. Kyllo v. United States, 533 U.S. 27 (2001) KYLLO V. UNITED STATES

[8] Department of Defense (DOD) Directive 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, 7.

potential of information being disseminated to improper individuals. When scientific research is being conducted with high powered surveillance technology, as is done at NOAA and NASA, there is a potential risk of releasing information to the public, under the heading of research data, which could violate U.S. persons' civil liberties.

This paper will utilize the problem/solution framework. It will address the developing problem of the increasing potential for abuse of civil rights as the use of domestic use of RPA increases and evaluate possible courses of action that can be taken to mitigate this problem. A review of existing regulations applicable to multiple government agencies will be conducted. This will be followed by a look at the regulations that only apply to certain agencies. The areas of potential shortfall in these regulations that may allow for compromise of civil rights, whether intentional or otherwise, will be identified. An assessment of possible alternative solutions, to include doing nothing, will be conducted and a recommendation for course of action will be made. Additionally, as this is a very broad and complex topic, recommendations will be made regarding areas for further research.

Chapter 2 - The Regulations

Law enforcement and intelligence agencies have regulations regarding how information may be collected and disseminated that only pertain to them, but all agencies have to abide by the airspace regulations generated by the Federal Aviation Administration (FAA). The FAA writes its regulations with safety as the primary focus,[9] not the protection of civil liberties, but by virtue of the fact the FAA controls when and where RPA can fly, their regulations have an impact on the protection or possible abuse of civil liberties. The two key regulations that impact

[9] Les Dorr, Jr. & Alison Duquette, "Fact Sheet – Unmanned Aircraft Systems (UAS), FAA News Release, 1 December 2010, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287 (accessed 15 January 2011).

RPA usage domestically are the FAA Interim Operational Approval Guidance 08-01, *Unmanned Aircraft Systems Operations in the U.S. National Airspace System*, and Title 14 of the Code of Federal Regulations, Section 91, *General Operating and Flight Rules*.

Title 14 of the Code of Federal Regulations (Aeronautics and Space) is the primary regulation governing airspace usage in the United States. Section 91 outlines the overarching regulations by which aircraft, whether manned or unmanned, must abide. Section 91.113, "Right-of-way rules: Except water operations", provides the largest hurdle to unrestricted airspace usage by RPA as it states that "vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft."[10] As RPA are unable to "see and avoid" other aircraft on their own due the lack of an onboard pilot, as well as the fact that some of them, due to size, are potentially very difficult to be seen and avoided by other aircraft, RPA are primarily limited to operating in Restricted, Prohibited, and Warning Areas' airspace,[11] where there is little to no risk of collision with other aircraft, and are well away from the urban areas.

Currently, FAA policy states that "flight of [RPA] is not permitted over populated areas"[12] but there are avenues for waiver of this policy. Given the increasing demand for domestic use of RPA by what the FAA categorizes as "public" ("one that is intrinsically governmental in nature"[13]), there has been a subsequent increase in demand for Special Airworthiness Certificates – Experimental Category and Certificates of Waiver or Authorization (COAs). Either a Special Airworthiness Certificates (for civil users) or a COA (for public users) is required to operate an RPA outside of restricted airspace and in the National Airspace System

[10] Title 14 of the Code of Federal Regulations, "Section 91.113.Right-of-way rules: Except water operations," CAO 13 January 2011. Accessible at: http://www.gpoaccess.gov/ecfr/
[11] Federal Aviation Administration, *Aeronautical Information Manual*, 11 February 2010, 3-4-1
[12] Unmanned Aircraft Systems Office - http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/
[13] Federal Aviation Administration, Interim Operational Approval Guidance 08-01. *Unmanned Aircraft Systems Operations in the U. S. National Airspace System*, 13 March 2008, 5.

(NAS).[14] In light of this, the FAA created Interim Operational Approval Guidance 08-01. This document provides guidance on alternate means for the RPA to comply with the "see and avoid" provisions of Title 14 Section 91. The alternate means of compliance to the "see and avoid" provisions that this guidance generally accepts is in the form of ground-based or airborne observers, or another method of segregation. Any user "proposing 'see and avoid' strategies in lieu of visual observers, need[s] to support proposed mitigations with system safety studies which indicate the operations can be conducted safely".[15]

This need for an observer is removed, however, when the RPA is conducting operations in Class A airspace (18,000 to 60,000 ft). In the case of Class A airspace usage, the RPA is required to be able to operate under Instrument Flight Rules,[16] but will still need an observer until it ascends to that altitude. This is allowance of flight in Class A airspace, with an IFR flight plan, is of particular interest to the research community who are doing atmospheric studies, as well as those organizations that may wish to conduct collection over a large area such as the border.

The need for an observer does not preclude the use of RPA over populated areas, though. As mentioned earlier, after Hurricane Katrina there was a push to lay the foundation for RPA to be used in the aftermath of natural disasters. This foundation is present in the Interim Guidance, as it states that while RPA operations should not normally be conducted over urban or populated areas, RPA "operations may be approved in emergency or relief situations if the proposed mitigation strategies are found to be acceptable".[17] Further, it should also be noted that there is a

[14]Les Dorr, Jr. & Alison Duquette, "Fact Sheet – Unmanned Aircraft Systems (UAS), FAA News Release, 1 December 2010, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287 (accessed 15 January 2011).
[15] Federal Aviation Administration, Interim Operational Approval Guidance 08-01. *Unmanned Aircraft Systems Operations in the U. S. National Airspace System*, 13 March 2008, 8.
[16] Ibid, 13.
[17] Ibid, 10.

provision in this guidance for National Security exemptions. If the DoD or Department of Homeland Security "declares a [RPA] operation is a matter of 'national security," the FAA may approve an application for a COA which, under normal circumstances, might not otherwise conform to the guidelines set forth".[18] These agencies just need to declare on the COA application that they accept all potential risks of this operation. This type of waiver does require the involvement of the FAA Administrator and an equivalent level official from the requesting agency.[19]

As mentioned previously, the FAA's focus is on safety of flight. Therefore, the only mention of the onboard collection capability of RPA found in the Interim Guidance discusses them in the context of meeting the "see and avoid" provisions.[20] Neither the FAA nor Title 14 Federal Code addresses what should and should not be collected over domestic territory or the ethical dissemination of any information that is collected. Overall regulations governing collection and dissemination differ based on the category of user. This paper will only focus on the government users: military, law enforcement, and research.

Military users of RPA fall under the jurisdiction of Intelligence Oversight regulations. These regulations are designed to strike a balance between obtaining the information required to protect national security and protecting the individual rights granted by the U.S. Constitution and U.S. laws. In particular, Intelligence Oversight is designed to protect the rights of U.S. persons, not just U.S. citizens.[21] Intelligence Oversight was established by Executive Order 12333 *United States Intelligence Activities* and implemented through DOD Directive 5240.1-R and service instructions (ex. Air Force Instruction 14-104 *Oversight of Intelligence Activities*). These

[18] Ibid, 6.
[19] Ibid, 6.
[20] Ibid, 8.
[21] Department of Defense (DOD) Directive 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, 7.

regulations apply to all members of the DOD intelligence components, whether they are active duty, Reserves, Guard, civilian or contractors, as long as they are involved in intelligence-related activities that could result in the collection, retention, or dissemination of information on U.S. persons. Even DOD members that are not members of an intelligence unit need to abide by the Intelligence Oversight regulations if they are conducting intelligence missions. For example, the F-16 pilot that is tasked to use his gun camera for Non-Traditional Intelligence (NTI) collection is subject to these regulations. Intelligence Oversight does not apply to criminal investigations by law enforcement agencies, such as the Air Force Office of Special Investigations (AFOSI), or the Army's Criminal Investigation Division (CID). Per EO12333, Para 2.2, "Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency". [22]

It is important to note that Intelligence Oversight does not prohibit the collection of information on U.S. persons. It merely provides direction as to what information can be collected, how it can be collected, under what conditions it can be collected, how it can be retained , and how and to whom it can be disseminated. DODD 5240.1-R contains 15 "Procedure" sections that breakdown these rules. Procedures 2 through 4 outline the regulations regarding the conditions under which collection, retention, and dissemination of intelligence on U.S. persons is permitted. Procedures 5 through 9 cover, in more detail, methods of collection and the associated guidance and restrictions. Of particular importance to this research paper are Procedures 12 and 15, which cover provisions for assistance to law enforcement, and the process for identifying, investigating, and reporting possible violations.[23]

[22] Executive Order 12333. *United States Intelligence Activities*, 4 December 1981, as amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008).
[23] Department of Defense (DOD) Directive 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, 3-5.

In order for an intelligence component to collect information on a U.S. person, the collection must fall into one of 13 categories, but above all it must be part of the mission of that intelligence component to collect that information. Even if information is publicly available, for example on the internet, an intelligence component cannot collect it in the course of their official duties without a legitimate mission requirement. If there is a legitimate mission, the information must then follow into one of these categories: information obtained with consent, publicly available information, foreign intelligence, counterintelligence, potential sources of assistance to intelligence activities, protection of intelligence sources and methods, physical security, personnel security, communications security, narcotics, threats to safety, overhead reconnaissance (not directed at a specific U.S. person), or administrative purposes.[24] As can be seen, intelligence components *are* allowed and *do* collect information on U.S. persons currently, but in a way that supports a balance between accomplishment of desired mission objectives and protection of civil rights. Intelligence units need to be allowed to collect, retain and disseminate certain information on U.S. persons to allow for effective mission accomplishment. Some examples of everyday uses of this information are personnel files, recall rosters, and evaluations.

When military intelligence components support law enforcement, they are no longer subject to the Procedure 2-4 restrictions, but rather they must abide by the appropriate law enforcement procedures and those found in Procedure 12.[25] Per Procedure 12, intelligence components, with proper authorization, may assist law enforcement "for the purpose of: [1.] Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities, [2.] Protecting DoD employees, information, property, and facilities, and [3.] Preventing, detecting, or investigating other

[24] Ibid, 16-18.
[25] Ibid, 13.

violations of law."[26] These provisions open the door for extensive collaboration and information sharing. While it may seem that DOD intelligence has been given permission to collect on U.S. persons, as long as it can be tied to some sort of law enforcement support, there are further provisions that cover the type of support that may be rendered. Primarily, any accidentally collected information that appears to relate to a violation of Federal, State, or local laws, or that may result in imminent loss of life or threat to DOD resources, to include people, may be shared. In order for the DOD intelligence component to utilize their specialized equipment or facilities, such as RPA, to support law enforcement the support must be in line with DODD 5525.5 "DoD Cooperation with Civilian Law Enforcement Officials".[27]

When Intelligence Oversight regulations are violated, the matter is referred for review to the Inspector General. If there is a violation of Federal criminal law, the General Council is involved. Regardless of the perceived severity, all potential intelligence oversight violations are taken very seriously, as the regulations governing it can be traced directly back to an Executive Order and any violation has the potential to directly impact civil liberties. For this reason, the use of intelligence collection assets, such as RPA, domestically receives much attention.

As has been mentioned, law enforcement agencies have a different set of procedures designed to protect civil rights. It is these procedures by which intelligence components supporting law enforcement must abide. The overarching provision governing law enforcement when gathering information on U.S. persons is the Fourth Amendment. The Fourth Amendment states that "The rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated…".[28] The increasing prevalence of aerial collection capability by law enforcement, whether via helicopter or RPA, has become a

[26] Ibid, 56.
[27] Ibid, 56-57.
[28] U.S. CONST. amend. IV.

point of debate, often resulting in accusations of privacy violations. Jay Stanley, a senior policy analyst with the American Civil Liberties Union's Speech, Privacy and Technology Project, said, "Drones raise the prospect of much more pervasive surveillance. We are not against them, absolutely. They can be a valuable tool in certain kinds of operations. But what we don't want to see is their pervasive use to watch over the American people."[29]

Since technology is continually advancing, it is impossible for all possible uses to be projected and therefore many of the determinations as to what constitutes an unreasonable search are being made in appeals courts. In 1986, the Supreme Court ruled that the Fourth Amendment was *not* violated when the police overflew a suspect's home at 1,000ft in a private aircraft, and photographed his marijuana crop, which led to a search warrant and conviction. The court stated that the police were not required to obtain a search warrant to observe the marijuana as "the police observations here took place within public navigable airspace, in a physically nonintrusive manner… Any member of the public flying in this airspace who cared to glance down could have seen everything that the officers observed".[30] This concept that the police can use the same means available to the general public to collect information, without the need for a warrant, was the basis for a search to be ruled illegal in the 2001 case of *Kyllo v. United States*. The police in that case utilized a thermal imaging device to determine if the suspect's residence was emitting heat consistent with the high-powered grow lights. The warrant was based on this information and the court ruled that since the police had used "a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical

[29] Cited in: Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, 22 January 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html (accessed 22 January 2011).
[30] California v. Ciraolo, 476 U. S. 207 (1986)

intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant".[31]

As law enforcement agencies look to increase the use of RPA in the course of their duties, the question that will continue to be asked by the legal system is, "what is considered in 'general public use'"? Is it the price? A thermal imaging camera can be purchased via Amazon.com for around $1,600. [32] Is it the number of members of the public that utilize that technology on a regular basis? The remote controlled aircraft hobbyist community is enormous. Remote control aircraft available to the public range in size from "peanut scale," which has a wingspan of 13" or less, to "giant scale", with a monoplane wing span of at least 80" and a biplane wing span of at least 60".[33] Or is it determined by the social acceptance of that use of the technology in question? The general public does not walk around looking at the thermal signatures of other people's homes, as was done in Kyllo v U.S., but they do take pictures of the ground from low flying aircraft on a daily basis. These questions illuminate a gap in the regulations that law enforcement must adhere to ensure they are protecting individuals' civil rights as they perform their duties.

The research community presents its own challenges, as there is no overarching guidance governing the use of RPA sensors for scientific purposes. Organizations such as NASA and NOAA utilize RPA for the collection of scientific data, sometimes in coordination with other organizations such as when NASA aided the Forest Service by providing data on the California wildfires. Unlike the intelligence and law enforcement communities, the RPA used by the research communities do not have a set sensor suite. The sensors that will be loaded onboard for a particular mission is determined by the scientists who designed the experiment or research

[31] Kyllo v. United States, 533 U.S. 27 (2001)
[32] http://www.amazon.com/Extech-i5-Thermal-Imaging-Camera/dp/B003B3N60E
[33] http://www.hooked-on-rc-airplanes.com/scale-rc-airplanes.html

mission which is being conducted. What the sensor then collects is driven by the parameters of the experiment or mission. The diversity of scientific usage does not allow for one overarching regulation dictating how the sensors can be utilized. The decisions regarding retention and dissemination of the data collected are governed by the research being completed. Given the fact that the focus of NASA's and NOAA's research and experiments are primarily focused on phenomenon (weather, atmospherics, effects of natural disasters), combined with FAA airspace regulations, there has not been identified, to date, a need for overarching rules regarding incidental collection of information on U.S. persons.

Chapter 3: The Problem and Evaluation Criteria

The problem that this paper seeks to address and recommend a solution for is a developing one. What is the best way to regulate domestic RPA use while balancing mission accomplishment with the protection of civil liberties? There is a growing concern that the increase in domestic use of RPA will result in increases in violations of civil liberties. At a recent net-centric warfare/network enabled operations conference, Dr. Ruth Doherty, Program Executive Officer for Counter-IED Science and Technology Directorate Department of Homeland Security, highlighted the need for public acceptance before aerial surveillance would be put into wide-spread domestic use to spot bombs. She pointed out that surveillance cameras found in subways and stadiums, as well the increased security measures the Transportation Security Administration has put into practice, are considered to be controversial enough.[34] The most recent subject of controversy has been the full body scanners, now at many airports and some courthouses, which render a semi-blurry unclothed image of the individual to check for

[34] Ms. Smith, "TSA: Show Us Your Body, or We'll Feel You Up," NetworkWorld.com, 1 November 2010, http://www.networkworld.com/community/blog/tsa-show-us-your-body-or-well-feel-you

weapons and explosive devices. The option provided individuals who do not want to use the body scanner, as well as those on whose person an anomaly is found, is an invasive pat-down that involves the TSA agent's hands coming in contact with the individual's chest, buttocks, and genitals. These new measures have resulted in inquiries by both parties in Congress as well as some lawsuits.[35]

Dr. Doherty stated, "We need technologies [that are] … acceptable to the public." [36] As was mentioned earlier in this paper, the ACLU's Speech, Privacy and Technology Project has voiced concerns that increased domestic use of RPA could result in "pervasive surveillance" of the American people.[37] As for the general public, bloggers run rampant with one-sided reporting designed to generate concern that the government is already utilizing RPA to spy on U.S. citizens and will soon graduate to using them to identify dissenters and take action against them.[38] While many of these blogs are written in an inflammatory tone, with very little physical evidence provided to support their claims, their concerns are being echoed by the ACLU. On 26 June 2010, the ACLU started a website called "Spy Files" to track and expose incidents of domestic political surveillance. Michael German, ACLU Policy Counsel and a former FBI Special Agent, has stated that U.S. law enforcement is starting to revert to "certain old, bad

[35] Alex Altman, "TSA Scrambles to Combat the Outcry Over Body Scanning," *Time*, 23 November 2010, http://www.time.com/time/nation/article/0,8599,2032786,00.html; Marnie Hunter, "Jesse Ventura slams TSA with lawsuit," CNN Travel, 25 January 2011, http://articles.cnn.com/2011-01-25/travel/jesse.ventura.tsa.lawsuit_1_pat-downs-and-full-body-tsa-lawsuit?_s=PM:TRAVEL

[36] Cited in: Spencer Ackerman, "Even DHS is freaked out by spy drones over America," *Danger Room*, 26 January 2011, http://www.wired.com/dangerroom/2011/01/spy-drones-over-america-dhs-would-rather-not/

[37] Cited in: Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, 22 January 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html (accessed 22 January 2011).

[38] http://newsjunkiepost.com/2010/01/08/domestic-espionage-alert-spy-drone-discovered/-" Domestic Espionage Alert: Spy Drone Discovered"; http://www.operationdefuse.com/2010/04/27/drone-aircraft-are-patrolling-u-s-cities/ - "Drone Aircraft are Patrolling U.S. Cities"; http://www.infowars.com/drone-surveillance-program-targeting-americans/ - "Drone Surveillance Program Targeting Americans?"; http://www.rense.com/general47/uav.htm - "The Role Of UAVs/MAVs In Domestic Surveillance And Control"

behaviors when it comes to political surveillance."[39] While the use of RPA domestically is not addressed on the Spy Files website, the behaviors by law enforcement that are creating the concern about the potential use of RPA for political surveillance are discussed in an attempt to bring possible civil rights violations to light.[40]

U.S. bloggers are not alone in these feelings, either. In the United Kingdom there is a push to utilize RPA domestically for law enforcement and security purposes ahead of the 2012 Olympics. This has resulted in accusations that the government purposely misled the public as to the extent of the intended utilization as a "public relations strategy designed to minimise(sic) civil liberty concerns."[41] Critics are even accusing officers of talking about "selling the surveillance data to private companies".[42]

Given the shortfalls currently inherent in the existing regulations, this concern about the potential for increased civil rights abuses is not unfounded. While the FAA does currently restrict flights over populated areas, there are means to get waivers through the COA process. More and more law enforcement agencies are applying for and being granted these waivers, as they are able to meet the technological requirements as well as showing a need for reasons of security. NASA and the FAA are working together to loosen those restrictions even more through the "UAS in the NAS" project with a goal of routine access to the NAS by civilian RPA by the end of 2020.[43] It has already been established that the guidance as to what is acceptable use of a RPA by law enforcement is not clearly defined, and that intelligence organizations can collect on U.S. persons if they are doing so in line with Intelligence Oversight regulations, or in

[39] Gautham Nagesh, "ACLU launches 'Spyfiles' to track domestic surveillance," Hillicon Valley, 26 Jane 2010, http://thehill.com/blogs/hillicon-valley/technology/106299-aclu-launches-qspyfilesq-to-track-domestic-surveillance
[40] http://www.aclu.org/spy-files - "ACLU Spy Files"
[41] Paul Lewis, "CCTV in the sky: police plan to use military-style spy drones," *The Guardian,* 23 January 2010, http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones
[42] Ibid.
[43] http://www.faa.gov/about/initiatives/uas/ - "FAA Civil/Public UAS Roadmap"

support of law enforcement. Additionally, research organizations lack any guidance regarding the collection of information on U.S. persons. By being proactive about identifying ways to address these potential shortfalls in civil rights protections, while maintaining the mission accomplishment capability of organizations using the assets, this developing problem can be mitigated, providing a balance between protection of civil rights and mission accomplishment, while the negative response from the public over the increase in domestic RPA usage can be reduced.

To determine the best course of action to address these rising issues, three alternative courses of action will be evaluated and rated utilizing a decision matrix. The three proposed alternatives are: 1. Complete prohibition on all domestic RPA usage, 2. Creation of additional regulations governing domestic RPA usage, with training programs for all sensor operators, and 3. No change to existing regulations and training programs.

There are three criteria that will be used to rank the proposed solutions. First, the impact the solution has on the capability to accomplish the mission, whether that mission is law enforcement, intelligence, or research related. The points for ranking will be awards as follows: "-2" = Significant negative impact on the capability to accomplish the mission, "-1" = Slight negative impact on mission accomplishment capability, "0"= No impact on the mission accomplishment capability in either direction, "+1"= Slight positive impact on mission accomplishment capability, and "+2"= Significant positive impact on mission accomplishment capability. The second criterion will be the impact on protection of civil rights of U.S. persons. The rating system will again range from "-2" to "+2", based on the impact the proposed solution has on the protection of civil rights, with "-2" being a significant negative impact and "+2" being a significant positive impact.

The third criterion is the feasibility of implementing the proposed solution in all applicable organizations (since one of the solutions does not affect all organizations). This criterion's rating scale will be slightly different: "0" = Simple to implement, "-1"= Slightly difficult to implement, "-2"= Significantly difficult to implement, "-3"= Unrealistic to implement. This criterion requires a different scale in order to weight it, since it has a different impact on the overall decision. If a solution is unrealistic to implement, it should receive enough points to counterbalance the positives that may occur. If a solution is easy to implement, there are no positive points, since ease of implementation should not be able to outweigh potential negatives to the mission and civil right protections.

Chapter 4: Evaluation of Alternative Solutions

The first proposed course of action is that all RPA be prohibited from operating domestically. This would mean that all remote pilot aircraft, regardless of size, purpose, or operator would be prohibited to operate anywhere in U.S. airspace, to include restricted airspace. This course of action would have a significant negative impact on the mission accomplishment of all users. RPA are an in-demand asset by all types of government agencies, and prohibiting their use domestically one hundred percent would remove a valuable asset that is able to address gaps in meeting our current requirements in every field from research to law enforcement to homeland security. The NOAA has identified that RPA will fill "critical environmental monitoring needs and requirements" that are currently unmet. They also identified that strengthening our capability in RPA technology will in turn strengthen our Global Economic Competitiveness.[44] Prohibiting all RPA from domestic usage would return many Customs and

[44] Sara Summers, "TAAC 2007 Conference NOAA UAS Applications" (Presentation, TAAC, Albuquerque, NM, 6 December 2007).

Border Protection (CBP) agents to harm's way. Currently, CBP is using RPA to monitor the border providing efficient surveillance, as well as allowing those viewing the images to remain safe from possible attack from drug runners crossing illegally. Their successes have resulted in Texas lawmakers calling for more waiver approvals from the FAA, and more RPA, to allow for more missions.[45] On the military front, the desire for domestic use of RPA after natural disasters to help find survivors, sparked in the aftermath of Hurricane Katrina, led to certification of Predators by the FAA. While the certification came too late for them to be utilized post-Katrina, they are now allowed to be called into action during future natural disasters.[46] If all RPA were prohibited from flying domestically, this enhanced search and rescue capability would be lost. Due to the Significant Negative Impact this course of action would have on the mission accomplishment capability of numerous government agencies, this COA gets a "-2" for this criterion.

By removing all RPA from domestic airspace, regardless of size or operator, they will not be able to violate U.S. persons' civil rights, since the sources of potential surveillance will be removed. This would give this COA a "+2" for having a significant positive impact on the protection of civil rights from overhead surveillance. A downside to this COA, though, would be that it would prohibit not just government operation of RPA, but hobbyists' recreational RPA. This could generate new areas for argument about government encroachment on individuals' rights. First person view (FPV) video generated by Radio Controlled (RC) aircraft is a growing pastime for some skilled hobbyists[47], the results of which can be found on YouTube.[48] A recent

[45] Joan Lowy, "FAA under pressure to open US skies to drones," *My Way News*, 14 June 2009, http://apnews.myway.com/article/20100614/D9GB009G0.html.
[46] SSgt. Amy Robinson, "FAA authorizes Predators to seek survivors," *Inside ACC*, 27 July 2006, http://www.acc.af.mil/media/archives/story.asp?storyID=123024134.
[47] http://fpvpilot.com/default.aspx
[48] http://www.youtube.com/watch?v=nifuuM9oltU – "FPV rc plane night flight police helicopter chase"

example of this, which was in the news in November 2010, would be the tour of New York City by Raphael Pirker, which included the Statue of Liberty, Brooklyn Bridge, and some building surfing.[49]

The final criterion is the feasibility of implementing this COA. To stop use of all RPA domestically would mean removing capabilities from the U.S.' arsenal that may save lives (e.g. search and rescue), address global issues (ex. climate change), or protect this country (ex. border security). A particularly visible example is that the U.S. often provides imagery support to disaster relief operations in foreign countries, ex. in Haiti through the use of a RQ-4 Global Hawk RPA.[50] To deny this same capability to our own citizens in a time of crisis does not make sense. Given the prevalence the private citizen RC aircraft community, combined with the existing integration of RPA into research, law enforcement operations, and now disaster relief, this COA is unrealistic to implement. The manpower and resources required to prevent operation of private RC aircraft alone would be prohibitive. This COA rates a "-3" in this criterion.

Table 1: COA #1 Assessment Results

Criteria	COA #1
Impact on Mission Accomplishment Capability	-2
Impact on Protection of Civil Rights	+2
Feasibility of Implementation	-3

[49] http://www.youtube.com/watch?v=M9cSxEqKQ78 – "New York City"
[50] Air Combat Command, "480th ISR Wing supports disaster relief efforts," *Inside ACC*, 15 January 2010, http://www.acc.af.mil/news/story.asp?id=123185802.

The second proposed course of action is the creation of additional regulations governing domestic RPA usage, with training programs for all sensor operators. These regulations would start off with an overarching guidance that would address general concepts to avoid the forced generation of unnecessarily inclusive regulations during implementation. More tailored regulations would then be generated to address specific areas of existing shortfalls. Regulations would be implemented to require a certain level of encryption to all sensor feeds. This would address the identified danger of the RPA feeds being intercepted by third parties and their contents used to invade others' privacy.[51] Law enforcement would gain regulations that would more clearly outline when RPA usage would be permitted with and without a search warrant. Similar to the intelligence community, there would be times that law enforcement would be required to identify its presence and any collection it does in the course of their official duties would have to be done with the open knowledge that it is law enforcement that is doing the collection, regardless if the information is in the public domain. For example, police would have to announce their desire to conduct RPA operations in public airspace, even if a RC hobbyist does not need to do the same. Just as with the intelligence community, the purpose of the collection does override that the information may be in the public domain. This announcement of intent would help address the accusations that law enforcement is trying to institute secret surveillance. The attempt to try out new technology in a secluded site without outright announcing it to the public resulted in some very bad publicity for the Houston Police Department and fueled a number of articles challenging the need for secrecy.[52] The test was coordinated with the FAA, a Certificate of Authorization was issued, and the test was conducted

[51] Geoffrey Christopher Rapp, "Unmanned Aerial Exposure: Civil Liability Concerns Arising From Domestic Law Enforcement Employment of Unmanned Aerial Systems," *North Dakota Law Rev*iew Vol 85: No 3 (2009): 623-648. Pg. 631. Available at: http://web.law.und.edu/LawReview/issues/web_assets/pdf/85-3/85NDLR623.pdf

[52] Stephen Dean, "Local 2 Investigates Police Secrecy Behind Unmanned Aircraft Test," *Click2Houston.com*, 21 November 2007, http://www.click2houston.com/investigates/14659066/detail.html

in Class G airspace (uncontrolled airspace), which didn't require a NOTAM (Notice to Airmen) or TFR (temporary flight restriction)[53], but the Houston PD informed the local news station that a NOTAM was issued and that the entire area was restricted.[54] The *perception* of wrong doing must be addressed. To further protect the rights of U.S. persons, the research community operators would implement guidance within their organizations as to the proper dissemination of their collected material, and instruction of how to handle incidental collection of information on U.S. persons, to include potential information on witness violations of law. Most importantly, laws outlining the penalties for using RPA to violate the civil rights of U.S. persons would be more clearly established, so that the public may know that it is taken seriously and there are repercussions.

The second part, training programs for all sensor operators from all agencies, would help to ensure that not only are the new regulations fully disseminated and understood by the affected agencies, but would also serve to better educate *all* users of RPA to the potential risks of civil rights abuse via the incidental, accidental, or intentional collection of information on U.S. persons. This education would help the users to better understand the risks of compromise, so that they can better protect the information they are being entrusted with, very similar to the training many military members receive on the protection of classified material and Operation Security (OPSEC). Just because something is not classified does not mean it is not an OPSEC threat, and just because information was collected via RPA for research purposes, does not mean it cannot be used inappropriately to violate someone's civil rights. Education can address this issue.

---

[53] Rob Stapleton, "More UAV Flights for Law Enforcement in US Airspace Planned," *Aero-News.net*, 30 November 2007, http://www.aero-news.net/index.cfm?ContentBlockID=114cd093-f6c8-4f43-a77c-f2f44247babc.
[54] Stephen Dean, "Local 2 Investigates Police Secrecy Behind Unmanned Aircraft Test," *Click2Houston.com*, 21 November 2007, http://www.click2houston.com/investigates/14659066/detail.html

The impact of this course of action would vary. Encryption technology may increase the cost of operating an RPA, potentially limiting access to them for some law enforcement organizations. By more clearly defining the times that a warrant is required to use an RPA to collect evidence, there may be few instances where an RPA can be utilized, but on those occasions (such as over watch for a tactical operation), there will be less concern over cases being appealed based on their use. The need to announce the law enforcement presence in certain situations will restrict the mission accomplishment if the reason the RPA was going to be utilized was as a stealth asset to collect evidence. The implementation of guidance in the research community on handling information collected on U.S. persons should have no impact on the mission effectiveness, as it is just providing guidance on the incidental collection and should not impact their primary mission. The implementation of clearly stated penalties and training programs should have no impact on the mission effectiveness of any of the organizations. Overall, this COA receives a "-1" for a slight impact on mission accomplishment capability.

These new regulations and training programs will address areas that have been highlighted as areas of potential civil rights abuse. By addressing not only the physical areas of weakness in the regulations, but also by addressing the perceptions of possible wrong doing through the implementation of clearly stated punishments and requiring greater transparency to the operations, this COA has a significant positive impact on the protection of civil rights. This COA receives a "+2" for this criterion.

The determination of when use of an RPA will require a warrant will be a difficult one to make as it involves Constitutional law and the application of the Fourth Amendment to new technologies. As has already been noted, this is an area that has not been well defined to date. The implementation of the other recommended regulations and training programs will only be

slightly difficult, as any new regulations take time to implement and training takes time away from the primary mission. Due to the Constitutional law implications the final criterion of feasibility of implementation will get a "-2" for significantly difficult to implement.

Table 2: COA #2 Assessment Results

Criteria	COA #2
Impact on Mission Accomplishment Capability	-1
Impact on Protection of Civil Rights	+2
Feasibility of Implementation	-2

The final alternative course of action is to not change any of the current regulations and training programs. This course of action would immediately terminate any pending changes to FAA regulations that would seek to open more airspace to RPA, while continuing to permit the current waiver process and granting of Certificates of Airworthiness to operate, on a limited basis, outside restrict airspace. No new regulations requiring encryption, or stipulating how information incidentally collected on U.S. persons by the research agencies would be implemented.

In terms of mission accomplishment capability, all agencies would be able to continue to accomplish their missions at the current level, but any further growth in capability would be limited by the lack of progress in integrating the RPA into the NAS. Impact on mission accomplishment capability would rate a "0".

By keeping all the same regulations and training, there will be a slightly positive impact on the protection of civil rights due to the termination of the integration of RPA into the NAS.

The privacy concerns will remain, however, as long as there remains a perception of possible wrong doing on the part of the RPA users. Since no new regulations would be implemented demonstrating the increased awareness of the need to protect and properly utilize the information collected by RPA, these concerns will continue to be present. Overall, this COA receives a rating of "+1" for impact on protection of civil rights.

Given the overwhelming desire for RPA to be integrated into the NAS, terminating this pursuit and keeping all the current regulations and training programs the same is not a feasible course of action. The expanded capability that operating RPA in the NAS would provide to not just the law enforcement community, but the research community as well is too much of an advantage. Integration of RPA into the NAS would allow a quicker response by assets, which would no longer require waivers, to areas of natural disaster, aiding in the faster identification of survivors and allowing for more efficient search and rescue operations. Law enforcement applications would be expanded as the RPA could now be used in a wider variety of situations and applications over urban areas. Researchers want to use them in hurricanes and tornados that are over non-restricted airspace.[55] Putting a stop to the eventual integration RPA into the NAS is not realistic. This COA rates a "-3" on the feasibility of implementation criterion.

Table 3: COA #3 Assessment Results

Criteria	COA #3
Impact on Mission Accomplishment Capability	0
Impact on Protection of Civil Rights	+1
Feasibility of Implementation	-3

[55] Joan Lowy, "FAA under pressure to open US skies to drones," *My Way News,* 14 June 2009, http://apnews.myway.com/article/20100614/D9GB009G0.html.

Chapter 5: Solution and Implementation Recommendations

As has been previously stated, the best course of action is going to be the best possible balance between mission accomplishment and the protection of civil liberties. As Table 4 shows, COA #2, the creation of additional regulations governing domestic RPA usage, with training programs for all sensor operators, provides the best balance of these two criteria along with the best feasibility of implementation.

Table 4: Summary of Assessment Results

Criteria	COA #1	COA #2	COA #3
Impact on Mission Accomplishment Capability	-2	-1	0
Impact on Protection of Civil Rights	+2	+2	+1
Feasibility of Implementation	-3	-2	-3
Total	-3	-1	-2

The first step to implementing this COA is the implementation of federal guidance that will then form the basis for agency regulations. The existing model of the Intelligence Oversight program provides a solid starting place. The top level regulations need to clearly outline when it is acceptable to collect information on U.S. persons, when that information may be retained and for how long and how it may be disseminated. It should also address, in general terms, a set level of protection of the information that must be maintained to protect civil rights. Scope of application will be dependent on the mission of the agency, as is true with intelligence oversight. For example, all agencies, regardless of whether they are law enforcement, intelligence or

research, would have to adhere to the protections that must be afforded any information collected related to U.S. persons. Additionally, similar to the existing intelligence oversight regulations, there will be guidance as to the handling of information collected regarding possible violations of law, whether intentionally collected or not. Law enforcement agencies would then have additional restrictions outlined for them in the sections discussing when, how and why information may be collected on U.S. persons. Since intelligence agencies must abide by law enforcement procedures and protocols when supporting law enforcement, they would then fall under this same guidance, thereby supplementing the existing intelligence oversight guidance. Once this high level general guidance is implemented, the various agencies would then be responsible for developing the necessary regulations to implement the guidance, just as DODD 5240.1-R and AFI 14-104 further develop the Intelligence Oversight program directed by EO12333.

As the agencies develop their implementation regulations, they should also develop the associated training programs to educate their staffs on the regulations. By allowing the agencies to develop their own implementation programs, the agencies will be able to address mission specific challenges in implementation. While it is recommended that law enforcement and intelligence agencies be required to declare their presence and intent to collect in certain situations, the research community would not need such regulations or procedures. On the other hand, the research agencies use a wider variety of sensors in a wider variety of environments and may share their scientific findings with a wider audience. Therefore, they may need to establish more procedures regarding how the information will be reviewed and sanitized prior to release to address any incidental or accidental collection of protected information, to meet the standards set down by the overarching regulations.

Mandatory encryption of RPA signals, by all agencies, will require some allowance of flexibility, as well. Since the purpose of the encryption is to prevent an unauthorized third party from intercepting the RPA signal, and the associated data being collected, it would not make sense for all agencies to use the same encryption. The individual agencies would need to be responsible for determining the level and type of encryption technology that best suits their needs, while meeting the level of information protection stipulated by the higher level guidance. Factors that will need to be taken into consideration will include cost, sensitivity of the information to be protected, and compatibility across agencies if there is a need to share information.

While the overall guidance will stipulate what situations, in general, it is permissible to utilize RPA domestically, the question of what specific situations will require that law enforcement have a warrant will need to be addressed elsewhere, as it speaks to Constitutional law. As mentioned previously, this will be one of the most difficult portions of COA #2 to implement. Determinations will need to be made regarding what technology is considered to be "generally in public use",[56] what situations require law enforcement to self-identify, and whether any special justification is required to obtain a warrant beyond that required for a standard search warrant, given the fact the collection asset is operating in public, vs. a targeted search of a set domicile by humans. For example, if a search warrant is approved to do surveillance on one domicile, but the camera picks up illegal activity next door, does the warrant extend to that domicile by virtue of the fact it was in the sensor's field of view?

[56] http://www.sherdog.net/forums/f54/uav-surveillance-advancing-rapidly-1036505/ - In 2001, the United States Supreme Court decided that performing FLIR surveillance of private property without a search warrant by law enforcement violates the Fourth Amendment's protection from unreasonable searches and seizures. Kyllo v. United States, 533 U.S. 27 (2001) KYLLO V. UNITED STATES

Regarding penalties for misuse of RPA domestically, a number of punitive avenues already exist and will be strengthened by the recommended new guidance. If an individual or agency fails to properly protect the information collected by the RPA per the overarching guidance, there are statutes for the protection of sensitive and classified information they can be punished under. If an RPA flies outside the areas it is authorized, there are existing repercussions via the FAA. Under the recommended new regulations designed to address incidental and accidental collection of information on U.S. persons, a researcher could be punished by his own organization for failure to follow established protocols for sensor operation, resulting in improper collection. If there is suspected intentional misuse of RPA for unauthorized purposes, resulting in the unauthorized collection on U.S. persons, Title 50, Chapter 36, "Foreign Intelligence Surveillance" provides detailed criminal sanctions, allowing for fines up to $10,000 and/or imprisonment up to 5 years, in addition to civil liability.[57] While having avenues of discipline is no guarantee that the regulations will be obeyed, having a means to enforce those regulations is an important step toward reassuring the public that their concerns are taken seriously and that there are repercussions for those that may try to violate their civil rights.

Chapter 6: Conclusion

There is no easy solution to address the potential for civil rights abuses through domestic RPA usage. The benefits that RPA provide to researchers, law enforcement, emergency response forces, and others, are well documented. The benefits of utilizing RPA domestically outweigh the negative of a potential compromise of civil rights, but that does not mean all steps

[57] Title 50 of the U.S. Code, Chapter 36, "Foreign Intelligence Surveillance," CAO 1 February 2010. Accessible at: http://uscode.house.gov/download/title_50.shtml

should not be taken to prevent such an event before it comes to pass. It is the pragmatic course of action to try to mitigate these concerns before an accidental infringement results in a call for all domestic RPA usage to be placed on hold, or become so restricted as to be useless to the mission. Through the implementation of new regulations and subsequent training for RPA operators, these concerns can be addressed. The government has a solid starting point for the creation of these regulations in the model of existing intelligence oversight regulations, as well as the existing avenues of punitive action for violations.

There are areas where further research needs to be done before further guidance can be established. The legal community is actively exploring the issues associated with the constitutional implications of using RPA in law enforcement. The ACLU is continuing to bring attention to surveillance that is viewed as infringing on individuals' civil rights and privacy, as is evidenced by a recent report on the proliferation of surveillance cameras in Chicago, and making recommendations for how the surveillance can become less intrusive.[58] The proliferation of FPV videos generated from RC aircraft opens the discussion up to whether there needs to be laws governing what type of collection the private individual can engage in with aircraft classified as "recreational". Raphael Pirker (the individual that did the FPV of New York City) stated in an interview with Flite Test, that there are perceived to be few limitations for the operation of recreational RC aircraft.[59] Regardless of whether or not there is an actual intention to use RPA to make inroads on the civil rights of U.S. persons, the public has a voiced a concern that needs to be addressed.

---

[58] ACLU of Illinoi, "Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy," ACLU of Illinois, February 2011, accessed at http://il.aclu.org/site/DocServer/Surveillance_Camera_Report1.pdf?docID=3261.

[59] http://www.youtube.com/watch?v=2MwfEVIfiGs – "Flite Test - Trappy Interview"

Bibliography

Air Combat Command, "480th ISR Wing supports disaster relief efforts," *Inside ACC*, 15 January 2010, http://www.acc.af.mil/news/story.asp?id=123185802.

Alex Altman, "TSA Scrambles to Combat the Outcry Over Body Scanning," *Time*, 23 November 2010, http://www.time.com/time/nation/article/0,8599,2032786,00.html

Amazon.com, "Extech i5 Thermal Imaging Camera," http://www.amazon.com/Extech-i5-Thermal-Imaging-Camera/dp/B003B3N60E

ACLU of Illinois, "Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy," ACLU of Illinois, February 2011, accessed at http://il.aclu.org/site/DocServer/Surveillance_Camera_Report1.pdf?docID=3261.

Activist Post, "Drone Surveillance Program Targeting Americans?" Infowars.com, 9 November 2010, http://www.infowars.com/drone-surveillance-program-targeting-americans/

American Civil Liberties Union, "ACLU Spy Files," http://www.aclu.org/spy-files

Brenda Livingston, "The Role Of UAVs/MAVs In Domestic Surveillance And Control," Rense.com, http://www.rense.com/general47/uav.htm

California v. Ciraolo, 476 U. S. 207 (1986)

Customs and Border Protection, "UAS Overview," http://www.cbp.gov/xp/cgov/border_security/air_marine/uas_program/uasoverview.xml

Department of Defense (DOD) Directive 5240.1-R. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

Executive Order 12333. *United States Intelligence Activities*, 4 December 1981, as amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008).

Federal Aviation Administration, *Aeronautical Information Manual*, 11 February 2010

Federal Aviation Administration, "FAA Civil/Public UAS Roadmap," http://www.faa.gov/about/initiatives/uas/

Federal Aviation Administration, Interim Operational Approval Guidance 08-01. *Unmanned Aircraft Systems Operations in the U. S. National Airspace System*, 13 March 2008.

Federal Aviation Administration, "Unmanned Aircraft Systems Office," http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/

FPVpilot.Com, http://fpvpilot.com/default.aspx

Gautham Nagesh, "ACLU launches 'Spyfiles' to track domestic surveillance," Hillicon Valley, 26 Jane 2010, http://thehill.com/blogs/hillicon-valley/technology/106299-aclu-launches-qspyfilesq-to-track-domestic-surveillance

Geoffrey Christopher Rapp, "Unmanned Aerial Exposure: Civil Liability Concerns Arising From Domestic Law Enforcement Employment of Unmanned Aerial Systems," *North Dakota Law Rev*iew Vol 85: No 3 (2009): 623-648. Available at: http://web.law.und.edu/LawReview/issues/web_assets/pdf/85-3/85NDLR623.pdf

Hooked on RC Airplanes, "Scale RC Airlanes," http://www.hooked-on-rc-airplanes.com/scale-rc-airplanes.html

Joan Lowy, "FAA under pressure to open US skies to drones," *My Way News*, 14 June 2009, http://apnews.myway.com/article/20100614/D9GB009G0.html.

Kyllo v. United States, 533 U.S. 27 (2001)

Les Dorr, Jr. & Alison Duquette, "Fact Sheet – Unmanned Aircraft Systems (UAS), FAA News Release, 1 December 2010, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287 (accessed 15 January 2011).

Marnie Hunter, "Jesse Ventura slams TSA with lawsuit," CNN Travel, 25 January 2011, http://articles.cnn.com/2011-01-25/travel/jesse.ventura.tsa.lawsuit_1_pat-downs-and-full-body-tsa-lawsuit?_s=PM:TRAVEL

Ms. Smith, "TSA: Show Us Your Body, or We'll Feel You Up," NetworkWorld.com, 1 November 2010, http://www.networkworld.com/community/blog/tsa-show-us-your-body-or-well-feel-you

NASA, "NASA Aircraft Flies California Post-burn Imaging Mission," NASA News Release, 24 November 2009, http://www.nasa.gov/centers/dryden/news/NewsReleases/2009/09-71.html (accessed 16 January 2011).

NASA, "NASA Flight Research Projects," http://www.nasa.gov/centers/dryden/research/index.html

NOAA, "NOAA UAS Town Hall - AUVSI Conference" (Presentation, AUVSI Conference, Washington, D.C., 8 December 2007). Accessible at http://uas.noaa.gov/library/presentations/index.html

Ole Ole Olson, " Domestic Espionage Alert: Spy Drone Discovered," NewsJunkie.com, 8 January 2010, http://newsjunkiepost.com/2010/01/08/domestic-espionage-alert-spy-drone-discovered/

Paul Lewis, "CCTV in the sky: police plan to use military-style spy drones," *The Guardian,* 23 January 2010, http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones

Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, 22 January 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html (accessed 22 January 2011).

Rob Stapleton, "More UAV Flights for Law Enforcement in US Airspace Planned," *Aero-News.net*, 30 November 2007, http://www.aero-news.net/index.cfm?ContentBlockID=114cd093-f6c8-4f43-a77c-f2f44247babc.

RyanLA, "Drone Aircraft are Patrolling U.S. Cities," *Public Intelligence*, 27 April 2010, http://www.operationdefuse.com/2010/04/27/drone-aircraft-are-patrolling-u-s-cities/ -

Sara Summers, "TAAC 2007 Conference NOAA UAS Applications" (Presentation, TAAC, Albuquerque, NM, 6 December 2007).

Spencer Ackerman, "Even DHS is freaked out by spy drones over America," *Danger Room*, 26 January 2011, http://www.wired.com/dangerroom/2011/01/spy-drones-over-america-dhs-would-rather-not/

Staff Sgt. Amy Robinson, "FAA authorizes Predators to seek survivors," Air Force Print News Today, 27 July 2006, http://www.af.mil/news/story.asp?storyID=123024467 (accessed 30 August 2009).

Stephen Dean, "Local 2 Investigates Police Secrecy Behind Unmanned Aircraft Test," *Click2Houston.com*, 21 November 2007, http://www.click2houston.com/investigates/14659066/detail.html

Tim Elfrink, "Miami-Dade police buy drones," Miami NewTimes, 09 December 2010, http://www.miaminewtimes.com/2010-12-09/news/miami-dade-police-buy-drones/ (accessed 7 January 2011).

Title 14 of the Code of Federal Regulations, Section 91.113. "Right-of-way rules: Except water operations," CAO 13 January 2011. Accessible at: http://www.gpoaccess.gov/ecfr/
Title 50 of the U.S. Code, Chapter 36, "Foreign Intelligence Surveillance," CAO 1 February 2010. Accessible at: http://uscode.house.gov/download/title_50.shtml
U.S. Constitution, Fourth Amendment.
U.S. Office of the Secretary of Defense, *Unmanned Aircraft Systems (UAS) Roadmap, 2005-2030* (Washington D.C.: U.S. Department of Defense, August 2005).
YouTube, "Flite Test - Trappy Interview," http://www.youtube.com/watch?v=2MwfEVIfiGs
YouTube, "FPV rc plane night flight police helicopter chase," http://www.youtube.com/watch?v=nifuuM9oltU
YouTube, "New York City," http://www.youtube.com/watch?v=M9cSxEqKQ78